Page 3674 - 3691 **DOI:** *https://doij.org/10.10000/IJLMH.1111954*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Cyber Crime against Children in Online Gaming Platforms: Issues, Challenges and Role of the Indian Judiciary

KOTHAINAYAGI V[1] AND DR. V. KARTHIKEYAN[2]

ABSTRACT

The proliferation of online gaming platforms in India has precipitated a consequential and largely underexamined dimension of cybercrime, namely, the systematic targeting of children through digital gaming ecosystems. This article examines the multifaceted issues and challenges that arise from cybercrime directed at minors within online gaming environments, drawing upon a detailed legal and empirical analysis of the phenomenon in the Indian context. Specifically, the article explores six principal categories of harm — online grooming and exploitation, cyberbullying and harassment, financial fraud and identity theft, privacy and data protection violations, exposure to harmful content, and gaming addiction — before proceeding to analyse the role, limitations, and reform imperatives of the Indian judiciary in addressing these concerns. The article further engages with landmark judicial pronouncements, including Justice K.S. Puttaswamy (Retd.) v. Union of India, Shreya Singhal v. Union of India, and Just Rights for Children Alliance v. S. Harish, to evaluate the evolving contours of cyber jurisprudence in India. Drawing upon a comparative analysis of regulatory models adopted by the United Kingdom and the United States, the article argues that the Indian legal framework, though foundational, remains insufficiently tailored to the dynamic risks presented by gaming technology. The article concludes with a set of normative recommendations directed at legislative reform, judicial specialisation, platform accountability, and child-centric digital governance.

Keywords: *Cybercrime; Children; Online Gaming; POCSO Act; Information Technology Act; Judicial Intervention; Data Protection; Digital Personal Data Protection Act 2023; Cyber Jurisprudence; Platform Accountability.*

I. INTRODUCTION

The intersection of technology and childhood has, in recent decades, engendered a landscape that is simultaneously enriching and fraught with peril. Online gaming platforms, once confined

[1] Author is an LL.M. Student at Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu, India.
[2] Author is an Assistant Professor at Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu, India.

 [ISSN 2581-5369]

to the realm of solitary or locally networked entertainment, have metamorphosed into sprawling interactive ecosystems that integrate real-time communication, social identity formation, virtual economies, and immersive digital experiences. Platforms such as Battlegrounds Mobile India, Garena Free Fire, and a host of other massively multiplayer online games have achieved extraordinary penetration within the Indian juvenile demographic, with children constituting a disproportionately large share of the user base. Notwithstanding the cognitive and recreational benefits that moderate gaming engagement may confer, the largely unregulated architecture of these platforms has created fertile ground for the commission of serious cyber offences targeting minors.

The Commission of offences against children in digital gaming environments is not a peripheral or speculative concern; it is substantiated by a disturbing corpus of documented incidents spanning the years 2019 to 2025, wherein minors across India have suffered grievous harm ranging from financial exploitation and psychological trauma to physical violence and suicide. What renders these offences particularly pernicious is the structural architecture of gaming platforms themselves — features such as anonymous user interaction, real-time voice and text communication, avatar-based identity concealment, and integrated micro-transaction systems collectively create an environment in which offenders may operate with a degree of impunity that traditional social and legal safeguards have proven manifestly inadequate to address.

The Indian legal framework, comprising principally the Information Technology Act, 2000 (hereinafter 'IT Act'), the Protection of Children from Sexual Offences Act, 2012 (hereinafter 'POCSO Act'), the Bharatiya Nyaya Sanhita, 2023 (hereinafter 'BNS'), and the Digital Personal Data Protection Act, 2023 (hereinafter 'DPDPA'), provides a foundational structure for addressing cybercrime and protecting children in digital environments. However, as this article shall demonstrate, these statutory instruments were not conceived with the specific architecture and risk topology of online gaming in mind. The consequent legislative lacunae, compounded by institutional and evidentiary challenges, have severely circumscribed the efficacy of legal intervention in this domain.[3][4][5][6]

This article proceeds in the following manner. Part II examines the specific issues and challenges of cybercrime against children in gaming platforms, encompassing online grooming, cyberbullying, financial fraud, data protection violations, exposure to harmful content, gaming

[3] Information Technology Act, 2000 (India) [hereinafter IT Act].
[4] Protection of Children from Sexual Offences Act, 2012 (India) [hereinafter POCSO Act].
[5] Bharatiya Nyaya Sanhita, 2023 (India) [hereinafter BNS].
[6] Digital Personal Data Protection Act, 2023 (India) [hereinafter DPDPA].

 [ISSN 2581-5369]

addiction, and the deficit of parental awareness. Part III analyses the role of the Indian judiciary in interpreting and enforcing cyber laws as they pertain to children, with particular reference to landmark judicial pronouncements. Part IV critically evaluates the challenges confronting the judiciary in regulating gaming-related cybercrime and argues for a comprehensive programme of judicial and legislative reform. Part V draws upon a comparative analysis of foreign jurisdictions to identify best practices and normative insights applicable to the Indian context. Part VI concludes the article with consolidated recommendations.

