

The Dark Side of Digital Play : Psychological Deterioration, Social Disruption and Legal Accountability.

Syeda Asna Fatima Nahri

BA LLB (Hons), 5th year

Hindustan Institute of Technology and Science, School of Law, Chennai

Abstract: *Online gaming has become a feature of youth culture, facilitating recreation, social interaction and participation while presenting challenges concerning psychological well-being, interpersonal relationships, privacy and cybersecurity. This paper examines the darker dimensions of digital play, focusing on problematic gaming, cyberbullying, online grooming, financial exploitation, data misuse and cybercrime. Its objective is to assess whether legal frameworks adequately prevent gaming-related harm, allocate responsibility and provide effective remedies while protecting legitimate participation. Employing doctrinal analysis and comparative legal methodology, the paper considers international human rights principles, children's digital rights, Indian legislation, selected foreign regulatory approaches and academic scholarship. It distinguishes gaming disorder from frequent gaming and evaluates associations between gaming and psychological distress without presuming causation. The Blue Whale Challenge is considered as a case study of digital safeguarding concerns and evidentiary uncertainty, rather than proof of a direct causal relationship between a game and reported deaths. The analysis identifies fragmented regulation, barriers to cross border investigations, inconsistent safeguards, opaque monetisation practices and limited remedial mechanisms as significant legal challenges as it argues that accountability should depend on the conduct of relevant factors, applicable legal obligations and established evidentiary standards, rather than the mere occurrence of harm. The paper integrates psychological and social vulnerabilities with platform governance and legal responsibility also it recommends proportionate, age-appropriate safeguards, transparent monetisation, privacy-conscious design, accessible reporting mechanisms, effective enforcement and stronger international cooperation. A rights based regulatory approach can address preventable harm, protect young users and preserve the recreational, social and expressive benefits of online gaming within an accountable environment.*

Keywords: Online Gaming, Youth Vulnerability, Psychological Harm, Cybercrime, Social Disruption.

I. INTRODUCTION

Online gaming refers to the playing of digital games through internet connected devices and platforms that enable users to interact, compete, communicate, and participate in shared virtual environments and its rapid expansion has transformed gaming into a significant feature of contemporary youth culture, offering opportunities for recreation, creativity, skill development, and social connection, but simultaneously raising serious concerns about psychological well-being, interpersonal relationships, privacy, and digital safety. Although online gaming does not inherently result in harm, its consequences demand careful examination because excessive engagement, harmful interactions, and exploitative platform practices may adversely affect users, particularly children and adolescents whose emotional development and understanding of digital risks are still evolving. The World Health Organisation (WHO) recognises gaming disorder as a pattern characterised by impaired control over gaming, increasing priority given to gaming over



other activities, and continuation despite negative consequences, whereas the broader risks of online gaming extend to cyberbullying, harassment, grooming, financial scams, identity theft, unauthorised transactions, and misuse of personal information as such experiences may cause psychological distress, social isolation, financial losses, and lasting damage to interpersonal relationships, while the anonymity and interactive nature of digital environments may complicate the identification of perpetrators, investigation of offences, and determination of legal responsibility as these concerns extend beyond individual behaviour to raise fundamental questions about the obligations of gaming platforms, the effectiveness of regulatory institutions, and the adequacy of existing safeguards in protecting vulnerable users without unnecessarily restricting legitimate digital participation. The cross border operation of online gaming services further complicates the application of national laws, cybercrime investigations, electronic evidence collection, jurisdiction, and access to effective remedies, whereas inconsistencies between national regulatory approaches may create significant gaps in protection and enforcement. Online gaming must therefore be examined as a multidimensional legal concern in which psychological harm, social disruption, cybercrime, consumer vulnerability, and platform accountability intersect but the central question is Whether existing legal and regulatory frameworks adequately address these interconnected risks while safeguarding the rights, dignity, and interests of young users ? As this research examines international human rights principles and comparative regulatory approaches alongside India's legal framework, including cyber law, data protection, consumer protection, and online gaming regulation. Through doctrinal analysis of legislation, judicial decisions, international instruments, and scholarly literature, it evaluates deficiencies in prevention, accountability, enforcement, institutional coordination, and victim redress, particularly where affected individuals encounter barriers to reporting incidents, preserving electronic evidence, identifying offenders, and obtaining timely remedies and it seeks to identify gaps in legal protection and establish the need for clearer platform responsibilities, stronger safeguards, effective regulatory oversight, and accessible avenues of justice. Ultimately, the research advocates a proportionate, rights based approach that addresses demonstrable risks, strengthens the protection of children and adolescents, and preserves the legitimate recreational and social value of online gaming without treating participation itself as inherently harmful.

