INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

ONLINE GROOMING VIA GAMING AND SOCIAL MEDIA PLATFORMS: A LEGAL AND SOCIO-CRIMINOLOGICAL ANALYSIS

AUTHORED BY - SANNA SYLVIA & PROF. (DR.) M S BAINS[1]

ABSTRACT

Online grooming through gaming and social media platforms has emerged as a significant pathway to child sexual exploitation in India, facilitated by always-on connectivity, private messaging, voice chat, pseudonymous identities, and rapid cross-platform migration. This study undertakes a doctrinal and socio-criminological analysis of grooming as a process offence that progresses from contact and trust-building to sexualised communication, coercion, sextortion, and circulation of child sexual abuse material. The research examines the applicability of the Protection of Children from Sexual Offences Act, 2012—particularly Sections 11–15 and the reporting mandate under Sections 19 and 21—alongside the Information Technology Act, 2000 (Sections 67, 67A, 67B), and intermediary due diligence duties under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. It further evaluates constitutional protections under Articles 15(3) and 21, and highlights evidentiary challenges in electronic records under the Bharatiya Sakshya Adhiniyam, 2023. The study concludes with recommendations centred on safety-by-design, rapid evidence preservation, and victim-centric enforcement.

Keywords: Online grooming; Gaming platforms; Social media; POCSO; Intermediary liability; Child sexual abuse material

[1] Student of LLM, Student ID:25072001032, University School of Law, Rayat Bahra University, Mohali; Professor (DR.), University School of Law, Rayat Bahra University, Mohali,

1 INTRODUCTION

Online grooming through gaming and social media platforms has emerged as a distinct form of technology-facilitated child sexual exploitation in India, where offenders use in-game chats, direct messages, voice channels, livestream features, and algorithmic "friend/suggested contact" systems to initiate contact, build trust, desensitise boundaries, and progressively sexualise communication, often culminating in coercion for sexual images, extortion, or offline abuse. The Indian legal response is presently anchored in a combination of child-protection offences and cyber-content offences: the Protection of Children from Sexual Offences Act, 2012 (POCSO) addresses sexually motivated conduct against children and related duties of reporting, while the Information Technology Act, 2000 targets publication/transmission of obscene or sexually explicit material in electronic form, including child sexual abuse material. The regulatory layer under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 imposes due-diligence duties on intermediaries to curb unlawful content and enable grievance and takedown mechanisms, thereby linking platform governance with child safety outcomes.[2]

Within this framework, "grooming" behaviours commonly map onto specific statutory hooks rather than a single standalone offence label: POCSO criminalises sexual harassment of a child and prescribes punishment (Sections 11 and 12), criminalises use of a child for pornographic purposes (Section 13) and related pornography offences (Sections 14–15), and creates mandatory reporting and penal consequences for failure to report (Sections 19 and 21). Parallelly, the IT Act provides punishment for publishing/transmitting sexually explicit material (Sections 67 and 67A) and specifically criminalises child sexual abuse material in electronic form (Section 67B), while policy communication from the Government has emphasised these provisions and the role of the IT Rules, 2021 in platform due diligence.[3]

The problem is amplified by India's scale of child internet access and the design of interactive platforms: multiplayer games and major social networks create persistent, low-supervision contact zones where anonymity, pseudonymity, quick switching between platforms, and private channels reduce guardianship and increase offender reach. Reporting infrastructure exists (including a

[2] Catharina Drejer et al., "Livestreaming Technology and Online Child Sexual Exploitation and Abuse: A Scoping Review," 25 *Trauma, violence & abuse* 260–74 (2024).
[3] Sneha Mahawar, "Protection of Children from Sexual Offences Act (POCSO), 2012" *iPleaders*, 2024 *available at*: https://blog.ipleaders.in/pocso-act-everything-you-need-to-know/ (last visited April 28, 2026).

national portal with dedicated focus on online child sexual abuse material reporting), but under-reporting persists due to fear, shame, retaliation, and evidentiary complexity—making it crucial to examine both legal norms and socio-criminological realities, including platform affordances, victim vulnerability, and enforcement capacity.