II. Issues and Challenges of Cybercrime Against Children in Online Gaming Platforms

A. Online Grooming and Sexual Exploitation

Online grooming constitutes one of the gravest cyber threats confronting children in digital gaming environments. The term denotes the deliberate and systematic process through which an offender cultivates an emotional rapport with a minor, exploiting the communicative features of digital platforms to establish trust prior to initiating exploitation or abuse. Gaming platforms, by their very structural design, are particularly amenable to grooming behaviour. The incorporation of live chat, voice communication channels, and multiplayer collaboration features furnishes predatory actors with an unmediated avenue of access to vulnerable users. Unlike social media platforms — which have attracted comparatively greater regulatory and parental scrutiny — gaming environments are frequently perceived as recreational spaces, thereby reducing the vigilance of children, guardians, and policymakers alike.[7]

The anonymity endemic to gaming platforms substantially amplifies the risk of grooming. Offenders routinely conceal their true identities, fabricating alternative personas — frequently presenting themselves as peers of the targeted child — thereby circumventing the child's innate caution. The absence of robust identity verification mechanisms on most gaming platforms compounds this vulnerability. The grooming process is characterised by its gradualism and deception: offenders typically refrain from disclosing exploitative intentions at the outset, instead engaging in prolonged communication designed to engender emotional dependency. This process may involve the conferral of in-game rewards, expressions of empathy, or the gradual extraction of sensitive personal information.

A particularly instructive illustration of this phenomenon is the Lucknow 'Advanced Stage' Online Gaming Fraud Case (2024), in which a minor was approached through a gaming

[7] Sonia Livingstone, Children and the Internet: Great Expectations, Challenging Realities 112 (Polity Press 2009).

 [ISSN 2581-5369]

platform by an unidentified individual who offered to unlock advanced game levels and provide in-game rewards. Having systematically built the child's trust, the offender induced the victim to access parental banking credentials, resulting in the transfer of approximately ₹5 lakh. From a jurisprudential standpoint, such conduct squarely engages the provisions of Section 66D of the IT Act, which criminalises cheating by personation using computer resources, as well as the cognate provision formerly under Section 420 of the Indian Penal Code, 1860 — now substantially replicated in the BNS — relating to cheating and dishonest inducement. Crucially, this case illustrates that online grooming in gaming environments is not confined to the sexual domain; it also extends to financial manipulation, underscoring the breadth of harm that the legal framework must be equipped to address.[89]

B. Cyberbullying and Online Harassment

Cyberbullying within gaming environments represents a distinctive and particularly virulent manifestation of online harassment, differing from its physical counterpart in critical respects: it operates continuously across temporal and spatial boundaries, it is often amplified by the communal dynamics of gaming ecosystems, and it is rendered far more difficult to detect and prosecute by virtue of the pseudonymous nature of user interaction. Children who participate in competitive multiplayer games are frequently exposed to abusive communication, targeted intimidation, deliberate exclusion from gameplay, and coordinated verbal assaults. The competitive and hierarchical culture pervasive in certain gaming communities further normalises such conduct, creating an environment in which victims may be dissuaded from reporting incidents out of concern that their grievances will be dismissed as ordinary facets of gaming culture.

The persistent nature of cyberbullying in gaming contexts inflicts significant psychological damage on child victims. Empirical research consistently demonstrates an association between sustained cyberbullying victimisation and adverse mental health outcomes, including clinical anxiety, depressive symptomatology, diminished self-esteem, and in extreme cases, suicidal ideation. The Pune 'Log Out' Suicide Case (2024) offers a tragically concrete illustration of this nexus. In that case, a fifteen-year-old boy died by suicide following a prolonged period of engagement with online gaming platforms, during which he experienced escalating emotional isolation and psychological distress. The posthumous note, bearing only the words 'log out,' has been widely interpreted as a symbolic articulation of terminal digital withdrawal — a haunting

[8] Lucknow 'Advanced Stage' Online Gaming Fraud Case (2024); IT Act § 66D (criminalising cheating by personation using computer resources).
[9] BNS § 318 (cheating and dishonest inducement), substantially replicating Indian Penal Code, 1860 § 420.