Commercial Exploitation of Youth Vulnerability in the Digital Gaming Ecosystem.

Online gaming has become an established feature of youth leisure, supported by smartphones, consoles, connectivity, and multiplayer platforms that enable interaction across geographical boundaries. Young people participate for entertainment, competition, creativity, and social connection, although experiences vary with age, circumstances, family support, and game design. Gaming should therefore not be treated as inherently harmful; the central concern is whether patterns of engagement or commercial practices undermine well being, autonomy, or legal rights. Many games use progression systems, rankings, streaks, limited time events, notifications, and rewards to encourage continued participation. These features may sustain interest but create pressure to remain active, complete time sensitive tasks, or maintain team status. Where gaming persistently displaces sleep, education, relationships, or other daily responsibilities, concerns about impaired self regulation become more significant. The World Health Organisation (WHO) distinguishes gaming disorder from frequent play by reference to impaired control, increasing priority given to gaming, continuation despite negative consequences, and significant impairment in important areas of functioning. The commercialisation of gaming raises distinct questions of consumer protection and platform accountability. The revenue models may include in game purchases, micro transactions, paid upgrades, cosmetic items, subscriptions, battle passes, advertising, virtual currencies, and paid random reward mechanisms such as loot boxes, these models are not unlawful in themselves, but their presentation and operation may create legal concerns where prices are unclear, virtual currencies obscure the real cost, purchases are difficult to reverse, advertising is inadequately disclosed, or interface design pressures users into spending. Such practices may engage consumer protection rules on misleading representations, unfair commercial practices, transparency, and informed consent; in some jurisdictions, specific loot box features may also raise questions under gambling law. The legal treatment varies between jurisdictions and depends on the product's design, applicable legislation, and evidence of the relevant conduct. Young users warrant particular attention because they may have limited financial experience and may be susceptible to peer pressure,



urgency cues, or reward based design and where games use behavioural data to personalise advertisements or spending prompts, privacy and data protection obligations may also arise. Accordingly, regulatory analysis should distinguish ordinary commercial engagement from deceptive, coercive, or exploitative practices, and assess whether safeguards such as clear real money pricing, spending controls, parental consent mechanisms, accessible refunds, and age appropriate design provide protection. The youth vulnerability thus emerges through the interaction of personal circumstances, social influence, game mechanics, and commercial incentives, requiring proportionate safeguards that preserve the recreational and social benefits of gaming while respecting young people's developing autonomy and digital participation.

Psychological Deterioration and Mental Health Risks of Online Gaming

Online gaming can provide recreation, problem solving opportunities, and social connection, but its psychological and medical effects depend on the nature, duration, and context of participation. The principal concern is not frequent play alone, but gaming that becomes difficult to regulate and interferes with everyday functioning. The World Health Organisation recognises gaming disorder in ICD 11 as a pattern involving impaired control, increasing priority given to gaming over other activities, and continuation despite negative consequences, with significant impairment generally evident for at least twelve months. This threshold distinguishes a clinically recognised disorder from enthusiasm, high engagement, or temporary periods of intensive play. Research reviews have found associations between problematic gaming and anxiety, depressive symptoms, attention difficulties, and other emotional or behavioural problems among adolescents; however, association does not establish that gaming itself causes these conditions. Psychological distress may precede excessive gaming, arise alongside it, or be intensified by it, making individual assessment essential. Diagnosis should be made by qualified clinicians. When gaming sessions extend into the night, delayed bedtimes and insufficient sleep can contribute to fatigue, irritability, reduced concentration, and difficulties regulating emotions.

