

Volume 02 | Issue 02 | June 2026 | Quarterly

CYBERPEACE

M A G A Z I N E

**ONLINE GAMING
BEYOND
ENTERTAINMENT:
GOVERNANCE AND
DIGITAL SOCIETY**

FREE DIGITAL EDITION



<https://magazine.cyperpeace.click/>

emerging technologies. digital laws and governance. trust and safety. cyber diplomacy.

© 2026 CyberPeace Foundation. All rights reserved.

CyberPeace Magazine is a publication of CyberPeace Foundation. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including electronic or mechanical, without prior written permission from the publisher, except for brief quotations with appropriate attribution.

This is a digital publication. An ISSN has been applied for.

The views and opinions expressed in this magazine are those of the respective authors and do not necessarily reflect the official policy or position of CyberPeace Foundation.

While every effort has been made to ensure the accuracy of the information presented, the publisher makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, or suitability of the content.

CyberPeace Magazine was formerly published as Cyber4n6 and is being rebranded to reflect an expanded scope and global focus.



Published by:

CyberPeace Foundation



For inquiries, collaborations, or permissions:

secretariat@cyberpeace.net



Website:

www.cyberpeace.org



Our Team

EDITOR-IN-CHIEF

Maj Vineet Kumar

Founder and Global
President CyberPeace



EDITORIAL BOARD



1. Lt Gen (Dr.) Rajesh Pant (retd)

Global Advisor, CyberPeace, PVSM, AVSM, VSM
Former National Cybersecurity Coordinator



2. Shri SN Pradhan

IPS (Retd), Global CEO, CyberPeace
Former Director General, Narcotics Control Bureau



3. Dr. Bhaskar Chatterjee

Former IAS, Global Advisory Council, CyberPeace



Our Team

EDITORIAL BOARD



**4 Prof. (Dr.)
Manish Prateek**

Professor and
Pro Vice-Chancellor,
DBS Global University



**5 Prof. (Dr.)
Scott J Shackleford**

Associate Vice President &
Vice Chancellor for Research,
Indiana University
Bloomington (IUB)

ADVISORS



1 Ms. Ronita Sengupta

Founder,
We Allies



2 Mr. Pavithran Rajan

Global Advisor,
CyberPeace

PROJECT COORDINATOR



Ms. Ayndri
Research Analyst,
Policy & Advocacy,
CyberPeace

EDITORIAL TEAM



1 Ms. Hithika Kohli
Consultant,
CyberPeace



**2 Ms. Anupma
Prakash
Srivastav**
Consultant,
CyberPeace



3 Ms. Naina Jain
Intern,
CyberPeace

DESIGN & PRODUCTION



Mr. Ajeet Kumar
Sr Graphic Designer,
CyberPeace

TABLE OF CONTENTS

Editorial Note

Maj Vineet Kumar

Founder & Global President, CyberPeace

India's New Online Gaming Rules: What Changes for Platforms, Players, and Regulation?

Editorial Team

Visual Intelligence: Mapping the Systems Behind Digital Gaming

Editorial Team

Expert Speak: Interview

Shailendra Vikram Singh (ex MHA)

Gaming Influencers: The New Architects of Digital Culture

Anupma Prakash Srivastava

Safeguarding the Digital Citizen: The Economic Impact of the Real-Money Gaming Ban

Dr. Julian Seal P, Avinash Verma

Addictive Game Design and Child Spending in Online Gaming: Evaluating India's Dark Pattern Regulatory Framework

Rahul Kumar

Compliance Checklist for Online Gaming Platforms: What Companies Need to Build, Monitor, and Maintain

Isharth Kumar

The Gaming Lexicon: Decoding the Jargon of Online Play

Hithika Kohli

Gaming as a Third Space: How Virtual Worlds Are Becoming Social Spaces for a Generation

Editorial Team

The Other Side of the Screen

Anupma Prakash Srivastava

CyberPeace in Action

CyberPeace Corps

EDITOR'S NOTE

Maj Vineet Kumar

Founder and Global President
CyberPeace

Dear Readers,
Welcome to the June 2026 edition of CyberPeace magazine

In this issue, we delve into the evolving phenomenon of online gaming, examining how it has transformed beyond entertainment to influence the trajectory of governance, social interaction and societal transformation.

What was once written off as a leisure activity has now grown into a multi-faceted digital ecosystem that is redefining how people communicate, collaborate, trade and express themselves online. Features such as virtual currencies, live-service models and AI-driven systems have reconfigured the patterns and dynamics of how users inhabit, interact and engage with the digital landscape. Moreover, multiverse platforms and virtual economies now function as independent entities in the form of social hubs and marketplaces.

The accelerating growth of this industry has brought forth critical conversations around privacy, online safety, cybersecurity, digital wellbeing and responsible innovation. Over the coming years, questions around youth safety, real-money gaming and platform accountability will sit along data protection and AI governance in legislation and policy debates. In view of these emerging challenges, this edition is a must-read for all readers interested in the complexities of this developing terrain.

