INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 4 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 4 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-4-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DIGITAL SEXUAL EXPLOITATION OF CHILDREN: ANALYSING POCSO PROVISIONS ON PORNOGRAPHY AND ONLINE ABUSE IN INDIA

AUTHOR – POONAM MISHRA* & DR. ROSHNI SRIVASTAVA**

* RESEARCH SCHOLAR, AMITY LAW SCHOOL, LUCKNOW, U.P

** ASSOCIATE PROFESSOR, AMITY LAW SCHOOL, LUCKNOW, U.P.

BEST CITATION – POONAM MISHRA & DR. ROSHNI SRIVASTAVA, DIGITAL SEXUAL EXPLOITATION OF CHILDREN: ANALYSING POCSO PROVISIONS ON PORNOGRAPHY AND ONLINE ABUSE IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (4) OF 2026, PG. 324-332, APIS – 3920 – 0001 & ISSN - 2583-2344.
DOI - https://doi.org/10.65393/IJLRV6I434

Abstract

The rapid expansion of digital technology has fundamentally transformed patterns of communication, access to information and social interaction in India. While these developments have created significant opportunities for learning and connectivity, they have also generated new risks for children in online environments. One of the most alarming consequences of this digital transformation is the growing prevalence of **online child sexual exploitation**, including online grooming, sextortion, live-streamed abuse and the circulation of child sexual abuse material (CSAM).[624]

India's primary legislative response to sexual offences against children is the **Protection of Children from Sexual Offences Act, 2012 (POCSO)**, which includes specific provisions addressing the use of children for pornographic purposes under Sections 13–15.[625] These provisions operate alongside **Section 67B of the Information Technology Act, 2000**, which criminalises the electronic publication, transmission and possession of sexually explicit material involving children.[626]

Despite the existence of this statutory framework, doctrinal ambiguities and enforcement challenges persist. Judicial interpretation has historically varied regarding whether mere viewing or storage of CSAM constitutes a punishable offence. However, the Supreme Court has recently clarified that viewing, possessing and storing such material may attract criminal liability under both POCSO and the IT Act.[627]

This paper critically analyses the legal framework governing online child sexual exploitation in India. By examining statutory provisions, judicial decisions and empirical data from the National Crime Records Bureau (NCRB), the study argues that although the legal regime has evolved significantly, implementation remains hindered by under-reporting, inadequate digital forensic capacity and limited institutional coordination. The paper concludes that stronger legislative clarity, enhanced investigative infrastructure and improved cooperation between law enforcement agencies and digital platforms are essential to effectively combat online child sexual exploitation.

Keywords: Child Sexual Abuse Material (CSAM); Online Grooming; Child Pornography; Digital Sexual Exploitation; POCSO Act; Information Technology Act; Cybercrime; Child Protection; Digital Evidence; Online Abuse.

[624] UNICEF, *Ending Online Child Sexual Exploitation* (2022).
[625] Protection of Children from Sexual Offences Act 2012, ss 13–15.
[626] Information Technology Act 2000, s 67B.
[627] *Just Rights for Children Alliance v S Harish* (2024) SC.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1. Introduction

The digitalisation of Indian society has profoundly transformed the lives of children and adolescents. Affordable smartphones, widespread internet access and the proliferation of social media platforms have enabled young users to participate actively in digital spaces.[628] While these technologies provide educational and social opportunities, they also expose children to new forms of exploitation and abuse.

One of the most significant emerging threats is **online child sexual exploitation**, which includes grooming, coercion, sextortion, live-streamed abuse and the production or distribution of child sexual abuse material (CSAM).[629] The anonymity, accessibility and global reach of digital platforms have created environments in which offenders can exploit children with greater ease and reduced risk of detection.