1.1 Background of the Study

India's child-protection and cyber law architecture has to respond to grooming as a process crime that often begins with seemingly "non-criminal" interactions (friend requests, game invites, gifts/skins, private chats) but moves toward sexualised communication and exploitation. Because grooming frequently results in demands for sexual content, threats, and dissemination, the applicable legal approach typically combines POCSO's offence provisions (including Sections 11–12 on sexual harassment and Sections 13–15 on pornographic use and related acts) with the IT Act's electronic-content offences (including Sections 67, 67A and 67B), while also engaging reporting duties and institutional pathways (POCSO Sections 19 and 21; national cybercrime reporting mechanisms). This study therefore situates grooming within Indian statutory design, platform responsibility, and reporting pathways rather than treating it as an isolated incident, and evaluates how these instruments operate in practice against rapidly evolving platform features.[4]

1.2 Meaning, Nature and Emerging Forms of Online Grooming

Online grooming, in the present context, refers to a patterned course of conduct in which an adult (or older adolescent) uses digital communication to cultivate a relationship with a child for sexual exploitation, including inducing sexualised talk, seeking sexual images/videos, arranging meetings, or leveraging coercion and threats. Indian law captures core grooming outcomes through offence categories and duties: sexually motivated communications and conduct can fall within POCSO's sexual harassment of a child (Section 11) punished under Section 12, while grooming that involves showing or eliciting sexual content, or using a child in any form of media for sexual gratification, engages POCSO's pornography-related provisions (Sections 13–15). Where grooming results in creation, transmission, browsing, advertisement, or facilitation of child sexual

[4] Maya Indira Ganesh, "Negotiating intimacy and harm: female internet users in Mumbai, India," 2015 *available at*: https://www.academia.edu/12698142/Negotiating_intimacy_and_harm_female_internet_users_in_Mumbai_India (last visited April 28, 2026).

abuse material in electronic form, the IT Act's Section 67B becomes central, supplemented by Sections 67 and 67A for obscene/sexually explicit electronic content. The "emerging forms" include grooming through voice chat and livestreaming, micro-transactions and gifting to build dependency, migration from public chats to encrypted/private channels, and sextortion through threats to circulate images—each raising questions of attribution, evidence preservation, and cross-platform continuity.

1.3 Growth of Gaming and Social Media Platforms as Spaces of Child Vulnerability

Gaming and social media ecosystems increasingly function as child social environments, not merely entertainment spaces, and their design features can unintentionally support grooming: frictionless discovery (friends-of-friends, "nearby/you may know," guilds/clans), persistent identity profiles, direct messaging, voice rooms, and mixed-age communities. This raises a governance question: how far platform operators and intermediaries must act to prevent hosting/transmitting unlawful sexual content involving children and to provide effective user safeguards. In India, intermediary due diligence obligations under the IT Rules, 2021 (made under the IT Act) require intermediaries to inform users not to host or share prohibited content and to act through grievance and takedown processes; additional obligations apply to significant social media intermediaries, including proactive measures to identify content depicting child sexual abuse (as reflected in the Rules' text and Government explanations). These regulatory duties interface with substantive criminal provisions (IT Act Sections 67, 67A, 67B; POCSO Sections 11–15) because grooming often uses platform architecture to transition from communication to sexual content production/dissemination.[5]

Child vulnerability is also shaped by social and criminological factors: unsupervised screen time, aspirational online identities, peer pressure, and the normalisation of "stranger interaction" in multiplayer settings, which can weaken risk perception. Reporting is complicated by fear of parental reaction, stigma, and threats by offenders, making accessible reporting channels and rapid action essential. India's national cybercrime reporting infrastructure explicitly includes reporting of online child sex abuse material/sexually explicit content, and recent government

[5] Dr. William Allchorn, "Beyond the Clan: Identity Formation, Influence, and Extremist Milieux in Online Gaming-Adjacent Spaces" *GNET*, 2026 *available at*: https://gnet-research.org/2026/04/17/beyond-the-clan-identity-formation-influence-and-extremist-milieux-in-online-gaming-adjacent-spaces/ (last visited April 28, 2026).

communications reiterate that POCSO and the IT Act/Rules together form the core framework against online sexual offences involving children—yet practical effectiveness depends on awareness, timely reporting, and platform responsiveness.[6]

1.4 Objectives of the Study

1. To analyse how online grooming via gaming and social media platforms is addressed under POCSO, 2012 (Sections 11–15, 19, 21) and the IT Act, 2000 (Sections 67, 67A, 67B).
2. To examine platform due-diligence obligations relevant to child safety under the IT Rules, 2021 and their operational significance.
3. To identify socio-criminological patterns of grooming (approach, trust-building, coercion, sextortion) in digital environments.
4. To assess challenges in reporting, investigation, and evidentiary handling in grooming-related offences involving electronic communication.

1.5 Research Questions

1. How do POCSO Sections 11–15, 19 and 21 apply to grooming behaviours that occur through gaming and social media communications?
2. How does the IT Act (Sections 67, 67A, 67B) address grooming outcomes involving sexual content and child sexual abuse material online?
3. What duties under the IT Rules, 2021 most directly affect prevention and response to grooming-related content and communications?
4. What socio-criminological factors increase child vulnerability on gaming and social media platforms in India?