 [ISSN 2581-5369]

testament to the psychological devastation that toxic gaming environments may precipitate in vulnerable adolescents.[1011]

The existing statutory framework offers partial but inadequate remedies for cyberbullying. Section 354D of the Indian Penal Code (now replicated in the BNS), which criminalises cyberstalking, and provisions addressing criminal intimidation and harassment, provide avenues for legal recourse. However, the enforcement challenges associated with identifying anonymous perpetrators in gaming environments, securing and authenticating digital evidence, and navigating the jurisdictional complexities that arise when offenders and victims are located in different states or countries, severely constrain the practical utility of these provisions. There is, accordingly, an urgent legislative imperative to enact dedicated cyberbullying legislation that is specifically calibrated to the interactive architecture of gaming platforms.[12]

C. Financial Fraud and Identity Theft

The integration of sophisticated virtual economies within contemporary gaming platforms has precipitated a new and rapidly expanding category of cybercrime: the financial exploitation of children. Modern gaming applications routinely incorporate mechanisms for in-game purchases, virtual currency acquisition, and the buying and selling of digital assets — mechanisms that, while ostensibly innocuous in design, expose children to significant financial risks. Children, owing to their cognitive developmental stage and limited understanding of financial security principles, constitute uniquely susceptible targets for phishing attacks, fraudulent in-game transactions, and schemes designed to procure parental financial credentials under the pretence of gaming-related rewards.[13]

The quantum of financial harm documented in reported cases is considerable and warrants serious legislative attention. In the Hyderabad Financial Fraud Case (2023), a sixteen-year-old transferred approximately ₹36 lakh from his mother's bank account — an amount comprising the family's life savings and accumulated benefits — for the purpose of acquiring virtual gaming items in Garena Free Fire. Similar incidents have been documented across multiple Indian states, with minors transferring amounts ranging from ₹28,000 to over ₹14 lakh from parental accounts, frequently in response to manipulation by online actors posing as gaming service

[10] Sameer Hinduja & Justin W. Patchin, Cyberbullying: Identification, Prevention, and Response, 41 J. Sch. Violence 1, 4–6 (2010).
[11] Pune 'Log Out' Suicide Case (2024) (unreported); see also UNICEF Office of Research, Protecting Children in Online Gaming 18 (2025).
[12] IT Act § 66C; BNS § 77 (criminalising cyberstalking, replicating Indian Penal Code, 1860 § 354D).
[13] Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction 203–07 (Routledge 2018).

 [ISSN 2581-5369]

providers. The Enforcement Directorate's action in Enforcement Directorate v. Coda Payments India Pvt. Ltd. (2022), in which assets worth ₹68.53 crore linked to alleged unauthorised gaming transactions involving minors were frozen, further underscores the systemic dimension of this problem.[14][15]

From a statutory perspective, such conduct is actionable under Sections 66C and 66D of the IT Act, which criminalise identity theft and cheating by personation using computer resources, respectively. The cognate provisions of the BNS addressing cheating and dishonest inducement are equally applicable. However, the transnational dimension of many such frauds — wherein the perpetrators operate from jurisdictions beyond the territorial reach of Indian enforcement agencies — and the evidentiary challenges inherent in attributing liability in digital transactions, substantially impede effective prosecution. The absence of comprehensive authentication requirements and robust parental consent mechanisms on gaming platforms further exacerbates these vulnerabilities.[16]

D. Privacy Violations and Data Protection Concerns

The collection, processing, and potential misuse of children's personal data by gaming platforms constitutes a domain of profound and growing legal concern. Contemporary gaming applications harvest vast volumes of user-generated data — encompassing personal identifying information, behavioural patterns, geolocation data, communication records, and financial transaction histories — ostensibly for the purposes of platform optimisation and personalised user experience. However, the manner in which such data is stored, shared with third-party commercial entities, and protected against unauthorised access frequently fails to satisfy even minimal standards of transparency and security, let alone the heightened protections that the vulnerability of child users demands.[17]

The constitutional foundation for privacy protection in digital environments was definitively established by the nine-judge bench of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, wherein the Court unanimously held that the right to privacy, including informational privacy, constitutes an inalienable component of the right to life and personal liberty guaranteed under Article 21 of the Constitution. The court's

[14] Hyderabad Financial Fraud Case (2023) (unreported); see Nir Kshetri, Cybercrime and Cybersecurity in India, 44 Telecom Policy 101, 104 (2020).
[15] Enforcement Directorate v. Coda Payments India Pvt. Ltd. (2022) (Enforcement Case No. ECIR/DLZO/27/2022) (assets of ₹68.53 crore frozen).
[16] IT Act §§ 66C–66D; BNS § 318.
[17] Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1820 (2011); Daniel J. Solove, Understanding Privacy 101–04 (Harvard University Press 2008).

 [ISSN 2581-5369]

articulation of informational autonomy as a constitutionally protected interest carries direct implications for the manner in which gaming platforms process children's data. Notwithstanding this constitutional recognition, the practical implementation of robust data protection safeguards in the gaming sector has remained conspicuously inadequate.[18]

The Digital Personal Data Protection Act, 2023 represents a significant statutory response to this deficit. The Act imposes obligations upon data fiduciaries — a category that encompasses gaming platforms — to process personal data lawfully and transparently, and mandates the obtaining of verifiable parental consent before processing the data of child users. Violations are actionable under Section 43 of the IT Act, which addresses unauthorised access and data extraction, and Section 66C, which criminalises identity theft. Nevertheless, enforcement gaps persist, particularly in relation to cross-border data flows involving multinational gaming companies, and the technological pace of the industry continues to outrun the adaptive capacity of the regulatory framework.[19]