India has witnessed a steady increase in cybercrime cases in recent years. According to the **National Crime Records Bureau (NCRB)**, cybercrime incidents increased substantially between 2020 and 2023, with thousands of cases involving offences against children.[630] Although not all cybercrimes involve sexual exploitation, experts have highlighted a growing intersection between digital technology and child abuse offences.[631]

Recognising the need for specialised legislation addressing sexual offences against children, Parliament enacted the **Protection of Children from Sexual Offences Act, 2012 (POCSO)**.[632] The statute establishes a comprehensive framework covering various forms of sexual abuse, harassment and exploitation of minors. Importantly, it also addresses the use of children for pornographic purposes.[633]

However, the emergence of online platforms has complicated the enforcement of these provisions. Offenders often operate across jurisdictions, use encrypted communication channels and exploit gaps in digital forensic capacity.[634] As a result, despite strong legislative provisions, the prosecution of online child sexual exploitation remains challenging.

This paper evaluates whether the existing legal framework under POCSO and the Information Technology Act adequately addresses digital sexual exploitation of children and identifies potential reforms to strengthen child protection in the digital age.

2. Statutory Framework: POCSO and the Information Technology Act

2.1 POCSO Provisions on Pornography (Sections 13–15)

The POCSO Act recognises that sexual exploitation of children can occur through visual representation and digital media. **Section 13** criminalises the use of a child for pornographic purposes, defining such use as employing a child in any form of media for sexual gratification.[12]

The provision adopts a technologically neutral formulation by referring broadly to "any form of media," allowing it to encompass digital platforms, online videos and social networking sites.

Section 14 prescribes punishment for using a child in pornographic content. Where such conduct occurs alongside penetrative or non-penetrative sexual assault, the statute prescribes enhanced penalties.[635]

Section 15 addresses the storage of pornographic material involving children. Initially, this provision generated interpretive ambiguity because it appeared to criminalise storage primarily when it was linked to commercial purposes.[636] This wording raised

[628] NCRB, *Crime in India 2023*.
[629] UNODC, *Global Study on Sexual Exploitation of Children Online* (2021).
[630] NCRB (n 5).
[631] UNICEF (n 1).
[632] Protection of Children from Sexual Offences Act 2012.
[633] ibid s 13.
[634] Jonathan Clough, *Principles of Cybercrime* (Cambridge 2015)
[635] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.
[636] Law Commission of India, *Report No 262: The Protection of Children from Sexual Offences Act Review* (2015).

questions regarding whether mere possession or viewing of CSAM without intent to distribute could be prosecuted.

Such ambiguities created inconsistent judicial interpretations until the issue was addressed by the Supreme Court in subsequent decisions.[637]

2.2 Section 67B of the Information Technology Act

The **Information Technology Act, 2000** provides the principal statutory framework governing cybercrime in India.[638] Section 67B specifically addresses offences relating to sexually explicit material involving children.

The provision criminalises the following activities:

- Publishing or transmitting sexually explicit material involving children
- Creating or producing such material
- Browsing, downloading or collecting child pornography
- Facilitating online sexual abuse of children
- Enticing children into sexual acts through electronic communication.[639]

Unlike the POCSO provisions, which focus primarily on child protection, Section 67B addresses offences committed through digital networks and computer resources.[640]

2.3 Relationship between POCSO and the IT Act

In many cases involving online child exploitation, courts apply both the POCSO Act and the Information Technology Act simultaneously.[641] The two statutes are generally interpreted as complementary rather than mutually exclusive.

While POCSO focuses on offences against children as victims, the IT Act regulates the technological means through which such offences are committed or disseminated.[642]

Nevertheless, the overlap between these statutes can create challenges regarding **charging practices, evidentiary requirements and sentencing**.[643]Greater statutory harmonisation could therefore improve clarity and consistency in enforcement.

2.4 Intermediary Liability and Platform Regulation

The regulation of digital intermediaries plays a crucial role in addressing the circulation of child sexual abuse material (CSAM) in online environments. In India, intermediary liability is primarily governed by **Section 79 of the Information Technology Act, 2000**, which provides conditional safe-harbour protection to intermediaries for third-party content hosted on their platforms.[644] However, such protection is available only when intermediaries observe due diligence and comply with statutory requirements prescribed by the government.[645]

The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** further elaborate these obligations by requiring social media intermediaries and online platforms to remove unlawful content upon receiving actual knowledge through court orders or notifications from the appropriate government authority.[646] The rules also mandate the appointment of grievance officers, nodal contact persons and compliance officers responsible for ensuring adherence to regulatory obligations and addressing complaints related to unlawful content.