Persistent disruption may affect school attendance, learning, and academic performance, although research on academic outcomes is mixed and may involve reciprocal relationships between school difficulties and problematic gaming. Competitive ranking systems, public performance metrics, social comparison, fear of missing limited time events, and pressure from teammates can create stress for some users, while online communities can also offer belonging, cooperation, and support. Reliance on gaming as the primary response to loneliness or distress may narrow coping strategies and increase emotional dependence, particularly when offline support is limited. Exposure to hostile communication, cyberbullying, sexual exploitation, gambling like reward systems, or deceptive purchase prompts may add further psychological strain. Violent game content also requires measured analysis: research has reported associations with some aggressive outcomes, but evidence does not justify claiming that violent games cause criminal or lethal violence. Extended gaming may also coincide with physical concerns such as eyestrain, musculoskeletal discomfort, reduced physical activity, and disrupted sleep routines, although these outcomes vary and should not be attributed to gaming without considering other factors. Accordingly, assessment should focus on loss of control, persistence, distress, and measurable impairment rather than hours played alone. A balanced public health and legal response should promote early support, age appropriate design, family and school awareness, and accessible mental health services while recognising that most gaming participation does not constitute a psychiatric disorder.

Social Fragmentation and the Erosion of Youth Social Wellbeing

Online gaming has become an important social environment for adolescents and young adults, providing opportunities for teamwork, friendship, creative expression, and participation in online communities. These benefits, however, coexist with social risks that depend on platform design, moderation practices, user behaviour, age, and individual circumstances. Multiplayer chats and voice channels can facilitate cyberbullying, targeted harassment, hate speech, and discriminatory conduct, while anonymity and the rapid circulation of messages may make abuse difficult to identify, document, or report. Difficulties arise when lengthy sessions displace family interaction, school responsibilities, sleep, or offline friendships, or when disagreements over spending and time online contribute to conflict at home. At the same time, online communities can provide social support, particularly for young people who feel isolated in their immediate environments. A further concern is the potential misuse of gaming spaces to contact and manipulate minors.



Grooming may involve trust building, requests for personal information or intimate images, coercion, and threats; identity deception can make it harder for young users to assess who is contacting them. UNICEF has identified online gaming communities as environments that can be misused for child exploitation and recruitment into violence, underscoring the importance of child centred safeguards and effective reporting mechanisms. Peer dynamics can also intensify vulnerability through status competition, rankings, team obligations, exclusion, and pressure to purchase virtual items to maintain social standing. Commercial practices warrant scrutiny where in game currencies obscure real prices, purchases are promoted through pressure tactics, or paid random reward mechanisms encourage repeated spending. Such features are not automatically unlawful, but may raise consumer protection concerns when information is unclear or marketing targets children inappropriately; the legal position depends on the jurisdiction and the product's design. Young users may also encounter gambling like spending patterns without fully appreciating cumulative costs. Social risks are not distributed equally: girls and women may experience gendered insults or sexualised harassment, while players with disabilities, minority identities, limited connectivity, or fewer resources may face barriers to safe and inclusive participation. These problems should not be framed as inevitable consequences of gaming, but as risks shaped by social norms, accessibility, platform governance, and enforcement. Effective responses therefore require accessible reporting and blocking tools, age appropriate privacy settings, transparent monetisation, consistent moderation, parental and school support, and cooperation between platforms, child protection bodies, and law enforcement agencies. A rights based approach should protect young users from abuse and exploitation while preserving the opportunities for social connection and participation that online gaming can offer.