1.6 Research Methodology

This study adopts a doctrinal research methodology based on primary legal sources and authoritative regulatory materials. It undertakes close textual analysis of the Protection of Children from Sexual Offences Act, 2012 (especially Sections 11–15, 19 and 21), the Information

[6] Michelle Slone, Ayelet Peer and Michael Egozi, "Adolescent Vulnerability to Internet Media Exposure: The Role of Self-Mastery in Mitigating Post-Traumatic Symptoms," 22 *International journal of environmental research and public health* 589 (2025).

Technology Act, 2000 (notably Sections 67, 67A and 67B), and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to evaluate how Indian law captures grooming processes and platform-facilitated exploitation. The method is supported by analysis of official governmental publications and statutory documents to assess coherence, scope, and enforceability, mapped against platform affordances and reported enforcement realities, without relying on case law.

2 DIGITAL ECOSYSTEMS, CHILD INTERACTION AND PATTERNS OF GROOMING

2.1 Architecture of Online Gaming Platforms and Social Media Interfaces

Online grooming in India is structurally enabled by platform architecture: multiplayer lobbies, guild/clan systems, matchmaking, "add friend" prompts, DMs, and voice channels reduce friction for adult–child contact and shift interactions from public spaces to private rooms. When this contact escalates into sexualised requests, inducement for images, or circulation of child sexual abuse material, legal engagement commonly arises under POCSO Act, 2012 (Sections 11–12 on sexual harassment; Sections 13–15 on pornographic use and related acts; Section 19 duty to report) and the Information Technology Act, 2000 (Sections 67, 67A, 67B). Platform governance is simultaneously implicated because intermediary obligations under the IT Rules, 2021 link user safety design and takedown systems to unlawful content control.[7]

2.2 Modes of Communication, Anonymity and Identity Manipulation

Grooming communications typically move through layered modes—public chat to private DM, then voice, then encrypted or ephemeral messaging—while offenders exploit anonymity, pseudonyms, multiple accounts, and age-masking to present a false "peer" identity. This pattern increases evidentiary complexity but does not reduce liability where the conduct amounts to sexual harassment or pornographic exploitation of a child under POCSO (Sections 11–15), or where electronic transmission/viewing/advertising of child sexual abuse material is involved under IT Act Section 67B (along with Sections 67 and 67A for obscene/sexually explicit electronic content).

[7] ASV law offices, "Protection of Children from Online Harm: Assessing Legal Measures under the IT Act and POCSO Act" *ASV Legal LLP*, 2026 *available at*: https://www.asvlawoffices.com/news-insights/protection-of-children-from-online-harm-assessing-legal-measures-under-the-it-act-and-pocso-act/ (last visited April 28, 2026).

The IT Rules, 2021 reinforce user-notice and due diligence duties that become crucial once grooming shifts into unlawful content exchange.[8]

2.3 Stages and Techniques Used in Online Grooming Practices

Grooming generally follows a staged process: (i) access and selection (targeting minors), (ii) rapport-building via compliments/gifts/in-game currency, (iii) boundary testing with sexualised jokes or dares, (iv) isolation to private channels, and (v) coercion through threats, doxxing, or sextortion. In Indian law, once "sexual intent" is evident and the conduct amounts to sexual harassment, POCSO Sections 11–12 become relevant; if the child is induced or used for pornographic purposes, POCSO Sections 13–15 apply; and when any CSAM is created, transmitted, browsed, or facilitated electronically, IT Act Section 67B is the central cyber-content offence. Mandatory reporting duties under POCSO Sections 19 and 21 frame institutional responsibility when parents, schools, or platforms receive information.

2.4 Vulnerability of Children and Adolescents in Interactive Digital Environments

Children's vulnerability in gaming/social ecosystems is intensified by developmental factors (risk-taking, need for belonging) and platform affordances (constant connectivity, parasocial bonds with streamers, "always-on" groups). Legally, "child" status is decisive: POCSO applies to persons below 18 (definition provisions in the Act), and the Bharatiya Nyaya Sanhita, 2023 also defines "child" as below eighteen years (Section 2(3)), supporting consistent age-based protection across substantive criminal law. Where grooming escalates into electronic sexual exploitation content, IT Act Sections 67/67A/67B and intermediary obligations under the IT Rules, 2021 shape prevention, reporting, and rapid response measures.