E. Exposure to Inappropriate Content and Gaming Addiction

Beyond the categories of harm discussed above, children in gaming environments are systematically exposed to two interrelated forms of risk that have attracted increasing concern among child protection advocates and legal scholars: first, exposure to age-inappropriate, violent, sexually suggestive, or otherwise harmful content; and second, the phenomenon of gaming addiction, clinically classified as Internet Gaming Disorder in the Diagnostic and Statistical Manual of Mental Disorders (DSM-5). These two dimensions of harm are frequently mutually reinforcing, insofar as the immersive and deliberately engineered engagement mechanisms of gaming platforms may simultaneously expose children to harmful content and foster patterns of compulsive usage that impair academic functioning, interpersonal relationships, and psychological well-being.[20]

The consequences of gaming addiction in the Indian context have been documented with alarming specificity. In the Lucknow Matricide Case (2022), a sixteen-year-old allegedly shot his mother with a licenced firearm following a series of disputes over restrictions imposed on his online gaming activities. The minor reportedly concealed the body for several days while continuing his normal routine — a pattern of behaviour that raises profound concerns about the

[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter Puttaswamy].
[19] DPDPA §§ 8–9 (obligations of data fiduciaries; verifiable parental consent for processing data of children); IT Act §§ 43, 66C.
[20] American Psychiatric Association, Diagnostic and Statistical Manual of Mental Disorders 795–98 (5th ed. 2013) (Internet Gaming Disorder); Daria J. Kuss & Mark D. Griffiths, Internet Gaming Addiction: A Systematic Review, 10 Int'l J. Mental Health & Addiction 278, 283 (2012).

degree of emotional desensitisation and detachment from moral reality that excessive immersion in violent gaming environments may precipitate. In the Bhiwandi Fratricide Case (2019), a fifteen-year-old allegedly killed his elder sibling over a dispute regarding mobile gaming access. These incidents, while they cannot be attributed solely to gaming, compellingly illustrate the manner in which unregulated digital dependency may serve as a situational catalyst in cases involving psychologically vulnerable minors.[2122]

From a constitutional perspective, the Supreme Court's pronouncements in Justice K.S. Puttaswamy (Retd.) v. Union of India firmly establish that the right to life under Article 21 encompasses the right to live with dignity and mental well-being. The psychological harms associated with gaming addiction — including anxiety, clinical depression, sleep disturbances, and social withdrawal — implicate this constitutional guarantee in a manner that calls for proactive legislative and regulatory intervention. The IT Act and POCSO Act provide partial remedies for specific categories of harmful content dissemination but offer no comprehensive framework for addressing the structural design features of gaming platforms that facilitate addiction and content-related harm.[23]

F. Enforcement Challenges and the Deficit of Parental Awareness

The effective enforcement of child protection laws in online gaming environments is beset by a convergence of legal, technological, and institutional challenges that collectively diminish the protective capacity of the existing framework. The anonymity afforded by gaming platforms renders the identification of perpetrators exceedingly difficult, requiring sophisticated digital forensic investigation involving the tracing of IP addresses, the analysis of digital footprints, and coordinated engagement with domestic and international service providers. The transient and mutable nature of digital evidence — including real-time chat logs, voice communications, and transaction records — further complicates the processes of evidence preservation and authentication that are prerequisites for admissibility under Section 65B of the Indian Evidence Act.[24]

The transnational character of gaming platforms introduces additional layers of jurisdictional complexity. Where perpetrators are located in foreign jurisdictions, the efficacy of domestic

[21] Lucknow Matricide Case (2022) (unreported); OECD, Children in the Digital Environment: Revised Typology of Risks 34 (2021).
[22] Bhiwandi Fratricide Case (2019) (unreported); see Galen Lamphere-Englund, Protecting Children in Online Gaming: Mitigating Risks from Organised Violence 12 (UNICEF Working Paper 2025).
[23] Puttaswamy, (2017) 10 SCC 1, ¶¶ 309–15; Constitution of India art. 21.
[24] Indian Evidence Act, 1872 § 65B; see also Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, 488 (India) [hereinafter Anvar P.V.].

 [ISSN 2581-5369]

enforcement is contingent upon international mutual legal assistance arrangements that are often slow, procedurally onerous, and insufficiently calibrated to the real-time urgency of cybercrime investigations. Compounding these structural challenges is the pervasive underreporting of gaming-related cybercrime, attributable both to children's limited awareness of the legal remedies available to them and to the social and emotional barriers — including fear of parental censure and embarrassment — that discourage victims from making disclosures to authorities.[25]

The deficit of parental awareness constitutes a critical structural vulnerability in the child protection architecture. Many parents and guardians, possessing limited familiarity with the interactive features of contemporary gaming platforms, fail to appreciate the scope of risks to which their children are exposed. The technological sophistication of modern gaming ecosystems — incorporating real-time global communication, microtransaction systems, and immersive social interaction — substantially exceeds the digital literacy of the majority of Indian parents, creating a supervision gap that predatory actors are well-positioned to exploit. Bridging this gap requires not merely legislative reform, but sustained investment in public digital literacy education and the development of accessible, user-friendly parental control technologies.[26]