Legal and Institutional Barriers in Addressing of Digital Play

Addressing online gaming-related harm presents substantial legal and institutional challenges because the occurrence of an incident does not automatically result in official recognition, identification of the alleged perpetrator, or access to an effective remedy. Victims of cyberbullying, online grooming, financial misconduct, and psychological injury may encounter difficulties reporting incidents, preserving evidence, and navigating complex legal procedures. These obstacles are particularly pronounced among children and adolescents, whose limited legal awareness, dependence on adults, fear of retaliation, and concerns about losing access to digital communities may discourage disclosure. Victims may delete abusive communications, block perpetrators before preserving relevant records, or delay complaints because of stigma or fear of blame, while parents may lack the technical expertise required to document suspicious interactions and preserve digital evidence. Delayed reporting can compromise investigations because accounts may disappear, usernames may change, messages may be automatically deleted, and relevant records may become inaccessible. Even after complaints are registered, victims may struggle to identify competent authorities, understand procedural requirements, obtain case updates, and comply with repeated requests for statements or supporting documentation. Investigating agencies may face shortages of trained personnel, inadequate cyber forensic infrastructure, substantial caseloads, and delays in obtaining information from gaming platforms. cross border incidents create further jurisdictional complications when victims, alleged perpetrators, platform operators, and relevant records are located in different countries, requiring international cooperation between authorities governed by distinct procedural rules, evidentiary standards, and legal frameworks. Establishing liability presents additional difficulties because financial loss or psychological distress alone does not establish the perpetrator's identity, prove causation, or demonstrate a platform's legal responsibility. Psychological injuries may be difficult to substantiate where symptoms develop gradually, multiple contributing factors exist, or professional assessments are unavailable. The World Health Organisation (WHO) recognition of gaming disorder under the International Classification of Diseases, Eleventh Revision, that does not establish that every adverse psychological outcome associated with gaming constitutes a diagnosable disorder or results directly from gaming participation. Institutional fragmentation further complicates enforcement because responsibilities may be distributed among police departments, cybercrime units, data protection regulators, consumer protection authorities, child protection institutions, and gaming regulators. Overlapping mandates, inconsistent procedures, and unclear jurisdictional boundaries can impede coordination and delay investigations. Existing criminal, consumer protection, privacy, and child safeguarding provisions may also encounter limitations



when applied to emerging technological practices, particularly where statutory definitions or jurisdictional rules do not adequately address the conduct concerned. The victims may face financial constraints, limited access to legal representation, prolonged proceedings, inadequate communication from authorities, and uncertainty regarding compensation or other remedies and the evidentiary dependence on platform operators creates a further imbalance because investigators may require privately controlled communication histories, account information, transaction records, and technical logs to reconstruct incidents. Data retention policies, privacy restrictions, inaccessible records, and delays in lawful disclosure may obstruct evidence collection. Furthermore, content removal or account suspension does not necessarily resolve financial losses, reputational damage, continuing psychological distress, or difficulties obtaining judicial redress. These interconnected procedural, evidentiary, jurisdictional, and institutional barriers complicate the attribution of liability and the pursuit of enforceable remedies.