3 SOCIO-CRIMINOLOGICAL DIMENSIONS OF ONLINE GROOMING

3.1 Social Behaviour, Trust Formation and Emotional Targeting in Cyberspace

Online trust is engineered through repeated micro-interactions—team play, "confiding" chats, gifts, and validation—allowing offenders to cultivate emotional dependence and secrecy. This socio-criminological "trust capture" is legally relevant because it often precedes conduct

[8] Tracey Cockerton, "Cyber Criminology" *Advanced Sciences and Technologies for Security Applications* (2018).

criminalised as sexual harassment (POCSO Sections 11–12) or pornographic exploitation (POCSO Sections 13–15), and it frequently culminates in electronic CSAM offences (IT Act Section 67B). The constitutional backdrop—Article 21 (life and personal liberty) read with the State's protective duties for children—supports a child-safety oriented interpretation of regulatory action and institutional response in digital contexts.[9]

3.2 Psychological Manipulation, Coercion and Gradual Sexualisation

Psychological grooming typically involves desensitisation (sexual humour, "truth or dare"), reciprocity traps ("I shared, now you"), and coercive control (threats to leak images or harm reputation). In India, once sexualised conduct targets a minor, POCSO Sections 11–12 provide a direct route for criminalisation of sexual harassment, while POCSO Sections 13–15 address pornographic use and related acts; coercion that produces or circulates sexual content triggers IT Act Sections 67A and 67B. The IT Rules, 2021 strengthen platform duties to act against prohibited content and enable grievance mechanisms, which matters in sextortion cycles where speed of takedown is central to harm reduction.

3.3 Role of Peer Culture, Digital Dependency and Platform Immersion

Peer culture in gaming (rank pressure, clan loyalty, social status) can normalise risky interactions with unknown adults, while digital dependency increases children's exposure time and susceptibility to manipulation. This is not merely behavioural: it implicates prevention duties and child welfare systems, including coordinated action under POCSO's mandatory reporting (Sections 19 and 21) and child protection pathways under the Juvenile Justice (Care and Protection of Children) Act, 2015, which structures institutional care/support for children in need of care and protection. Regulatory emphasis on online reporting channels for child sexual abuse material also reflects the need to convert social barriers into actionable complaints.

3.4 Offender Profiles, Victim Patterns and Reporting Barriers

Offenders range from opportunistic "contact" abusers to organised networks trading CSAM;

[9] "POCSO Act, 2012 provides for safeguarding children against sexual offences, including online sexual abuse," *Press Information Bureau available at*: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2245026&reg=3&lang=1 (last visited April 28, 2026).

victims are often targeted for loneliness, secrecy, or high online engagement, and reporting is blocked by shame, fear of parental reaction, and threats of dissemination. India's substantive framework addresses these outcomes through POCSO Sections 11–15 and IT Act Section 67B (including viewing/downloading/advertising/facilitating CSAM), while cross-border and remote offending remains prosecutable where offences target a computer resource located in India, reflected in BNS extraterritorial application provisions (Section 1(5)(c)). The National Cyber Crime Reporting Portal provides a dedicated route for online CSAM/sexually explicit content complaints, operationalising the reporting imperative.[10]

4 LEGAL FRAMEWORK GOVERNING ONLINE GROOMING IN INDIA

4.1 Constitutional Protection of Children in the Digital Environment

Constitutional guarantees frame child safety online through enforceable rights and State obligations: Article 21 protects life and personal liberty (including dignity and safety), Article 21A supports the child's right to education (often impacted by online exploitation trauma), and Article 15(3) permits special provisions for children, justifying targeted child-protection laws and protective digital regulation. These principles support robust enforcement of child-focused statutes such as POCSO, 2012 (including Sections 11–15 and Sections 19/21 on reporting) and cyber-content controls under the IT Act, 2000 (Sections 67/67A/67B), especially where platforms create foreseeable risk environments for minors.

4.2 Statutory Regulation under Penal, Child Protection and Information Technology Laws

The core statutory structure is dual: POCSO criminalises sexually motivated conduct against children (Sections 11–12) and pornography-related exploitation (Sections 13–15), while the IT Act criminalises obscene and sexually explicit electronic publication/transmission (Sections 67 and 67A) and specifically targets child sexual abuse material (Section 67B). Where grooming includes threats, deception, or coercive tactics, general criminal law under the Bharatiya Nyaya Sanhita,

[10] "Reframing Child Protection Laws: Supreme Court Addresses Viewing of CESAM Under POCSO Act - Maheshwari and Co.," *Maheshwari & Co. available at*: https://www.maheshwariandco.com/press-release/reframing-child-protection-laws-supreme-court-addresses-viewing-of-cesam-under-pocso-act/ (last visited April 28, 2026).