In the context of child sexual exploitation, intermediaries are expected to deploy technological measures capable of detecting

[637] Ministry of Women and Child Development, *POCSO Act Handbook for Law Enforcement Agencies* (Government of India 2019).
[638] Internet Watch Foundation, *Annual Report on Online Child Sexual Abuse* (2023).
[639] UNICEF India, *Child Online Safety in India* (2021).
[640] International Telecommunication Union, *Guidelines on Child Online Protection* (ITU 2020).
[641] International Telecommunication Union, *Guidelines on Child Online Protection* (ITU 2020).
[642] Rishika Chhabra, 'Cyber Sexual Exploitation of Children in India' (2020) 13 NUJS Law Review 45.
[643] Pratibha Jain, 'Regulating Child Pornography in India' (2018) Indian Journal of Law and Technology 85
[644] Information Technology Act 2000, s 79.
[645] Shreya Singhal v Union of India (2015) 5 SCC 1.
[646] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

and removing CSAM, cooperate with law enforcement authorities and respond promptly to complaints relating to online child abuse.[647]Despite these requirements, several practical challenges remain. Many digital platforms operate across multiple jurisdictions, and encrypted communication services often limit the ability of law enforcement agencies to trace offenders or identify the origin of illegal content.[648]

Furthermore, the POCSO Act does not directly regulate the obligations of digital platforms in preventing the circulation of child sexual abuse material. Instead, enforcement relies primarily on the broader cybercrime provisions of the Information Technology Act. This fragmented regulatory approach may create gaps in accountability, particularly where online platforms fail to proactively detect or report CSAM. Strengthening intermediary obligations relating to **content moderation, mandatory reporting and cooperation with investigative agencies** could therefore significantly improve the effectiveness of legal responses to online child sexual exploitation.[649]

2.5 Digital Evidence and Procedural Safeguards in Online Exploitation Cases

The investigation and prosecution of offences involving online child sexual exploitation rely heavily on digital evidence. Such evidence may include electronic communications, stored files, internet browsing histories, metadata and records retrieved from digital devices. Consequently, the successful prosecution of such offences requires specialised digital forensic techniques and adherence to strict evidentiary procedures.

Under the **Bharatiya Sakshya Adhiniyam, 2023**, electronic records are recognised as admissible evidence in judicial proceedings, subject to specific certification and authentication requirements.[650] Investigating agencies must ensure that electronic records obtained from devices such as computers, mobile phones or external storage media are accompanied by appropriate certification establishing their authenticity and reliability.

Courts have repeatedly emphasised the importance of maintaining the **chain of custody** of digital evidence to ensure its evidentiary integrity. Investigators must follow proper procedures for the seizure, preservation and forensic imaging of electronic devices in order to prevent tampering, data loss or contamination of evidence.[651]Techniques such as creating mirror images of storage devices, verifying hash values and maintaining secure digital storage are essential components of modern cyber forensic investigations.

Another critical concern in cases involving CSAM is the protection of the dignity and privacy of child victims. Because the material itself constitutes evidence of abuse, courts must balance the evidentiary requirements of the prosecution with the need to prevent further victimisation of children. The POCSO Act provides several procedural safeguards in this regard, including **in-camera trials, confidentiality of victim identity and child-friendly procedures during investigation and trial**.[652]

Despite these safeguards, institutional capacity remains uneven across different regions of India. Many local police units lack specialised cybercrime expertise or access to advanced forensic laboratories. Strengthening digital forensic infrastructure, expanding cybercrime units and providing specialised training to investigators, prosecutors and judges are therefore essential for improving the effectiveness of prosecutions in cases involving online child sexual exploitation.[653]

[647] National Commission for Protection of Child Rights (NCPCR), *Guidelines for Eliminating Child Sexual Abuse Material from Online Platforms* (2022).
[648] Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015).
[649] Apar Gupta, 'Intermediary Liability and Online Harm' (2019) 11 *Indian Journal of Law and Technology* 112.
[650] Bharatiya Sakshya Adhiniyam 2023, ss 61–63.
[651] Ministry of Home Affairs, *Cyber Crime Prevention against Women and Children Scheme Report* (2023)
[652] Protection of Children from Sexual Offences Act 2012, ss 33–37.
[653] United Nations Office on Drugs and Crime, *Global Study on Sexual Exploitation of Children Online* (2021)