III. THE ROLE OF THE INDIAN JUDICIARY IN ADDRESSING GAMING-RELATED CYBERCRIME

A. Evolution of Judicial Approach to Cybercrime Against Children

The trajectory of judicial engagement with cybercrime in India has traversed a considerable distance from its early, statute-centric and predominantly reactive posture to an increasingly rights-oriented and constitutionally informed jurisprudence. In the formative period of cyber law adjudication, courts addressed digital offences largely by transposing general criminal law principles onto novel factual matrices, without developing a specialised understanding of the technological architecture or operational dynamics of digital platforms. The concept of gaming environments as distinct and uniquely risky social spaces for children was conspicuously absent from judicial consciousness during this phase, notwithstanding the rapid growth of online gaming's juvenile user base.

[25] Jonathan Clough, Principles of Cybercrime 401–08 (2d ed., Cambridge University Press 2015); Susan W. Brenner, Cybercrime and the Law: Challenges, Issues and Outcomes 198–202 (Northeastern University Press 2012).

[26] Livingstone, supra note 5, at 78–82; Aparna Viswanathan, Cyber Law Reforms in India, 8 NUJS L. Rev. 221, 229 (2015).

 [ISSN 2581-5369]

A transformative inflection point in Indian cyber jurisprudence was the Supreme Court's watershed decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), which established the constitutional right to privacy as a component of Article 21 and provided, for the first time, a principled constitutional foundation for data protection and informational autonomy. This ruling carries substantial implications for the regulation of gaming platforms that engage in the pervasive collection and commercial exploitation of children's personal data, even though the Court did not directly address the gaming context. Equally significant, but from a different direction, was Shreya Singhal v. Union of India, (2015) 5 SCC 1, in which the Supreme Court struck down Section 66A of the IT Act on grounds of constitutional overbreadth and violation of the right to freedom of speech and expression. While this decision reinforced important constitutional freedoms, it simultaneously constrained the breadth of available regulatory tools for addressing harmful digital communication — a tension that remains unresolved in the context of gaming-related harassment and exploitation.[27][28]

B. Landmark Judicial Pronouncements and Their Implications for Gaming Environments

Several judicial pronouncements have shaped the contours of child protection law as it applies, whether directly or by extension, to gaming environments. In Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, the Supreme Court clarified the procedural requirements for the admissibility of electronic records, holding that such records must satisfy the certification requirements of Section 65B of the Indian Evidence Act to be admissible in criminal proceedings. This ruling has significant practical implications for the prosecution of cybercrime arising from gaming platforms, where the primary evidence invariably consists of electronic records — chat logs, transaction histories, and access records — that must be carefully preserved and authenticated to withstand judicial scrutiny.[29]

A directly germane judicial intervention is Sneha Kalita v. Union of India (2017), in which the Supreme Court responded to the dangers posed by the 'Blue Whale Challenge' — an online phenomenon characterised by structured self-harm tasks directed at adolescent users — by directing governmental authorities to take immediate measures to block the relevant platforms and to implement protective measures for children. While the conduct addressed in that case shares structural parallels with the manipulative mechanics of certain gaming environments, the

[27] Puttaswamy, (2017) 10 SCC 1, ¶¶ 179–81 (right to informational autonomy as component of Art. 21).
[28] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India) (striking down IT Act § 66A for constitutional overbreadth).
[29] Anvar P.V., (2014) 10 SCC 473, 486–89 (certification requirements under Indian Evidence Act § 65B for admissibility of electronic records).

 [ISSN 2581-5369]

judicial response was largely reactive and focused on content suppression rather than the articulation of broader regulatory principles. The ruling is nonetheless significant as an early acknowledgment of the judiciary's willingness to intervene proactively where digital platforms pose demonstrable risks to child welfare.[30]

Particularly consequential for the architecture of child protection law in digital contexts is the Supreme Court's recent decision in Just Rights for Children Alliance v. S. Harish, (2024) INSC 716. In this case, the Court adopted a purposive interpretive approach to hold that even the passive viewing, storing, and possession of child sexual exploitative and abuse material (CSEAM) constitutes a punishable offence under the POCSO Act and the IT Act. The Court's emphasis that passive consumption contributes to the perpetuation of exploitation significantly expands the scope of criminal liability in digital environments. In the context of gaming platforms, where CSEAM may circulate through private messaging functions, user-generated content channels, and concealed communication mechanisms embedded within games, this ruling furnishes a potent legal instrument for prosecuting a hitherto undertreated category of online child abuse.[31]