As gaming platforms revolutionise into influential digital social spaces (especially with respect to minors and younger generations), regulatory mechanisms are synchronously being compelled to strike a balance between innovation and accountability. The future of online gaming depends not only on technological advancements, but also on how conscientiously these modern digital ecosystems will be designed, governed and protected.

To support this, our June edition talks about India's evolving online gaming regulations and presents a practical compliance checklist for platforms. Sections also explore business, market and governance structures to highlight the high risks and legal compliance in gaming communities that increasingly serve as spaces for learning, interaction and engagement. The edition also encapsulates a comprehensive gaming lexicon section that introduces some of the key terms, concepts and trends that underpin modern digital play. It also incorporates updates from CyberPeace's field initiatives showcasing how awareness, capacity-building and collaborative actions deliver meaningful impact on the ground.

At CyberPeace, we remain committed to promoting cyber awareness, digital safety and informed dialogue around emerging technologies and online risks. We hope this edition offers valuable insights and enriches the deliberative process and policy discourse pertaining to gaming, governance and the future of digital society.



“

To support this, our June edition talks about India's evolving online gaming regulations and presents a practical compliance checklist for platforms.

INDIA'S NEW ONLINE GAMING RULES: WHAT CHANGES FOR PLATFORMS, PLAYERS, AND REGULATION?

-EDITORIAL TEAM

India's online gaming industry has expanded rapidly in recent years, fuelled by smartphone penetration, digital payments, competitive gaming culture, and increasing investor interest. Yet regulation has struggled to keep pace. Questions around real-money gaming, consumer protection, platform accountability, and legal uncertainty have repeatedly placed the sector at the centre of policy debate.

The Promotion and Regulation of Online Gaming (PROG) Rules, 2026, notified by the Ministry of Electronics and Information Technology (MeitY)

seek to operationalise India's new online gaming framework under the PROG Act, 2025. The Rules intend to promote legitimate online gaming and e-sports while tightening oversight of online money games and strengthening user safeguards.

A NEW REGULATOR FOR INDIA'S GAMING ECOSYSTEM

At the centre of the framework is the creation of the Online Gaming Authority of India (OGAI) under MeitY.

Designed as a digital-first regulatory authority headquartered in Delhi, OGAI is chaired by the Additional Secretary, MeitYY, and includes representation from ministries such as Home Affairs, Finance, Information & Broadcasting, Sports, and Investment. Its creation signals a move toward a centrally regulated regulatory model for online gaming oversight.

The Authority's mandate is broad. Its responsibilities include:

- classifying online games;
- maintaining a list of prohibited online money games;
- registering notified games and e-sports;
- issuing codes of practice and operational directors;
- handling appeals and grievances; and
- coordinating with financial institutions and payment systems.

Rather than dispersing oversight across multiple agencies, the Rules place substantial regulatory authority within a single institutional framework

FROM LEGAL AMBIGUITY TO STRUCTURED REGULATION

Rather than dispersing oversight across multiple agencies, the Rules place substantial regulatory authority within a single institutional framework

Historically, India's gaming regulation relied heavily on judicial distinctions between games of skill and games of chance. Courts examined whether success depended primarily on a player's judgment, knowledge, or strategy rather than luck. However, digital gaming ecosystems have complicated this traditional framework.

Modern online platforms frequently combine virtual assets, in-game purchases, real-time payments, algorithmic engagement systems, and cross-border participation. As a result, regulatory concerns today extend beyond gambling law in issues of financialising digital consumer protection, platform governance, and other key policy

The PROG Rules attempt to respond to these challenges by moving regulation away from broad conceptual categories and toward a more formal system of classification, registration, compliance, and enforcement.





HOW GAMES WILL BE CLASSIFIED

One of the most significant changes introduced by the Rules is a formal determination mechanism for classifying online games.

A game may be reviewed through:

- ▶ suo motu action by CCAI;
- ▶ an application from a gaming service provider; or
- ▶ government notification of specified categories of games for review.

In making its determination, the Authority may consider several factors, including whether users pay stakes or deposits, whether monetary winnings are expected, how the platform operates (revenue share or not), and whether rewards or virtual assets can be traded or monetised outside the gaming ecosystem.



This is an important regulatory shift. Instead of relying exclusively on the traditional skill-versus-choice distinction, the Rules examine the economic and operational design of platforms.



The framework also introduces procedural timelines, with determinations expected to be completed within ninety days in most cases.



WHAT CHANGES FOR PLATFORMS?