2023 provides supplementary coverage for related offences while retaining the age-centric definition of "child" (Section 2(3)), ensuring that grooming is treated as both a child-protection and cyber-content harm rather than a mere "online misbehaviour."

4.3 Liability of Intermediaries, Platform Governance and Due Diligence Obligations

Platform responsibility in India is shaped by the IT Act's intermediary safe-harbour (Section 79) conditioned on due diligence, and by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which specify user-notice, grievance redressal, and content takedown workflows. For grooming-linked harms, these duties matter because the harm pathway often depends on platform features (DMs, groups, livestreams) and content persistence; timely disabling of access to CSAM-like content engages IT Act Section 67B risks, while systemic compliance failures can undermine safe-harbour conditions under Section 79.

Government directions for blocking in defined circumstances may also arise under IT Act Section 69A, particularly for public access control of unlawful content.[11]

4.4 Evidentiary Issues, Investigation Standards and Procedural Challenges

Online grooming prosecutions depend on electronic evidence integrity: chat logs, voice recordings, screenshots, device extractions, and platform metadata must meet admissibility requirements. Under the Bharatiya Sakshya Adhiniyam, 2023, electronic/digital records are recognised (Section 61), and special provisions govern proof and admissibility of electronic records (Sections 62–63), including certificate requirements for "computer output" evidence (Section 63(4)) and presumptions relating to electronic records and signatures (Sections 85–87). Procedurally, the Bharatiya Nagarik Suraksha Sanhita, 2023 recognises electronic-mode proceedings (including Section 530 on trial and proceedings in electronic mode), which can support child-friendly recording and faster processing when paired with POCSO's reporting and protective duties (Sections 19 and 21).

[11] "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021," *PRS Legislative Research available at*: https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 (last visited April 28, 2026).

5 ENFORCEMENT GAPS AND INSTITUTIONAL RESPONSE

5.1 Policing Online Grooming through Cyber Cells and Special Agencies Enforcement typically begins with complaint intake, preservation of digital evidence, device seizure/forensics, and requests to platforms for subscriber data and logs; capacity is uneven across regions, making specialised cyber cells and coordinated monitoring essential. For child sexual exploitation online, the national reporting infrastructure (National Cyber Crime Reporting Portal) provides a centralised entry point, particularly for reporting CSAM/sexually explicit content, complementing POCSO's duty-to-report regime (Sections 19 and 21). Once content-based offences are involved, IT Act Section 67B and intermediary compliance mechanisms under the IT Rules, 2021 become crucial for rapid takedown and prevention of further circulation.[12]

5.2 Challenges in Detection, Complaint Registration and Digital Evidence Collection

Grooming is hard to detect early because "non-criminal" contact precedes explicit illegality, and victims may delete chats under fear; additionally, cross-platform migration fragments evidence. Investigation must therefore prioritise immediate preservation (hashing, chain of custody, platform requests) so that electronic records satisfy Bharatiya Sakshya Adhiniyam requirements (Sections 61–63, especially Section 63 certificate expectations) and remain reliable against manipulation claims. Complaint registration must also reflect POCSO's mandatory reporting framework (Sections 19 and 21), while the cybercrime portal's CSAM-focused reporting pathways help convert online harm into actionable criminal procedure.

5.3 Role of Schools, Families, Child Welfare Authorities and Civil Society

Prevention and response require a multi-institution approach: parents and schools are often first to observe behavioural changes, while child welfare systems provide protective support and rehabilitation pathways. Legally, once knowledge of a sexual offence against a child arises, POCSO imposes a reporting duty (Section 19) and penalises failure to report (Section 21), making institutional "silence" a legal risk. Where the child needs protection/support services, the Juvenile Justice Act, 2015 provides the broader child welfare framework, and official child-safety toolkits

[12] "Digital Forensics and Investigation: From Data to Digital Evidence - DOKUMEN.PUB," *dokumen.pub available at*: https://dokumen.pub/digital-forensics-and-investigation-from-data-to-digital-evidence.html (last visited April 28, 2026).

and guidance by child protection bodies reinforce practical steps for cybercrime victim support alongside formal criminal reporting.[13]

5.4 Gaps in Coordination, Capacity Building and Victim-Centred Response Mechanisms

Key gaps include delayed platform data sharing, inconsistent forensic training, limited child-friendly interviewing capacity, and weak coordination between local police, cyber units, CWCs, and prosecutors. Victim-centred response depends on reducing secondary trauma and ensuring quick containment of harmful content—where IT Act Section 67B risks expand rapidly once CSAM is circulated, and IT Rules, 2021 due diligence and grievance systems become operationally significant. Procedural modernisation under the Bharatiya Nagarik Suraksha Sanhita, 2023 (including electronic-mode proceedings provisions such as Section 530) can support faster, less intimidating processes, but only if matched with adequate infrastructure and trained personnel.