Victim Protection and the Limits of Legal Remedies in Digital Play

The effectiveness of legal regulation in online gaming must be assessed not only by its capacity to prevent unlawful conduct, but also by the remedies available to individuals who experience harm. Victims of cyberbullying, online grooming, financial exploitation, identity theft, unauthorised transactions, and harmful digital interactions may face substantial difficulties in reporting incidents, preserving electronic evidence, identifying perpetrators, and obtaining timely assistance, whereas children and adolescents may lack the legal awareness, financial resources, or confidence necessary to initiate proceedings, and fear of parental restrictions, social stigma, retaliation, or losing access to online communities may discourage disclosure. In India, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Protection of Children from Sexual Offences Act, 2012, and the Consumer Protection Act, 2019, may provide applicable remedies depending on the conduct and relevant legal provisions, but statutory protection does not necessarily guarantee effective redress or timely relief. The victims may remain uncertain about appropriate reporting authorities, while overlapping institutional responsibilities, delayed investigations, difficulties obtaining platform held information, and challenges identifying perpetrators can obstruct enforcement, particularly where electronic evidence is incomplete or distributed across multiple service providers and the claims involving psychological injury present additional evidentiary challenges because emotional distress may have several contributing factors, making it necessary to establish a credible connection between harmful conduct and the injury suffered, whereas the consequences of online exploitation may persist long after the original incident. Cross border incidents further complicate proceedings when offenders, gaming operators, payment intermediaries, and electronic records are situated in different jurisdictions, and platform complaint mechanisms may prove inadequate when decisions lack transparency, appeals are inaccessible, or content removal and account restrictions fail to address underlying misconduct. These limitations raise broader concerns regarding procedural fairness, institutional accountability, victim participation, and access to justice, particularly where individuals must navigate complex procedures without adequate guidance or support. Children affected by online exploitation or harassment require particular consideration because their interests extend beyond criminal prosecution to confidentiality, psychological assistance, protection against retaliation, and age appropriate participation in legal proceedings, while manipulation, threats, and coercion may intensify their vulnerability. A comprehensive legal assessment must therefore examine whether existing mechanisms facilitate timely investigations, proportionate accountability, effective remedies, and meaningful support without imposing unreasonable evidentiary or procedural burdens on victims, especially where platforms possess information essential to establishing responsibility. The central concern is not merely whether the law recognises online gaming related misconduct, but whether affected individuals can translate that recognition into enforceable rights and practical relief, because delayed justice and inadequate institutional responses may deepen psychological distress, financial loss, and social disruption. Access to justice must consequently remain a central measure of the adequacy of online gaming regulation, whereas protecting users, particularly children and adolescents, demands sustained attention to effective enforcement, institutional responsibility, and the lasting consequences of digital harm.



The Statutory and Regulatory Framework for Online Gaming in India

The legal framework governing online gaming in India combines constitutional principles, central legislation, state gaming laws, data protection, consumer protection and criminal law. The Articles 14, 19 and 21 frame questions of equality, commercial freedom, personal liberty and proportionality, but do not create an unconditional right to operate every gaming service. The principal recent development is the Promotion and Regulation of Online Gaming Act, 2025, in force from 1 May 2026, together with the Promotion and Regulation of Online Gaming Rules, 2026. The Sections 5 to 7 prohibit offering online money games, related advertising and facilitating payments for such games. The Rules establish the Online Gaming Authority of India and provide for game classification, registration of specified categories, user-safety requirements and grievance redressal. The Act's constitutional validity remains pending before the Supreme Court, as of October 2026, no stay of its operation had been reported and this central prohibition must be distinguished from state legislation governing betting and gambling. In *State of Tamil Nadu v. Junglee Games India Private Limited*, 2026 INSC 594, the Supreme Court upheld challenged Tamil Nadu and Karnataka laws regulating or prohibiting online games played for stakes, recognising state legislative competence over betting and gambling. Earlier decisions, including *R.M.D. Chamarbaugwala v. Union of India*, AIR 1957 SC 628, *State of Andhra Pradesh v. K. Satyanarayana*, AIR 1968 SC 825 and also the *Dr. K.R. Lakshmanan v. State of Tamil Nadu*, (1996) 2 SCC 226, developed the distinction between skill and chance within their statutory contexts as they do not establish a blanket exemption for skill-based games involving monetary stakes following the 2026 ruling. The Information Technology Act, 2000, addresses related cyber conduct. Sections 43 and 66 may apply to unauthorised access or interference with computer resources, while Sections 66C and 66D cover identity theft and cheating by personation. Section 79 provides conditional intermediary protection, subject to statutory requirements and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. In the case of *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, the Supreme Court clarified important limits on online content restrictions and intermediary takedown obligations. The Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025, provide a framework for personal-data processing, security and accountability, including safeguards concerning children. Their principal data-processing duties are subject to phased commencement and are not all fully operative as of October 2026. The Consumer Protection Act, 2019, may address misleading gaming advertisements and unfair trade practices, while the *Bharatiya Nyaya Sanhita*, 2023 and the Protection of Children from Sexual Offences Act, 2012, apply where conduct satisfies the elements of a recognised offence. The applicable legal requirements therefore depend on the game's classification, the relevant central or state legislation, and the nature of the conduct in question.