- ▶ For gaming companies, the Rules introduce both regulatory clarity and new compliance obligations. Importantly, no online game requires registration. Registration becomes mandatory mainly for certified categories of higher-risk platforms, requiring users to proof their safety and maintaining designated compliance contact.
- ▶ Where registration is required, approved entities receive a digital registration certificate and must comply with operational obligations, including display of required safety protocols, and maintaining designated compliance contact.
- ▶ The Rules also draw a clear line between e-sports and online money gaming. Online money games cannot be registered as e-sports, limiting attempts to use e-sports legitimacy to shield wagerer-style activities.
- ▶ At the same time, industry stakeholders may face new compliance costs relating to platform design, safety mechanisms, grievance systems, and engagement with regulatory programs. Recent industry respuesta to these concerns around implementation clarity and operational burdens.



KEY TAKEAWAY



The new Rules aim to create a more accountable and transparent gaming ecosystem—balancing innovation and user protection while bringing much-needed regulatory structure to the sector.

WHAT CHANGES FOR PLAYERS?

The Rules place considerable emphasis on user protection, particularly for children and vulnerable users.



A notable innovation is the introduction of 'user safety features' tailored to a game's risk profile. These safeguards may include:



age verification and age restrictions;



parental controls;



session or time-management tools;



mechanisms to report child-safety concerns;



counselling or support measures; and



systems to promote fair gameplay.

This marks a broader transition from compliance-based regulation toward safety-by-design principles in digital platform governance.

The grievance system has also been formalised. Platforms must first establish their own internal grievance redressal mechanisms. Where users remain dissatisfied, or receive no response, they may appeal to OGAI, followed by a further appellate remedy before the Secretary, MeitY.



For players, this creates clearer procedural channels for complaints and dispute resolution.



A NEW REGULATORY DIRECTION AND NEW QUESTIONS

The PROG Rules represent one of India's most significant attempts to regulate the online gaming ecosystem through a dedicated national framework. By creating a specialised regulator, introducing structured classification mechanisms, and embedding user-protection obligations into platform governance, the Rules seek to balance innovation with accountability.

Yet the concentration of authority within OGAI raises issues around regulatory discretion, transparency, and consistency in decision-making. Compliance requirements could also affect smaller operators and emerging gaming businesses differently from larger, well-resourced platforms.

ENFORCEMENT THROUGH FINANCIAL INFRASTRUCTURE

The Rules also strengthen enforcement by involving the financial ecosystem.

Banks, payment intermediaries, and payment systems may be required to cooperate in preventing or disrupting financial transactions associated with prohibited online money games. This potentially gives regulators a stronger enforcement mechanism by targeting the payment architecture that enables unfair platforms to operate.

Proceedings are designed to be conducted largely through digital processes, with penalties taking into account factors such as scale, unfair gain, and user harm.



Ultimately, the long-term success of India's online gaming framework will depend not only on the text of the Rules but on how fairly, predictably, and transparently they are implemented in practice.

VISUAL INTELLIGENCE

MAPPING THE SYSTEMS BEHIND DIGITAL GAMING

01 INDIA'S GAMING ECOSYSTEM

India's gaming ecosystem extends far beyond entertainment. It now intersects with governance, digital payments, cybersecurity, data privacy, artificial intelligence, and platform accountability. This visual map highlights the major sectors driving the industry and the governance challenges shaping its future.



02 THE ANATOMY OF A GAMING

Modern gaming applications operate as interconnected digital ecosystems. Behind gameplay lies a complex infrastructure involving advertising networks, analytics systems, AI recommendation engines, cloud services, payment gateways, and social integrations. Each layer creates opportunities for innovation while also introducing privacy, security, and governance concerns.



The modern gaming ecosystem is defined by more than solely play:
by platforms, policy, and data.

3

WHO GOVERNS GAMING IN INDIA?

The governance of online gaming in India is distributed across multiple institutions, including central ministries, state governments, courts, regulatory bodies, payment systems, and digital platforms. This fragmented framework reflects the growing complexity of regulating gaming, taxation, cybersecurity, child safety, and platform accountability in the digital age.



A DAY IN THE LIFE OF A GAMER'S DATA

Every interaction within a gaming platform generates data. From logging in and voice chats to in-app purchases and social sharing, gaming ecosystems continuously collect behavioural, financial, and interaction-based information. This data powers recommendation systems, monetisation models, targeted advertising, and platform engagement strategies.



In digital gaming ecosystems, data becomes as valuable as gameplay itself.

EXPERT SPEAK

INTERVIEW WITH MR SHAILENDRA VIKRAM SINGH

Shailendra Vikram Singh is a technology policy and national security professional with extensive experience at the intersection of digital governance, cybersecurity, public policy, and emerging technologies. During his decade-long tenure with the Ministry of Home Affairs (MHA), Government of India, he contributed to policy formulation and governance frameworks relating to online activities, digital platforms, public safety, and compliance oversight. His work focused on addressing emerging challenges in the digital domain from a national security, law enforcement, and public safety perspective.