At the High Court level, Play Games 24x7 Private Limited v. State of Tamil Nadu (2025) represents an important instance of direct judicial engagement with gaming regulation. The Madras High Court upheld restrictions on gaming hours and mandatory Know Your Customer requirements, recognising that a substantial proportion of gaming platform users are minors and affirming the State's legitimate interest in protecting them from addiction and financial exploitation. Although the judgment's scope is delimited to real-money gaming and does not comprehensively address issues of grooming, content-based harm, or psychological exploitation, it signals a nascent judicial willingness to treat gaming regulation as a domain warranting proactive oversight rather than mere passive adjudication.[32]

C. Critical Appraisal of Judicial Trends

A critical appraisal of the foregoing judicial developments reveals a jurisprudential landscape that is progressive in its constitutional ambitions but inadequate in its technical specificity. The judiciary has demonstrably expanded the scope of child protection through constitutional interpretation and the purposive application of statutory provisions to digital contexts. However,

[30] Sneha Kalita v. Union of India, W.P. (C) No. 10498/2017 (India) (directions to block Blue Whale Challenge platforms and implement child-protective measures).
[31] Just Rights for Children Alliance v. S. Harish, (2024) INSC 716 (India) (passive possession of CSEAM punishable under POCSO Act and IT Act).
[32] Play Games 24x7 Private Limited v. State of Tamil Nadu (2025) (Madras High Court) (upholding restrictions on gaming hours and mandatory KYC requirements for gaming platforms).

 [ISSN 2581-5369]

it has not developed a coherent and technologically informed body of jurisprudence specifically calibrated to the operational realities of online gaming ecosystems. Courts have largely addressed gaming-related harms as factual variations within the established framework of cyber offences, rather than recognising gaming platforms as structurally distinct digital environments that present a unique risk topology requiring bespoke legal treatment.

This limitation is not trivial. The immersive design, real-time interactivity, virtual economy integration, and algorithmic engagement mechanisms of contemporary gaming platforms give rise to forms of harm — including behavioural manipulation, addiction facilitation, and virtual-world exploitation — that are not meaningfully captured by the legal categories and analytical frameworks developed for social media or general internet regulation. The transposition of those frameworks to gaming contexts, without adaptation, risks producing legal responses that are formally applicable but substantively inadequate. There is accordingly a compelling need for the judiciary to develop platform-specific guidelines, engage more rigorously with the technological architecture of gaming ecosystems, and adopt a proactively anticipatory rather than reactively responsive posture.[33]

IV. JUDICIAL CHALLENGES AND THE IMPERATIVE OF REFORM

The effective judicial regulation of cybercrime in gaming environments is impeded by a constellation of legal, technical, and institutional challenges that collectively compromise the capacity of the courts to deliver timely, accurate, and just outcomes in cases involving child victims. These challenges may be systematically identified as follows.

First, there is the challenge of technical comprehension. Cybercrime cases arising from gaming platforms routinely involve encrypted communications, virtual identities, algorithm-driven engagement, and the forensic analysis of real-time digital data. Conventional judicial training and legal reasoning, while sophisticated in their own domain, frequently lack the technical vocabulary and conceptual apparatus required to engage meaningfully with these complexities. The risk is that courts may misapprehend the nature of the offending conduct, misattribute causality, or apply legal standards in ways that are technically uninformed and therefore unjust.

Second, the anonymity and pseudonymity that characterise user interaction in gaming platforms present formidable obstacles to the attribution of legal liability. Offenders operating through avatar-based identities and encrypted communication channels may evade detection despite the most diligent investigative efforts, and the processes required to 'pierce the veil' of digital

[33] Majid Yar & Kevin F. Steinmetz, Cybercrime and Society 211–16 (3d ed., Sage Publications 2019); Lilian Edwards, Law, Policy and the Internet 187–92 (Hart Publishing 2018).

 [ISSN 2581-5369]

anonymity — including the compulsion of service providers to disclose user data — are procedurally complex, time-consuming, and not always conclusive.

Third, jurisdictional complexity constitutes a structural impediment of significant proportions. The global architecture of major gaming platforms means that perpetrators and victims may be separated by thousands of miles and multiple legal systems, requiring international judicial cooperation that is rarely swift or straightforward. The inadequacy of existing mutual legal assistance treaty frameworks for addressing the real-time exigencies of gaming-related cybercrime investigations is a deficiency that demands urgent diplomatic and legislative attention.

Fourth, the inherently time-consuming nature of judicial proceedings ill-suits the real-time urgency of cybercrime involving children. The psychological and financial harm occasioned by gaming-related offences frequently continues or intensifies pending the resolution of judicial proceedings, and the absence of effective interim relief mechanisms capable of rapid deployment represents a significant gap in the protective framework.