Comparative Perspectives on the International Online Gaming Regulation

The International approaches to online gaming are guided by human rights, child protection, privacy, freedom of expression and national regulatory policies. Articles 17 and 19 of the International Covenant on Civil and Political Rights protect privacy and freedom of expression, subject to applicable legal restrictions, while Articles 3, 16 and 17 of the United Nations Convention on the Rights of the Child address children's best interests, privacy and access to information and the Committee on the Rights of the Child's General Comment No. 25 (2021) explains how these protections apply to digital environments, including online risks, exploitation and commercial practices affecting children. In the European Union, the Digital Services Act, Regulation (EU) 2022/2065, imposes due-diligence obligations on covered intermediary services, with Article 28 requiring appropriate and proportionate measures to protect minors privacy, safety and security. The European Commission's 2025 guidelines further address cyberbullying, harmful content, unwanted contact and addictive design, while emphasising that child-safety measures should respect children's fundamental rights. In the United Kingdom, the Online Safety Act, 2023 requires in-scope user-to-user and search services to assess risks to children and implement applicable safety measures. In the United States, the Children's Online Privacy Protection Act (COPPA) regulates the collection of personal information from children under thirteen by covered online services, including qualifying gaming applications; it does not constitute a comprehensive online gaming safety regime whereas China follows a more restrictive approach, requiring real-name registration and limiting minors' online gaming to specified periods. Judicial decisions further demonstrate the balance



between individual rights and regulatory authority. In *Brown v. Entertainment Merchants Association*, the United States Supreme Court recognised video games as protected expression and invalidated a restriction on minors access to violent video games, highlighting constitutional limits on content-based regulation. Conversely, in *Liga Portuguesa de Futebol Profissional v. Bwin International*, the Court of Justice of the European Union accepted restrictions on cross border online gambling intended to combat fraud and crime, illustrating the scope of national regulatory authority under European Union law. The Council of Europe's Convention on Cybercrime (Budapest Convention) also provides a structured framework for criminalising specified cyber offences and facilitating international cooperation and electronic-evidence gathering, although it does not establish a gaming-specific regulatory regime. Additionally, the World Health Organisation recognition of gaming disorder in ICD-11 informs international public-health discussions by distinguishing clinically significant impairment from ordinary gaming. Collectively, these approaches demonstrate that international online gaming governance remains fragmented, with differences in child-safety standards, gambling restrictions, privacy obligations and enforcement powers. cross border platforms further complicate jurisdiction, evidence gathering and accountability, making the reconciliation of fundamental rights, public protection and consistent regulatory enforcement a central challenge.