He currently works with industry while collaborating closely with governments, regulators, and other responsible agencies to promote a secure, trusted, and resilient digital environment. His areas of engagement include cybersecurity, government, and artificial intelligence, cloud computing, critical digital infrastructure, online gaming, digital platforms, intermediary governance, fintech, digital payments, and privacy and data protection frameworks. He actively contributes to policy dialogue, regulatory engagement, and compliance initiatives relating to emerging technologies, digital trust, platform accountability, and security governance with a focus on collaboration while strengthening online public safety, and national security outcomes. CyberPeace spoke with Mr Singh to explore how gaming is evolving beyond recreation into a complex digital ecosystem shaped by social interaction, technology, security, governance, and policy considerations. He can be reached on LinkedIn at:

in.linkedin.com/in/shailendra-vikram-singh-a9579219
and email: svsbsf@gmail.com

Key excerpts from the interview:



PLAYING FOR TOMORROW

BUILDING SAFER, SMARTER AND MORE TRUSTED GAMING ECOSYSTEMS

As gaming platforms increasingly evolve into social spaces rather than merely entertainment, how should policymakers and industry leaders rethink user safety in this ecosystem, given their popularity among minors and young adults?



Gaming platforms are no longer simply entertainment products; they have evolved into digital social spaces where millions of users communicate, collaborate, transact, and build communities. This transformation requires policymakers and industry leaders to rethink user safety beyond traditional content moderation.



Safety-by-design should become a foundational principle. Platforms should incorporate age-appropriate experiences, parental controls, privacy safeguards, reporting mechanisms, and proactive detection of harmful behaviour from the outset rather than as afterthoughts. Given the significant presence of minors and young adults, special attention must be paid to cyberbullying, grooming risks, harassment, fraud, and exposure to harmful content.



Equally important is recognising that gaming platforms increasingly function as large-scale communication ecosystems. Voice chats, private networks, and some online platforms can create unmonitored channels that may be vulnerable to misuse for criminal activity, radicalisation, recruitment, misinformation, or other harmful activities. While privacy must be respected, platforms should adopt appropriate user authentication measures, risk-based monitoring mechanisms, and metadata retention practices consistent with applicable laws and due process requirements to prevent security violations and enforcement investigations, and national security objectives.



India's gaming landscape incorporates elements of technology, finance, cybersecurity, and culture. In your view, what are the most significant governance or regulatory challenges that will shape the sector over the next five years?



The most significant governance challenge over the next five years will be balancing innovation with trust and security. Gaming today sits at the intersection of technology, finance, cybersecurity, culture, and social interaction, making governance increasingly complex.



Key issues will include user safety and child protection, cybersecurity and data governance, AI-driven engagement practices, and the misuse of gaming platforms for fraud, criminal activities, radicalisation, or other harmful behaviour. As gaming platforms increasingly function as communication ecosystems, policymakers will also need to address questions around authentication, accountability, and lawful access while respecting user privacy.



At the same time, India may avoid viewing gaming solely through a compliance lens. The large opportunity lies in fostering innovation, indigenous IP creation, and culturally rooted digital experiences. Ingathering and AI-powered gaming will be developed to develop a governance framework that enables growth and competitiveness while ensuring trust, safety, and security.



BALANCING INNOVATION AND RESPONSIBILITY

With the rise of AI-driven behavioural analytics and monetisation strategies in gaming, where should the line be drawn between user engagement and manipulative design practices, particularly for younger audiences?

The line between engagement and manipulation is crossed when technology begins exploiting behavioural vulnerabilities rather than enhancing user experience. AI can undoubtedly make gaming more immersive, personalised, and enjoyable, but it should not be used to encourage excessive spending, unhealthy screen time, or addictive behaviours, particularly among minors.

As AI-driven behavioural analytics become more sophisticated, transparency and accountability become increasingly important. Users should have a clear understanding of how recommendations, rewards, and monetisation mechanisms influence their choices. Special safeguarders are also necessary for younger audiences, who may be more susceptible to persuasive design techniques.

The objective should not be to limit innovation but to promote responsible innovation. AI should be used to improve gameplay, accessibility, safety, and user experience, while ensuring that engagement remains ethical, transparent, and respectful of user autonomy.



India is simultaneously positioning itself as a major AVGC and gaming innovation hub while also debating questions around taxation, compliance, and platform regulation. How can the country balance innovation with responsible digital governance?

India's gaming story presents a unique paradox. While the country is positioning itself as an AVGC and gaming innovation hub, much of the tech-powered industry is subject to regulatory oversight. In my view, user safety, responsibility gaming, and game development are key objectives, but governance frameworks must also recognise gaming's broader role as a driver of innovation, creativity, digital skills, and economic growth.

The challenge is to ensure that regulatory authorities and frameworks remain proportionate to the risks being addressed. While gaming evolves into a mainstream digital economy, the risk-based approach that distinguishes between different categories of gaming services is evolving, and unregulatory compliance becomes a key consideration for governments and burdens that could discourage investment, innovation, and indigenous IP creation. Equally, the predictability and globally competitive tax framework that supports long-term growth while ensuring appropriate regulatory oversight.