In light of these challenges, a comprehensive programme of judicial reform is both warranted and overdue. First and most urgently, the establishment of specialised cyber courts or dedicated benches equipped with trained judges and technical advisors would substantially enhance the quality of adjudication in gaming-related cybercrime cases. Such courts exist in various forms in a number of common law jurisdictions and have proven effective in improving both the accuracy and efficiency of proceedings involving complex digital evidence. Second, the superior courts should develop and issue platform-specific guidelines governing the obligations of gaming companies with respect to content moderation, user identification, and the reporting of suspected child exploitation — obligations that courts can then monitor and enforce through contempt proceedings and regulatory mandates. Third, the evidentiary rules applicable to digital evidence generated in gaming contexts should be revisited and modernised to reflect the technical realities of real-time data generation and the practical constraints faced by investigators in preserving such evidence.[34]

V. Comparative Legal Analysis: Lessons from the United Kingdom and the United States

A comparative analysis of the legal frameworks governing cybercrime against children in online gaming environments, as applied in the United Kingdom and the United States, illuminates

[34] Aparna Chandra et al., The POCSO Act: A Commentary 312–16 (Oxford University Press 2018); Clough, supra note 23, at 415–18.

important systemic differences that carry normative implications for the reform of the Indian legal framework. Comparative legal methodology, which entails the examination of similarities and differences between legal systems for the purpose of identifying best practices and informing reform initiatives, offers a valuable analytical lens through which the limitations of the Indian approach may be appraised and potential improvements identified.

The United Kingdom's Online Safety Act 2023 represents the most comprehensive legislative instrument currently operative in any common law jurisdiction for the regulation of online platforms in relation to user safety, particularly child safety. The Act imposes a statutory duty of care upon online service providers — a category sufficiently broad to encompass gaming platforms — requiring them to proactively identify and mitigate risks of harm to users, and to undertake mandatory risk assessments, implement robust content moderation systems, and promptly remove harmful content. The Ofcom, designated as the principal regulatory authority under the Act, is vested with substantial enforcement powers, including the imposition of significant financial penalties for non-compliance. Crucially, the Act's regulatory philosophy is fundamentally preventive: it obliges platforms to ensure safety rather than merely to respond to incidents of harm after they occur. This conceptual inversion — from reactive liability to proactive duty of care — represents a paradigmatic shift that the Indian framework has not yet replicated.[35]

In the United States, the Children's Online Privacy Protection Act (COPPA) 1998, 15 U.S.C. §§ 6501–6506, adopts a sector-specific regulatory model concentrated upon the protection of children's personal data. COPPA mandates that online service providers obtain verifiable parental consent before collecting, using, or disclosing the personal information of children under thirteen years of age, and requires platforms to maintain transparent and accessible privacy policies. The Federal Trade Commission is responsible for enforcement, and substantial civil penalties have been imposed upon non-compliant platforms. While COPPA's scope is narrower than the UK model — focusing primarily on data privacy rather than broader online safety — it provides a structurally clear and operationally coherent framework for child data protection that has proven reasonably effective in practice, and that offers instructive lessons for the development of child-specific data protection provisions in the DPDPA.[36]

The divergences between these foreign models and the Indian framework are both structural

[35] Online Safety Act 2023 (U.K.) c. 50, §§ 2, 7–11, 34 (statutory duty of care; mandatory risk assessments; Ofcom as enforcement authority with power to impose financial penalties).
[36] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2018) [hereinafter COPPA] (verifiable parental consent requirement for children under thirteen; FTC enforcement authority).

 [ISSN 2581-5369]

and philosophical. The Indian framework remains predominantly reactive — predicated upon the penalisation of harmful conduct after its occurrence — and lacks the equivalent of a statutory duty of care that would compel platforms to assume affirmative responsibility for child safety. The intermediary liability provisions of the IT Act, as currently framed, extend conditional immunity to platforms that comply with due diligence requirements, but these requirements are not specifically calibrated to the risks presented by gaming environments. There is no Indian legislative equivalent of the UK's proactive risk assessment mandate, no gaming-specific regulatory authority, and no comprehensive framework governing in-game financial transactions, user identification requirements, or the design-level safety obligations that are increasingly being recognised internationally as essential components of child-safe digital architecture.[37]

VI. RECOMMENDATIONS AND CONCLUSION

The foregoing analysis establishes, with considerable clarity, that the existing Indian legal framework, while not without merit, is structurally inadequate to address the multidimensional risks that online gaming platforms present to child users. The following recommendations are advanced as a basis for a comprehensive reform programme.

Legislative Reform: Parliament should enact a dedicated Online Gaming (Child Safety) Act that imposes a statutory duty of care upon gaming platform operators, mandates proactive risk assessments and content moderation systems, prohibits the deployment of manipulative design features targeting minors, and establishes minimum standards for identity verification and parental consent. The DPDPA should be amended to introduce child-specific data protection provisions that are binding upon gaming companies and enforceable by a dedicated regulatory authority with technical expertise in digital platforms.

Judicial Specialisation: The establishment of specialised cyber courts with dedicated jurisdiction over cybercrime cases involving children, staffed by judges with specialised training in digital law and supported by standing panels of independent technical experts, would materially enhance the quality, speed, and accuracy of adjudication. The Supreme Court and High Courts should consider issuing practice directions governing the collection, preservation, and admissibility of digital evidence generated in gaming environments.