Platform Accountability and Regulatory Reforms in Online Gaming

Online gaming platforms have legal and ethical responsibilities to protect young users from foreseeable risks while respecting privacy and freedom of expression. Regulatory gaps arise when safety duties are unclear, age safeguards are ineffective, commercial design is opaque, or complaint mechanisms fail to provide meaningful remedies. Platforms should conduct documented risk assessments identifying risks linked to chat functions, user generated content, recommendation systems, in game purchases, and contact between adults and minors. They should appoint a responsible safety lead and publish reports describing risks, moderation actions, and complaint outcomes without exposing users personal information. Age assurance should be proportionate to the risk and collect the minimum information necessary. Child accounts should default to restrictive privacy settings, limit unsolicited contact and location sharing, and provide clear parental controls. Privacy should be built into product design through data minimisation, limited retention, secure storage, and clear explanations of why information is collected and shared. Platforms should test game features for foreseeable harms, including harassment, grooming, and discriminatory conduct, and provide users with simple tools to block, mute, report, and appeal. Monetisation requires safeguards. Prices should be shown in real currency before purchase, virtual currency exchange rates should be clear, recurring subscriptions should be easy to cancel, and spending histories and limits should be available to users and guardians. Paid random reward systems should disclose probabilities and costs, while advertising should be identifiable and unsuitable targeting of children prohibited. Complaints about harassment, fraud, unauthorised purchases, or account theft should receive timely acknowledgement, a reasoned decision, and an accessible appeal route. Where evidence indicates criminal conduct or imminent danger, platforms should preserve relevant records and refer matters to competent authorities in accordance with law. Regulators should establish measurable standards, conduct independent audits, impose proportionate penalties for serious or repeated failures, and require effective remedies for affected users. Cross border cooperation is essential because services, users, payments, and electronic evidence may be located in different jurisdictions. Governments should develop compatible procedures for lawful evidence requests, incident reporting, and child protection referrals while maintaining privacy and due process safeguards. These recommendations reflect emerging risk based approaches to child safety in the EU and UK, alongside UNICEF's guidance for the gaming industry. A rights based framework should place responsibility on companies in proportion to their control and capacity, involve young people in safety design throughout the development lifecycle, and preserve lawful gaming, expression, and social connection.

Case Study: The Blue Whale Challenge (2017)

The Blue Whale Challenge provides a case study for examining the darker dimensions of online gaming, including psychological vulnerability, social disruption, and legal accountability. Widely reported during the late 2016 and 2017, the phenomenon was described as a series of online tasks allegedly communicated to participants by other users, with



reports of escalating instructions involving self-harm. Its status as a conventional game remains debatable. Its relevance to online gaming lies in the use of game-like sequencing, digital communication, secrecy, and behavioural pressure to influence vulnerable individuals. Psychologically, such interactions raise concerns about distress, isolation, coercion, and the imitation of harmful behaviour, especially among adolescents. Socially, they can create fear among families and schools, complicate the identification of risks, and encourage the circulation of unverified claims through digital networks. The Indian Supreme Court proceedings demonstrate how these concerns can become questions of public responsibility, in the case of *N.S. Ponnaiah v. Union of India and Others*, W.P. (C) No. 872 of 2017 and the connected matter *Sneha Kalita v. Union of India and Another*, W.P. (C) No. 943 of 2017, the petitioners sought action against the Blue Whale Challenge and similar harmful online games. In its orders of 27 October and 20 November 2017, the Court addressed the matter through directions relating to public awareness and coordination among relevant authorities, the proceedings illustrate judicial attention to reported digital risks, but the petitioners' allegations should not be treated as proof that the Challenge caused particular deaths or as a judicial finding establishing causation. The Government's technical investigation, as recorded in the 20 November order, stated that CERT-In had been unable to establish the Challenge's involvement in the incidents reported to it, so this qualification is central to responsible legal analysis because media coverage, allegations, and verified findings are distinct categories and the research done by Khasawneh and colleagues examined 60 YouTube videos, 1,112 comments, and 150 Twitter posts referring to the Challenge. The researchers found that most videos failed to meet at least half of the suicide-prevention messaging guidelines used in their analysis, raising concerns about harmful portrayals and online amplification. The study did not establish that exposure directly caused acts of self-harm or suicide. The case illustrates legal difficulties in identifying anonymous actors, preserving electronic evidence, addressing cross border conduct, and determining when platforms may be responsible under applicable law and it also highlights tensions between child protection, privacy, freedom of expression, and proportionate content regulation. The Blue Whale Challenge should not be presented as evidence that gaming itself causes suicide rather, it demonstrates how coercive digital interactions can exploit online participation and expose gaps in public understanding, platform governance, and legal attribution, its significance is the need to assess online harms through reliable evidence while recognising their psychological and social consequences.