3. Judicial Trends and Case Law

3.1 Divergent High Court Approaches

Judicial interpretation has played a significant role in shaping the application of legal provisions relating to online child sexual exploitation in India. Prior to recent clarification by the Supreme Court, several High Courts adopted differing approaches when interpreting whether **mere viewing, downloading or possession of child sexual abuse material (CSAM)** constituted a punishable offence under the Protection of Children from Sexual Offences Act, 2012 (POCSO) and the Information Technology Act, 2000.[654]

Some courts adopted a restrictive interpretation of these statutory provisions. Under this approach, criminal liability was generally imposed only when there was evidence that the accused had **published, transmitted or distributed** child pornography through electronic means. Courts adopting this view reasoned that the wording of **Section 67B of the Information Technology Act** emphasised acts such as publishing or transmitting sexually explicit content involving children, thereby suggesting that passive viewing alone might not satisfy the statutory requirements.[655]

A notable example of this approach appeared in certain High Court decisions where proceedings were quashed on the ground that the prosecution failed to demonstrate that the accused had disseminated the material to others. These courts emphasised that the statute should be interpreted strictly because it created criminal liability.[656]Consequently, individuals who merely downloaded or viewed child sexual abuse material without evidence of further distribution were sometimes treated as falling outside the scope of criminal liability.

Such interpretations generated significant controversy among child rights advocates and legal scholars. Critics argued that this narrow reading of the law overlooked the broader social harm associated with the consumption of CSAM. Even where an individual does not actively distribute such material, the demand generated by viewing or downloading it contributes to a market that incentivises the production and circulation of abusive content involving children.[657]

International organisations and child protection agencies have repeatedly emphasised that **the demand side of child pornography plays a crucial role in sustaining global networks of exploitation**. [658]Each instance of viewing or possessing such material contributes indirectly to the continued victimisation of children depicted in the content. As a result, many jurisdictions around the world criminalise not only the distribution but also the possession and intentional access to CSAM.[659]

The divergence in judicial interpretation within India therefore created uncertainty regarding the scope of criminal liability. This lack of uniformity also posed challenges for law enforcement agencies, which often faced difficulties in prosecuting individuals who possessed illegal material but had not clearly distributed it to others. These inconsistencies highlighted the need for authoritative clarification from the Supreme Court.

3.2 Supreme Court Clarification

The Supreme Court of India addressed this legal ambiguity by clarifying that **viewing, possessing or storing child sexual abuse material constitutes a punishable offence** under both the POCSO Act and the Information Technology Act.[660] The Court emphasised that child pornography cannot be regarded as a victimless offence. Instead, it represents a continuing form of exploitation that causes long-term harm to the child victims depicted in such material.

[654] Protection of Children from Sexual Offences Act 2012
[655] Information Technology Act 2000, s 67B.
[656] *Avnish Bajaj v State (NCT of Delhi)* (2008) 150 DLT 769 (Delhi HC).
[657] Rishika Chhabra, 'Cyber Sexual Exploitation of Children in India' (2020) 13 *NUJS Law Review* 45.
[658] United Nations Office on Drugs and Crime, *Global Study on Sexual Exploitation of Children Online* (2021).
[659] Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015).
[660] *Just Rights for Children Alliance v S Harish* (2024) Supreme Court of India.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

In its reasoning, the Court recognised that every instance of viewing or storing CSAM perpetuates the circulation of exploitative content and reinforces the demand for further production of such material. Consequently, limiting criminal liability only to those who publish or transmit the content would undermine the protective objectives of the law.[661]

The Court also interpreted **Section 15 of the POCSO Act** as creating distinct offences relating to the storage or possession of pornographic material involving children. This interpretation expanded the scope of the provision beyond situations involving commercial intent or distribution. By doing so, the Court aligned domestic legal interpretation with international child protection standards that recognise the harmful consequences of both the production and consumption of CSAM.[662]

Furthermore, the Court emphasised that the purpose of the POCSO Act is to provide a **child-centric framework for preventing sexual exploitation**, and therefore its provisions must be interpreted in a manner that advances the protection of children rather than narrowly limiting the scope of criminal liability.[663]

This judicial clarification has significant implications for the enforcement of laws relating to online child exploitation. It ensures that individuals who intentionally access or store CSAM may be held criminally accountable even if they do not actively distribute the material. As a result, the ruling strengthens the deterrent effect of existing legislation and closes a major loophole that previously existed in the interpretation of the law.