At the same time, India should focus on enabling the larger AVGC vision through targeted support for game development, skill development, research, startup ecosystems, and culturally rooted content creation. This is particularly important given the opportunity to showcase India's cultural and historical narratives to global audiences through interactive digital experiences.

Strong safeguards for cybersecurity, child protection, user safety, and data governance will remain essential. However, long-term success will depend on achieving the right balance between regulation and innovation. India's ambition should not be limited to being one of the world's largest gaming markets; it should be to become a leading global hub for gaming creation, innovation, and trusted digital experiences.

ONLINE GAMING PLATFORMS HAVE INCREASINGLY BECOME SPACES WHERE ISSUES SUCH AS TOXICITY, HARASSMENT, HATE SPEECH, AND HARMFUL ONLINE BEHAVIOUR EMERGE ALONGSIDE COMMUNITY BUILDING AND SOCIAL INTERACTION. IN YOUR VIEW, WHAT RESPONSIBILITY SHOULD GAMING PLATFORMS, REGULATORS, AND USERS SHARE IN CREATING SAFER AND MORE INCLUSIVE DIGITAL GAMING ENVIRONMENTS?



In my view, creating safer and more inclusive gaming environments requires a shared responsibility framework involving platforms, regulators, users, and parents. As gaming increasingly evolves into a social and community-driven digital ecosystem, safety cannot be treated as the responsibility of any single stakeholder.



Platforms have the primary responsibility to embed safety-by-design principles into their services through effective moderation tools, age-appropriate safeguards, reporting mechanisms, parental controls, and measures to address harassment, hate speech, fraud, and other harmful behaviour. They should also invest in transparency, accountability, and user awareness.

Regulators, on the other hand, should focus on establishing clear principles around user safety.



Child protection, cybersecurity, data governance and grievance redressal while ensuring that regulatory approaches remain proportionate and innovation-friendly.



Users also have an important role to play. Promoting digital citizenship, responsible online behaviour, and awareness of online risks is essential to building healthy digital communities. Parents and educators can further contribute by fostering digital literacy and responsible engagement among younger users.



Ultimately, the goal should not merely be to reduce harm, but to create trusted, inclusive, and resilient digital environments where innovation, community-building, and user wellbeing can thrive together.



DID YOU KNOW?

The global gaming industry is larger than the film and music industries combined.

Source: Global entertainment and media industry revenues to hit **US\$3.5 trillion by 2029**, driven by advertising, live events, and video games: PwC Global Entertainment & Media Outlook



\$3.5 TRILLION
Market Size by 2029



HIGH GROWTH
Across Platforms



3+ BILLION
Global Gamers



GAMING INFLUENCERS

THE NEW ARCHITECTS OF DIGITAL CULTURE

-ANUPMA PRAKASH SRIVASTAVA

The global gaming industry is expected to reach USD 350 billion in revenue by 2030. At the centre of this growth is a new type of digital creator, the gaming influencer, whose role has changed from just entertainment. These influencers shape consumer behavior, drive viral trends, and are an important link between game developers and their audiences. By changing what was once a solitary hobby into a community experience, gaming influencers have transformed how millions engage with digital culture.



REVENUE STREAMS: HOW GAMING INFLUENCERS MONETISE THEIR PLATFORMS

The rise of social media has not only increased the reach of gaming content but has also created a variety of ways for creators to earn money. The main revenue streams include:



SPONSORED CONTENT AND BRAND PARTNERSHIPS:

Integrating gaming brands and products into content is still one of the most profitable options for established creators. This offers both direct payments and long-term benefits.



MERCHANDISE AND DIGITAL PRODUCTS:

Influencers with dedicated audiences often generate extra income through branded merchandise, strengthening their identity both in and out of the gaming world.



PAID SUBSCRIPTIONS AND MEMBERSHIPS:

Exclusive content for members through subscription tiers creates a steady income, providing financial stability along with fluctuating advertising revenue.



SPEAKER ENGAGEMENTS:

The credibility that comes with a well-known gaming brand often leads to invitations to stand at industry conferences, exhibitions, and workshops.



COMMUNITY EVENTS AND WORKSHOPS:

Hosting paid sessions for subscribers, which can range from gameplay clinics to digital skill workshops, allows creators to engage more with their audiences while diversifying their income.

“They don't just play the game. They shape how the world plays.”



**INFLUENCE. ENGAGE.
EARN. REPEAT.**

GLOBAL REACH: TOP GAMING CREATORS

BY PLATFORM

Spanish-language gaming creators attract a surprisingly large global audience compared to their linguistic reach, mainly due to high visual appeal, expressive styles, and content that goes beyond language barriers.