Conclusion

The darker dimensions of online gaming demand urgent and sustained attention from governments, technology companies, legal institutions, and the international community, as the psychological, social, and financial consequences of digital exploitation can extend far beyond the incident itself and, in some circumstances, cause lasting harm that cannot be fully reversed. Although online gaming offers legitimate opportunities for recreation, creativity, and social connection, these benefits must not obscure the risks of cyberbullying, online grooming, financial exploitation, privacy violations, problematic gaming, and other forms of digital abuse, particularly where children and young people lack the experience or resources necessary to protect themselves, the central concern is not simply the occurrence of such harms, but the institutional failures, evidentiary barriers, fragmented regulations, and inadequate remedies that can allow preventable suffering to persist without meaningful accountability. At the same time, responsible legal analysis requires a distinction between established wrongdoing and alleged harm, problematic gaming and ordinary participation, and correlation and causation, since effective protection must rest on reliable evidence rather than fear or indiscriminate restrictions. The Blue Whale Challenge illustrates the importance of confronting credible digital threats without treating unverified allegations as proven facts, while recognising that uncertainty must never become an excuse for indifference towards vulnerable users. The legal protection must therefore extend beyond the enactment of legislation to encompass effective enforcement, transparent commercial practices, privacy conscious design, age appropriate safeguards, accessible reporting, timely preservation of evidence, and meaningful support for victims. International cooperation is equally essential because digital platforms operate across national boundaries, whereas investigative powers, regulatory standards, and access to remedies remain divided among jurisdictions and the governments must establish clear responsibilities and enforceable standards, technology companies must be held accountable for failures to meet applicable legal obligations, and educational institutions and families must be equipped



to recognise risks without placing the entire burden of protection on young users themselves. The time has come for the world to move beyond acknowledging these dangers and to treat the protection of digital users, especially children and adolescents, as an urgent legal and social responsibility. Prevention cannot guarantee that every harm will be avoided, but delayed intervention can leave victims facing consequences that no subsequent investigation, penalty, or compensation can fully repair. Ultimately, the legitimacy of digital progress must be measured not only by innovation, engagement, or commercial success, but also by the safety, dignity, and rights of the people who inhabit these virtual spaces, because a digital environment that exposes its youngest participants to preventable harm without effective accountability is not progress worthy of protection.

BIBLIOGRAPHY

1. Problematic gaming, psychiatric comorbidities, and adolescence: A systematic review of the literature. (2024) <https://pubmed.ncbi.nlm.nih.gov/38901145/>
2. Gaming disorder in the ICD-11: the state of the game. (2025) <https://pmc.ncbi.nlm.nih.gov/articles/PMC12640003/>
3. General comment No. 25 (2021) on children's rights in relation to the digital environment. <https://digitallibrary.un.org/record/3906061?ln=en&v=pdf>
4. Online Gaming Addiction and Basic Psychological Needs Among Adolescents: The Mediating Roles of Meaning in Life and Responsibility. (2023) <https://pmc.ncbi.nlm.nih.gov/articles/PMC9831379/>
5. European Parliament and Council of the European Union (2022) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services (Digital Services Act). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R2065>
6. United Kingdom, Online Safety Act (2023) <https://www.legislation.gov.uk/ukpga/2023/50>
7. Information Technology Act, 2000 https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
8. N.S. Ponnaiah v. Union of India and Others, Public Interest Litigation, W.P. (Civil), Supreme Court of India. (2017) <https://images.assettype.com/barandbench/import/2017/09/brindtha-watermark.pdf>
9. Sneha Kalita v. Union of India & Anr., W.P. (Civil) Nos. 943 and 872 of 2017, Supreme Court of India. (2017) <https://indiankanoon.org/doc/92334486/>
10. Promotion and Regulation of Online Gaming Act, 2025 <https://www.meity.gov.in/static/uploads/2025/10/8a7f103cefc68ed8aaa2ebc9a2ed7c13.pdf>