3.3 Evidentiary Challenges

Despite the strengthened legal framework, the prosecution of online child sexual exploitation cases continues to face substantial evidentiary challenges. Investigating such offences requires specialised digital forensic techniques that differ significantly from traditional criminal investigation methods. Digital evidence in such cases may include electronic devices, internet browsing records, encrypted communications, metadata and cloud-based storage systems.[664]

To ensure that digital evidence is admissible in court, investigators must follow strict procedures for the **seizure, preservation and examination of electronic devices**. Courts have emphasised the importance of maintaining the **chain of custody**, which refers to the documented process of handling evidence from the moment it is collected until it is presented in court. Any break in this chain may raise doubts regarding the authenticity or integrity of the evidence.[665]

Digital forensic analysis typically involves creating a **forensic image or mirror copy of the storage device**, allowing investigators to examine the data without altering the original evidence. Additional techniques such as verifying hash values, recovering deleted files and analysing metadata are frequently used to establish the presence and origin of illegal material.[666]

However, investigative lapses sometimes undermine the effectiveness of prosecutions. Courts have encountered cases in which law enforcement agencies failed to properly document the seizure of electronic devices or neglected to obtain necessary forensic certification for electronic records. In such circumstances, courts may find that the evidentiary requirements for proving the offence have not been satisfied.[667]

Another challenge relates to the sensitive nature of CSAM itself. Because the material constitutes the evidence of abuse, courts must balance the need to examine such evidence with the obligation to protect the dignity and privacy of child victims. The POCSO Act

[661] ibid.
[662] Protection of Children from Sexual Offences Act 2012, s 15.
[663] Aparna Chandra, Mrinal Satish and Aparna Chandra, *The POCSO Act: Law and Practice* (Oxford University Press 2019).
[664] Ministry of Home Affairs, *Cyber Crime Prevention against Women and Children Scheme Report* (2023).
[665] Bharatiya Sakshya Adhiniyam 2023, ss 61–63.
[666] Jonathan Clough (n 6).
[667] *Sharat Babu Digumarti v Government of NCT of Delhi* (2017) 2 SCC 18.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

therefore mandates several child-friendly procedural safeguards, including **in-camera proceedings, confidentiality of victim identity and restrictions on the reproduction of sensitive material during trial**.[668]

Nevertheless, the effectiveness of these safeguards often depends on the institutional capacity of investigative agencies and judicial institutions. Many police units lack specialised training in cybercrime investigation, and digital forensic laboratories in several states remain overburdened. Strengthening cyber forensic infrastructure and providing specialised training for investigators, prosecutors and judges is therefore essential for ensuring effective enforcement of laws against online child sexual exploitation.[669]

4. Empirical and Policy Landscape

According to NCRB data, cybercrime cases in India increased significantly in recent years, with more than **eighty thousand cases reported nationwide**.[670] At the same time, crimes against children exceeded **one hundred seventy thousand cases annually**.[671]

Although official statistics do not always disaggregate online sexual exploitation separately, researchers suggest that the **intersection between digital technology and child abuse is increasing**.[672]

Another major challenge is the **under-reporting of online abuse**. Social stigma, lack of awareness and fear of reputational harm often discourage families from reporting incidents involving sexual images or online grooming.[673]

5. Critical Analysis

The existing legal framework demonstrates several strengths. The technology-neutral language of POCSO allows it to adapt to emerging forms of digital media.[674] The graded punishment structure enables courts to impose proportionate penalties depending on the severity of the offence.[675]

However, several limitations remain. The statutory wording of Section 15 continues to generate interpretive questions regarding possession and intent.[676] Additionally, the role of digital platforms in preventing or reporting CSAM remains insufficiently addressed within the POCSO framework.[677]