MrBeast Gaming (Jimmy Donaldson): One of YouTube's most subscribed gaming channels, with over 10.9 billion total views. MrBeast Gaming stands out due to its large-scale production, high viewer engagement per video, unique and high-quality branding, and giveaways that serve as entertainment and marketing. The channel has moved from just commentary to original game development, having two widely played mobile titles.



MikeCrack (Miguel Bernal Montes): A Spanish language creator with over 21.8 billion total views, MikeCrack gained his audience through Minecraft and Roblox gameplay aimed at families and younger viewers. His signature character, a bright yellow dog named Mikey, has become a recognizable brand in its own right, demonstrating how strong character design can build a creator's commercial identity.



JuegaGerman (Germán Garmendia): A Chilean creator and Guinness World Record holder for the most subscribers on a non-English YouTube channel, MikeCrack is known for his high-quality content, based on relatable humor and everyday life observations, has evolved from variety gaming to broader entertainment, maintaining a loyal audience across both formats.



GLOBAL REACH: TOP GAMING CREATORS BY PLATFORM

India's gaming influencer scene began to grow around 2017, fueled by affordable smartphones, cheap mobile data, and the arrival of PUBG. The COVID-19 lockdowns in 2020 sped up this growth, pushing gaming content into the mainstream and allowing several Indian creators to build large audiences.



Total Gaming (Ajendra Variya — 'Aju Bhai'):

With 45.7 million subscribers and over 5.1 billion total views, Total Gaming is one of India's largest gaming channels. Known for Free Fire gameplay and consistent family-friendly, the channel's branding has been supported by regular content updates, personal audience interactions, and a reputation for clean, approachable content.



Techno Gamers (Ujjwal Chaurasia):

Across his various channels — Techno Gamer, Ujival, and Ujival Shorts. Ujjwal Chaurasia has over 7+ million active subscribers and 10+ streams of reviews. His cinematic GTA roleplay series and survival gameplay, presented in accessible Hindi with consistent humor, helped introduce a generation of Indian viewers to long-form gaming content. Early tutorials were created in Brazil and mobile gaming greatly promoted his initial subscriber growth.



CarryIsLive (Ajey Nagar):

With 12.4 million subscribers and 1.8 billion total views, CarryIsLive benefits from the existing loyal audience of CarryMinati, Ajey Nagar's primary roasting channel. The gaming channel streams titles like BGMI, Valorant, and Resident Evil, and is known for live audience engagement and charity fundraising through streaming events.



(All subscriber and view data recorded as of 30 May 2026.)

FORMATS THAT DRIVE GAMING CONTENT

Today's variety of gaming content reflects both the many platforms available and the different ways audiences consume digital media.



LONG-FORM CONTENT:

In-depth walkthroughs, tutorials, strategic guides, and narrative essays make up long-form gaming content. Mostly distributed through YouTube, this format serves both entertainment and educational purposes, helping players navigate complex games and gain specific knowledge.



SHORT-FORM CONTENT:

Short clips, highlight reels, and funny edits optimized for TikTok, Instagram Reels, and YouTube Shorts keep audiences engaged between longer viewing sessions and attract new viewers who may not be familiar with a creator's longer content.



LIVESTREAMS:

Live gameplay streamed to audiences allows for direct interaction between creators and viewers. This fosters a sense of community and a shared experience that sets gaming content apart from traditional media consumption.



GAME REVIEWS AND CRITIQUES:

Honest, independent reviews of newly released titles are important for gaming communities. They help inform purchasing decisions and hold developers accountable for quality.



DID YOU KNOW?



India is among the world's fastest-growing markets for gaming content consumption on YouTube and livestreaming platforms.

Source: From: *Recreation and Revenue: How Gaming Is Redefining Careers in India*



CONCLUSION »

The gaming influencer economy is one of the most dynamic parts of the broader creator industry. Successful channels require constant creativity, awareness of audiences, and the ability to adapt across formats and platforms. The most lasting creators have established identities—through character, language, tone, or community—that go beyond any single game or trend. As esports continues to become more professional and India's gaming market matures, the impact of gaming creators on consumer behaviour and cultural discussions will deepen. The challenge for individual creators, and for the ecosystem as a whole, remains the same: keeping audience engagement without crossing the line from entertainment into dependency.



GAMING INFLUENCERS HAVE EVOLVED BEYOND CONTENT CREATORS INTO CULTURAL INTERMEDIARIES WHO SHAPE PURCHASING DECISIONS, PLATFORM TRENDS, GAMING COMMUNITIES, AND PUBLIC PERCEPTIONS.

SAFEGUARDING THE DIGITAL CITIZEN

THE ECONOMIC IMPACT OF THE REAL-MONEY GAMING BAN

- DR JULIAN SEAL PASARI, AVINASH VERMA

The online gaming industry in India saw a compound annual growth rate (CAGR) of 28% in FY20–FY23. Industry projections have also been optimistic with the market expected to reach INR 33,243 crore by FY28 with 15% CAGR, while the India Brand Equity Foundation (IBEF) forecast a market size of INR 77,688 crore by 2029, approximately US\$9 billion in dollars. By any measure, the sector has been touted as the next big thing.