5.5 Case Laws

In ***Shreya Singhal v. Union of India***[14] the Supreme Court struck down Section 66A, Information Technology Act, 2000 and read down Section 79 (intermediary safe harbour) by clarifying that "actual knowledge" for takedown is tied to lawful orders/authorised government directions, shaping how platforms respond to unlawful content and complaints relevant to grooming-linked harm. Article 19(1)(a) and Article 19(2), Constitution of India were central to this balancing, which remains relevant when restricting or removing child-sexual exploitation material online.

In ***Avnish Bajaj v. State (NCT of Delhi)***[15] Delhi High Court examined criminal process in relation to online obscene listings and discussed liability questions in the context of Section 67, IT Act, 2000 and parallel penal provisions (then Section 292, IPC), illustrating how "publication/transmission" issues arise for online platforms when unlawful sexual content is circulated. This reasoning is frequently cited in platform-facilitated exploitation discussions, alongside later developments under Section 79, IT Act and intermediary due diligence norms.

[13] Upasana Tyagi et al., "Knowledge and awareness of child sexual abuse related to POCSO (Protection of Children from Sexual Offences) Act among medical and dental professionals in India: A cross-sectional study," 13 *Journal of family medicine and primary care* 4880–4 (2024).
[14] Shreya Singhal v. Union of India, (2015) 5 SCC 1
[15] Avnish Bajaj v. State (NCT of Delhi), 116 (2005) DLT 427

In ***Anvar P.V. v. P.K. Basheer***[16] the Supreme Court held that electronic records must satisfy the statutory certificate requirement (then Section 65B, Indian Evidence Act, 1872) for admissibility of computer outputs, a principle crucial for grooming prosecutions built on chats, screenshots, call logs, and platform records. The decision anchors digital-evidence discipline for offences prosecuted under POCSO Act, 2012 and IT Act, 2000.

In ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal***[17] a three-judge bench reaffirmed and clarified the rule on Section 65B, Evidence Act (including when and how a certificate is required, and limited exceptions), directly affecting the proof of electronic communications in online grooming and CSAM-linked cases under Section 67B, IT Act, 2000 and relevant POCSO offences.

In ***In Re: Prajwala Letter dated 18.02.2015: Videos of Sexual Violence and Recommendations***[18] the Supreme Court dealt with systemic measures to curb circulation of rape/child sexual abuse content online, engaging the State and intermediaries on mechanisms for identification, reporting and blocking, a policy-judicial backdrop for enforcement of Sections 67/67A/67B, IT Act, 2000 and platform due diligence under subordinate rules.

In ***Nipun Saxena v. Union of India***,[19] the Court strengthened protections against disclosure of a sexual-offence victim's identity under Section 228A, IPC and clarified safeguards that apply with special force where the victim is a minor (including cases under POCSO, 2012), shaping media, police, and institutional handling of grooming-related complaints to prevent secondary victimisation.

In ***Justice K.S. Puttaswamy (Retd.) v. Union of India***[20] the nine-judge bench affirmed privacy as a fundamental right under Article 21 (and linked facets under Articles 14 and 19), recognising informational privacy threats from both State and non-State actors—an essential constitutional lens when designing child-safety interventions, platform governance, and proportionate restrictions to prevent online grooming and CSAM circulation.

In ***Sabu Mathew George v. Union of India***[21] the Supreme Court issued directions to search engines to curb illegal advertisements under the PCPNDT law and discussed intermediary

[16] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
[17] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1
[18] In Re: Prajwala Letter dated 18.02.2015: Videos of Sexual Violence and Recommendations, Suo Motu W.P. (Crl.) No. 3/2015
[19] Nipun Saxena v. Union of India, (2019) 2 SCC 703 (SC),
[20] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[21] Sabu Mathew George v. Union of India, (2017) SCC OnLine SC 1269

responsibilities, offering an important governance template for proactive/technical compliance models that inform contemporary expectations of platform action against illegal child-sexual exploitation content under IT Act, 2000 (notably Sections 69A and 79) and associated rules.

6 COMPARATIVE REGULATORY APPROACHES AND INTERNATIONAL STANDARDS

6.1 International Norms on Child Safety in Digital Communication Spaces

International child-protection standards treat grooming and online sexual exploitation as State obligations: the UN Convention on the Rights of the Child mandates protection from sexual exploitation and abuse (including Articles 19 and 34), and the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography requires criminalisation of child pornography-related harms. These norms align with India's domestic scheme under POCSO (Sections 11–15) and IT Act Section 67B, supporting the argument that grooming is not a marginal cyber issue but a core child-rights protection duty that should shape platform governance and enforcement priorities.