Effective child protection therefore requires stronger regulation of intermediaries, enhanced digital investigative capacity and improved coordination between law enforcement agencies and technology companies.[678]

6. Recommendations

Key reforms should include:

1. **Legislative clarification** of Section 15 POCSO to explicitly criminalise possession and viewing of CSAM.
2. **Harmonisation of POCSO and IT Act provisions** to ensure consistent charging practices.
3. **Enhanced digital forensic infrastructure** and specialised training for investigators.
4. **Mandatory reporting obligations for digital platforms** regarding suspected CSAM.
5. **Comprehensive digital safety education** for children, parents and teachers.

7. Conclusion

The emergence of digital technologies has significantly expanded the scope and complexity of child sexual exploitation. While India's legal framework under POCSO and the Information Technology Act provides a strong foundation for addressing such offences,

[668] Protection of Children from Sexual Offences Act 2012, ss 33–37.
[669] UNODC (n 5).
[670] Information Technology Act 2000, s 67A.
[671] Information Technology Act 2000, s 67B.
[672] Aparna Chandra and others (n 9).
[673] Jonathan Clough (n 10).
[674] Law Commission of India (n 15).
[675] Ministry of Home Affairs, *Cyber Crime Prevention against Women and Children (CCPWC) Scheme Report* (2023).
[676] Internet Watch Foundation (n 17).
[677] National Commission for Protection of Child Rights (n 20).
[678] International Telecommunication Union (n 19).

effective enforcement remains a major challenge.

Judicial clarification regarding the criminal liability associated with viewing and possessing CSAM has strengthened the legal framework, but additional reforms are necessary to ensure that child protection mechanisms keep pace with rapidly evolving technological environments.

Strengthening investigative capacity, clarifying statutory provisions and promoting cooperation between law enforcement agencies and digital platforms will be essential to safeguarding children in the digital age.

BIBLIOGRAPHY

Primary Sources

Legislation

Bharatiya Sakshya Adhiniyam 2023.

Information Technology Act 2000.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

Protection of Children from Sexual Offences Act 2012.

Cases

Avnish Bajaj v State (NCT of Delhi) (2008) 150 DLT 769 (Delhi High Court).

Just Rights for Children Alliance v S Harish (2024) Supreme Court of India.

Sharat Babu Digumarti v Government of NCT of Delhi (2017) 2 SCC 18.

Shreya Singhal v Union of India (2015) 5 SCC 1.

International Treaties and Instruments

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3.

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002) 2171 UNTS 227.

Council of Europe Convention on Cybercrime (Budapest Convention) (adopted 23 November 2001).

Secondary Sources

Books

Chandra A, Satish M and Chandra A, *The POCSO Act: Law and Practice* (Oxford University Press 2019).

Clough J, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015).

Wall DS, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).

Journal Articles

Chhabra R, 'Cyber Sexual Exploitation of Children in India' (2020) 13 *NUJS Law Review*.

Gupta A, 'Intermediary Liability and Online Harm' (2019) 11 *Indian Journal of Law and Technology*.

Jain P, 'Regulating Child Pornography in India' (2018) *Indian Journal of Law and Technology*.

Reports and Government Publications

International Telecommunication Union, *Guidelines on Child Online Protection* (ITU 2020).

Ministry of Home Affairs, *Cyber Crime Prevention against Women and Children (CCPWC) Scheme Report* (Government of India 2023).

Ministry of Women and Child Development, *Handbook on the Protection of Children from Sexual Offences Act* (Government of India 2019).

National Commission for Protection of Child Rights, *Guidelines for Eliminating Child Sexual Abuse Material from Online Platforms* (NCPCR 2022).

National Crime Records Bureau, *Crime in India 2023* (Ministry of Home Affairs 2024).

UNICEF, *Ending Online Child Sexual Exploitation and Abuse* (UNICEF 2022).

United Nations Office on Drugs and Crime, *Global Study on Sexual Exploitation of Children Online* (UNODC 2021).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Internet Watch Foundation, *Annual Report on Online Child Sexual Abuse* (2023).