There is, however, a lot more to the numbers. Behind the numbers lies a darker reality of debt-ridden households, the psychologically preoccupied young, and capital that consistently cascades into the offshore and parallel world. In this era of online gaming growth, many of India's players moved from fun to a much more serious and dangerous sport: real-money gaming (RMG) that plays on some fine and often intentionally thin hairs of skill versus chance.

The Indian Parliament's solution to this issue is the Promotion and Regulation of Online Gaming Act, 2025 (the Act or PROGA), which was assented to by the President on 22 August 2025. The Act doesn't just tweak the current regulatory framework; it breaks down the financial support system on which the RMG platforms have been constructed and simultaneously aims to carve out a safe, development-centric area in the world of esports and social gaming. This article maps the mechanism by which gaming gets transitioned into monetary harm, examines the proposed blockade facility that PROGA introduced, and assesses whether the new regulatory setting can truly help channel the gaming economy in India towards a safer and more sustainable trajectory.



Gaming regulation has economic consequences that extend well beyond gaming platforms themselves.



28%

CAGR
(FY20–FY23)



INR 33,243
crore
by FY28



INR 77,688
crore
by 2029
(~US\$9 Billion)



WHEN GAMING BECOMES GAMBLING:

THE MECHANICS OF FINANCIAL HARM



Regulation begins at the design phase. With the growing popularity of modern video games, especially those that are mobile and are targeted at Indians, there has been an increasing number of monetisation features embedded in games that have been proven to exploit psychology. At the heart of this worry are microtransactions and loot boxes.



A loot box is a digital “mystery bundle” to be purchased in-game, delivering randomised virtual rewards like skins, weapons, characters, or in-game currency. The mechanic mirrors a slot machine: a small, uncertain payment for a random outcome. In a 2018 study, DL King and PH Delfabbro argued that these schemes qualify as “predatory monetisation” because they exploit variable-reward conditioning, the same psychological mechanism that underpins gambling, while being embedded in games otherwise framed as skill-based entertainment. Their analysis found that the commercial incentive to maximise in-game revenue had led developers to design mechanics that prioritise compulsive spending over player welfare.

In 2024, a study published on PMC explored the correlation between microtransaction engagement and problem gambling, and found a statistically significant relationship between spending money regularly on in-game content and gambling-related harm. Microtransactions serve as a gateway for a relevant group of users; they make it commonplace to pay for uncertain rewards, and, in time, reduce the psychological barrier to the use of real-money games.



All of this has taken a toll. According to a 2025 study by Csrbox, online RPGs resulted in an estimated Rs 87,000 crore loss of revenue to the nation and 56 days a year of lost employable days.



per individual online RPG user. It is not money that has been lost; it is money that has been put into other things. It has been diverted from household savings and education investments, and redirected towards gaming platforms – even offshore ones – that are beyond India’s regulatory control.



The study also showed increased psychological distress, disrupted family life, and found that young and middle-class users are disproportionately more likely to suffer from addiction, the very segment that the Indian digital economy is banking on as its productive force. The results of the CSRBOX study are used to inform the deliberations of lawmakers and are included as part of the factual evidence for PROGA.



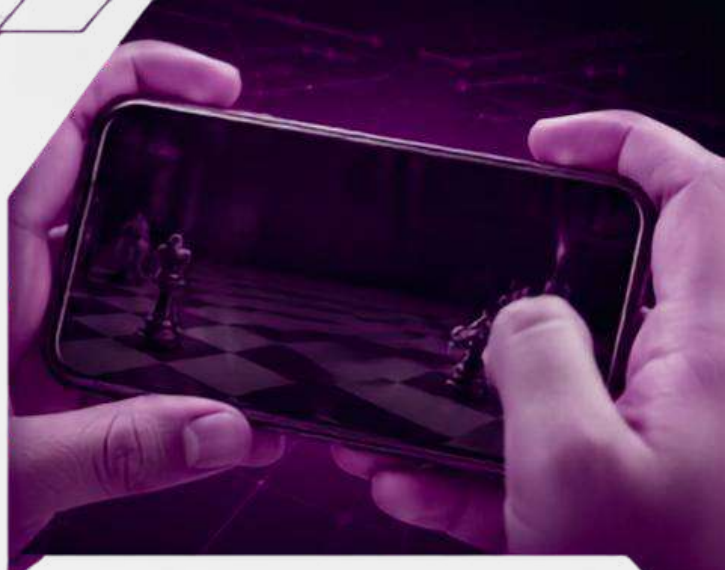
But there is a compelling argument to be made for the fact that many fantasy sports sites are actually a mixture of skill, statistical analysis and sports knowledge and that blanket regulation does not differentiate between what is a proper game of skill and what is just a straight bet. As of 2024, there were around 155 million players engaging in paid gaming in India. There is no question of harm. It does cause harm, in fact, according to the evidence. What is being called for is a proportional policy response.