6.2 Regulatory Approaches to Platform Accountability and Child Protection

Comparative regimes increasingly impose "systems-based" duties on platforms to assess and mitigate risks to minors, rather than relying only on post-harm takedowns. The Council of Europe's Lanzarote Convention framework explicitly treats online solicitation of children for sexual purposes (grooming) as conduct requiring criminalisation (Article 23), reflecting a direct grooming-specific approach. India's model is more "combined" (POCSO + IT Act + IT Rules), where intermediary obligations (IT Act Section 79 and IT Rules, 2021) create compliance-based accountability even without a single stand-alone grooming offence label, thereby positioning platform due diligence as a central prevention lever.[22]

6.3 Age Verification, Content Moderation and Safety-by-Design Measures

Global regulatory thinking increasingly pushes safety-by-design: age-appropriate design, default

[22] "Government's measures to ensure safe and accountable internet," *available at*: https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2201456 (last visited April 28, 2026).

privacy, restricted DMs for minors, friction for adult–minor contact, and stronger detection/takedown for CSAM. In India, the legal "trigger" remains child status (POCSO applicability; BNS definition of child in Section 2(3)) and unlawful electronic sexual content (IT Act Sections 67A and 67B), while the IT Rules, 2021 provide the compliance channel to operationalise safeguards via user-notice, reporting, and due diligence systems. Comparative guidance, such as EU child-safety guidelines under the Digital Services Act ecosystem, illustrates how risk mitigation can be formalised as ongoing platform obligations rather than episodic enforcement.

6.4 Lessons for Strengthening the Indian Legal and Enforcement Framework

India can strengthen grooming control by (i) clearer statutory recognition of grooming-pattern conduct within child-protection enforcement practice, (ii) faster platform-preservation and takedown pipelines under IT Act Sections 67B/69A and IT Rules due diligence, and (iii) stronger evidence readiness under Bharatiya Sakshya Adhiniyam Sections 61–63 (including robust certification and hashing practices.[23]

7 CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

Online grooming via gaming and social media platforms in India should be understood as a process-based pathway to child sexual exploitation, where platform design enables access and secrecy, and social dynamics enable trust capture and coercion. India's response is legally substantial but operationally uneven: POCSO (Sections 11–15; Sections 19/21), the IT Act (Sections 67, 67A, 67B; intermediary safe-harbour in Section 79), and the IT Rules, 2021 provide the substantive and regulatory spine, while admissibility and procedure depend on Bharatiya Sakshya Adhiniyam Sections 61–63 and Bharatiya Nagarik Suraksha Sanhita provisions for modernised proceedings. The central challenge is converting these norms into rapid reporting, credible evidence, and victim-centred enforcement.

[23] "Addressing the Gaps in India's Child Protection Laws: Safeguarding Children from Online 'Grooming,'" *The Journal of Indian Law and Society*, 2022 *available at*: https://jilsblognujs.wordpress.com/2022/06/21/addressing-the-gaps-in-indias-child-protection-laws-safeguarding-children-from-online-grooming/ (last visited April 28, 2026).

7.2 Recommendations

A legally grounded strategy should combine prevention, accountability, and child-centred justice: mandate school-level and community awareness that aligns with POCSO reporting duties (Sections 19 and 21); strengthen cyber-police SOPs for immediate electronic evidence capture consistent with Bharatiya Sakshya Adhiniyam Section 63 certification requirements; require platforms to implement safety-by-design measures for minors through stricter enforcement of intermediary due diligence under IT Rules, 2021 and conditional safe-harbour under IT Act Section 79; and expand rapid CSAM containment using IT Act Section 67B enforcement, coordinated with national reporting channels. Finally, integrate child welfare support under the Juvenile Justice Act, 2015 to ensure counselling, protection, and rehabilitation, so the legal response addresses both criminal accountability and long-term child recovery.