Platform Accountability: Gaming companies operating in India should be subject to mandatory registration and periodic compliance audits by a statutory regulator. They should be

[37] See generally Schwartz & Solove, supra note 15, at 1850–55; Edwards, supra note 31, at 193–97.

 [ISSN 2581-5369]

required to implement robust age verification mechanisms, real-time content moderation with human oversight, transparent reporting mechanisms for harmful content and interactions, spending limits for accounts associated with minors, and OTP-based parental consent systems for account registration and financial transactions.

Digital Literacy and Parental Education: A sustained national programme of digital literacy education, directed at children, parents, educators, and law enforcement personnel, is an indispensable complement to legislative and judicial reform. Such a programme should equip stakeholders with the knowledge and skills necessary to identify, report, and respond to cybercrime in gaming environments, and should be supported by publicly accessible resources regarding the parental control features available on major gaming platforms.

International Cooperation: Given the inherently transnational character of major gaming platforms and the cross-border dimension of a significant proportion of gaming-related cybercrime, India should actively pursue the negotiation of expedited mutual legal assistance protocols with key partner jurisdictions, and should engage constructively with multilateral initiatives — including those led by INTERPOL, the UNODC, and UNICEF — directed at the development of harmonised international standards for child protection in online gaming environments.

In conclusion, the protection of children from cybercrime in online gaming environments is not merely a technological or regulatory challenge; it is a constitutional imperative and a fundamental obligation of the Indian State under Articles 21 and 39(f) of the Constitution, as well as under international instruments including the United Nations Convention on the Rights of the Child. The documented harms — ranging from the financial devastation of families to the psychological destruction of individual children — are not abstract risks but concrete realities that demand an urgent, comprehensive, and structurally sophisticated legislative and judicial response. The trajectory of India's cyber jurisprudence has been marked by significant progress, but the evolving architecture of gaming technology continues to outpace the adaptive capacity of the legal framework. Closing this gap, through the coordinated pursuit of legislative reform, judicial specialisation, platform accountability, and digital literacy, is an obligation from which neither the legislature, the judiciary, nor the executive may in good conscience resile.[38]

*****

[38] Constitution of India arts. 21, 39(f); United Nations Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3, arts. 16, 17, 19, 34.

 [ISSN 2581-5369]

VII. REFERENCES

Statutes and Legislation

1. Information Technology Act, 2000 (India), §§ 43, 66C, 66D.
2. Protection of Children from Sexual Offences Act, 2012 (India), §§ 11, 13, 14.
3. Digital Personal Data Protection Act, 2023 (India).
4. Bharatiya Nyaya Sanhita, 2023 (India).
5. Online Safety Act, 2023 (United Kingdom).
6. Children's Online Privacy Protection Act, 1998 (United States), 15 U.S.C. §§ 6501–6506.

Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
3. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
4. Just Rights for Children Alliance v. S. Harish, (2024) INSC 716.
5. Sneha Kalita v. Union of India, Writ Petition (2017) (India).
6. Play Games 24x7 Private Limited v. State of Tamil Nadu (2025) (India).
7. Enforcement Directorate v. Coda Payments India Pvt. Ltd. (2022).

Secondary Sources

1. Susan W. Brenner, Cybercrime and the Law: Challenges, Issues and Outcomes (Northeastern University Press 2012).
2. Jonathan Clough, Principles of Cybercrime (2d ed., Cambridge University Press 2015).
3. Majid Yar & Kevin F. Steinmetz, Cybercrime and Society (3d ed., Sage Publications 2019).
4. Daniel J. Solove, Understanding Privacy (Harvard University Press 2008).
5. Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction (Routledge 2018).
6. Sonia Livingstone, Children and the Internet: Great Expectations, Challenging Realities (Polity Press 2009).

 [ISSN 2581-5369]

7. Aparna Chandra et al., The POCSO Act: A Commentary (Oxford University Press 2018).
8. Daria J. Kuss & Mark D. Griffiths, Internet Gaming Addiction: A Systematic Review, 10 International Journal of Mental Health and Addiction 278 (2012).
9. Sameer Hinduja & Justin W. Patchin, Cyberbullying: Identification, Prevention, and Response, 41 Journal of School Violence 1 (2010).
10. Galen Lamphere-Englund, Protecting Children in Online Gaming: Mitigating Risks from Organized Violence (UNICEF Working Paper 2025).
11. Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011).
12. Nir Kshetri, Cybercrime and Cybersecurity in India, 44 Telecom Policy 101 (2020).
13. Aparna Viswanathan, Cyber Law Reforms in India, 8 NUJS L. Rev. 221 (2015).
14. Lilian Edwards, Law, Policy and the Internet (Hart Publishing 2018).
15. American Psychiatric Association, Diagnostic and Statistical Manual of Mental Disorders (DSM-5) (5th ed. 2013).
16. OECD, Children in the Digital Environment: Revised Typology of Risks (2021).
17. UNICEF Office of Research, Protecting Children in Online Gaming (2025).

*****

 [ISSN 2581-5369]