BIBLIOGRAPHY

Statutes

1. The Constitution of India, 1950
2. The Protection of Children from Sexual Offences Act, 2012
3. The Information Technology Act, 2000
4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
5. The Juvenile Justice (Care and Protection of Children) Act, 2015
6. The Bharatiya Nyaya Sanhita, 2023
7. The Bharatiya Nagarik Suraksha Sanhita, 2023
8. The Bharatiya Sakshya Adhiniyam, 2023
9. The Digital Personal Data Protection Act, 2023

Books

10. Pavan Duggal, *Cyberlaw – The Indian Perspective* (Saakshar Law Publications, New Delhi, 2002). https://cyberlawuniversity.com/product/cyberlaw-the-indian-perspective/
11. Pavan Duggal, *Judicial and Practical Approaches to Electronic Evidence Law in India* (Cyberlaw University, New Delhi, 2015). https://cyberlawuniversity.com/product/judicial-and-practical-approaches-to-electronic-

evidence-law-in-india/

12. Ganguly, *Commentary on The Protection of Children from Sexual Offences Act, 2012 (POCSO)* (Sweet and Soft Publications, 5th edn., 2025). https://www.ebcwebstore.com/product/commentary-on-the-protection-of-children-from-sexual-offences-act-2012-pocso-ganguly
13. Ratanlal & Dhirajlal, *The Indian Penal Code* (LexisNexis, 36th edn., 2020). https://www.flipkart.com/indian-penal-code-ratanlal-dhirajlal/p/itmaea3879e0905f
14. Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell & Adrian Scott, *Image-based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery* (Routledge, Abingdon (Oxon), 2021). https://research.monash.edu/en/publications/image-based-sexual-abuse-a-study-on-the-causes-and-consequences-o/

Journal

15. Daniel Manoj, Ranjit Immanuel James, Senthil Kumaran, Gerard Pradeep Devnath, Benjy Tom Varughese, Antony L. Arakkal & Latif Rajesh Johnson, "Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation" 4 *Child Protection and Practice* 100088 (2025). https://doi.org/10.1016/j.chipro.2024.100088
16. Poonam Mishra & Dr. Roshni Srivastava, "Digital Sexual Exploitation of Children: Analysing POCSO Provisions on Pornography and Online Abuse in India" 6(4) *Indian Journal of Legal Review* 324–332 (2024). https://ijlr.iledu.in/v6i434/
17. Nayana Teron, "Protecting Our Innocence: Addressing Child Pornography in India" 13(1) *Institutionalised Children: Explorations and Beyond* 80–88 (2026). https://journals.sagepub.com/doi/10.1177/23493003241274014
18. Gurmeet Kaur, "Internet Crimes Against Minors and Legal Framework in India" 68(4) *Indian Journal of Public Administration* 705–718 (2022). https://doi.org/10.1177/00195561221091381
19. Subham Krishna Borah, Sheila Ramaswamy & Shekhar Seshadri, "The Online Specter: Artificial Intelligence and Its Risks for Child Sexual Abuse and Exploitation" 21(2) *Journal of Indian Association for Child and Adolescent Mental Health* 107–112 (2025).

https://doi.org/10.1177/09731342251334293

20. Lina Acca Mathew, "Online Child Safety from Sexual Abuse in India" 2009(1) *Journal of Information, Law & Technology* 1–23(2009). http://go.warwick.ac.uk/jilt/2009_1/mathew
21. Aanchal Kabra & Rohit Gupta, "Carving an Indian Mosaic for Image-Based Sexual Abuse" 34(1) *National Law School of India Review* 205–245 (2022). https://repository.nls.ac.in/nlsir/vol34/iss1/10/
22. Ian A. Elliott & Anthony R. Beech, "Understanding Online Child Pornography Use: Applying Sexual Offense Theory to Internet Offenders" 14(3) *Aggression and Violent Behavior* 180–193 (2009). https://doi.org/10.1016/j.avb.2009.03.002
23. Daniel Middleton, Rachael Mandeville-Norden & Elizabeth Hayes, "Does Treatment Work with Internet Sex Offenders? Emerging Findings from the Internet Sex Offender Treatment Programme (i-SOTP)" 15(1) *Journal of Sexual Aggression* 5–19 (2009). https://doi.org/10.1080/13552600802673444
24. Helen Whittle, Catherine Hamilton-Giachritsis, Anthony Beech & Guy Collings, "A Review of Online Grooming: Characteristics and Concerns" 18(1) *Aggression and Violent Behavior* 62–70 (2013). https://doi.org/10.1016/j.avb.2012.09.003
25. Helen Whittle, Catherine Hamilton-Giachritsis, Anthony Beech & Guy Collings, "A Review of Young People's Vulnerabilities to Online Grooming" 18(1) *Aggression and Violent Behavior* 135–146 (2013). https://doi.org/10.1016/j.avb.2012.11.008
26. Samantha Craven, Sarah J. Brown & Elizabeth Gilchrist, "Sexual Grooming of Children: Review of Literature and Theoretical Considerations" 12(3) *Journal of Sexual Aggression* 287–299 (2006). https://doi.org/10.1080/13552600601069414