From a cost-effect perspective, TS Ulen’s research on gambling regulation leads him to conclude that prohibition should be justified if the social costs of a game are larger. The game is 1080 x 1080 pixels. The game is marketed in the household financial difficulties, mental ill health, and losses in learning from productivity reductions – are greater on the whole than the private benefits. In the Indian context, the annual cost of Rs 87,000 crore and 56 days of employable labour for every user is significant.



EVALUATING THE 2025 ACT



PROGA is a conscious policy decision. India decided to strike at the financial level, in contrast to domain-level blocking, which could be easily bypassed with the help of VPNs or mirrors sites. Three provisions are carrying the load.

Section 5 introduces the blanket ban on online money games and real-money games. Section 6 imposes advertising and promotion bans on all media for such games, eliminating marketing channels that help acquire users. The ban on these games are applicable to banks, financial institutions, and payment processors like UPI. The actual payment system now becomes the regulatory gatekeeper.



This is not domain blocking, however, as it prevents an offshore platform's ability to collect money without barring access to the platform itself. This "financial-first" approach is a reflection of a real regulatory void, as foreign operators have for years been capable of catering to Indian users without any Indian law enforcement intervention.



The counter-argument is that the Act is not a calibrated intervention, it is a blunt instrument. A number of major skill-gaming firms such as A23 Games (Head Digital Works) and Clubboom 11 Sports have petitioned the Supreme Court seeking to strike down the blanket ban under Article 14 and 19(1)(g) of the Indian constitution, claiming that the blanket ban does not differentiate between the games of chance and skill-based games. The distinction between skill and chance has been tested in Indian courts for decades, and a blanket ban that presumes a similar level of regulatory seriousness in fantasy gaming as in online poker is not proportional.



The economic shock has already been huge. Services by banks, payment gateways and intermediaries were instantly discontinued upon the publication of PROGA on 22 August 2025, due to the fear of penal consequences under Section 7. All UPI transactions were blocked, settlements were frozen, and Head Digital Works announced a reduction of its workforce from 606 to 178 employees within a few months.



There is an aspect for comparison. The European Union is tackling online gaming with licensing, stringent consumer protection regulations, and anti-money laundering controls, and allows skill-based and real-money games to be played as long as they are properly protected. The U.S. has a "fractured" state-based model. India's 2025 Act, in contrast, has a central prohibition that is uniform and more restrictive than most of its international counterparts and is possibly less precise. A staged, multi-level process, in which different formats are separated, where KYC is rigorously enforced, and where operators who comply with the rules are licensed, could have had the same protective effect, but with less collateral damage for legitimate businesses.



But, on the other hand, the Act is commendable for addressing a structural issue that had not been adequately addressed by the hitherto existing patchwork of state-level gambling laws, which are based on the Public Gaming Act, 1867. This is a structure that was not conceived for the internet. PROGA might have scope for improvement, but its objectives are to create a unified national framework. It's too early to tell which will be more effective over time, prohibition or regulated licensing, but the goal of shielding middle-class and youth consumers from predatory digital extraction can hardly be faulted on principle.



The Act also introduces the Online Gaming Authority of India (OGAI), comprising six members of an inter-ministry regulatory committee under the Ministry of Electronics and Information Technology, which will categorise games, settle grievances, and ensure compliance. Over time, a well-resourced and technologically advanced OGAI might evolve into a more sophisticated regulatory model that would eventually move beyond prohibition to a more nuanced form of oversight.

BEYOND THE BAN: ESPORTS AND SOCIAL GAMING AS INDIA'S DIGITAL FUTURE

PROGA's ban is an indication of what India is shutting down. The way it treats esports and social gaming gives an indication of what India is actively working towards.

The Act officially draws the distinction between esports and money games. For the purposes of PROGA, the term 'esports' is used to describe any form of multiplayer game that has a competitive element and is played based on physical agility, mental sharpness, or strategic gameplay rather than luck or monetary bets. This is a very important distinction because it lifts the 'gambling stigma' that has traditionally impeded commercial investment in the sector and provides greater regulatory certainty for sponsors, broadcasters, and foreign investors to commit capital.

The market data is in line with this pivot. India's esports market reached a valuation of USD 247.97 million in 2025 and is expected to grow at a CAGR of around 18.80% till 2035, reaching a value of USD 1.38 billion by 2035. More than 61% of esports revenue comes from sponsorships and advertising, and by FMCG, automotive, BFSI and telecom brands seeking to reach India's digitally native youth population. Now that the curtain has been lifted on the regulation of industry, and the stigma of money gaming has been officially removed, there's a strong argument that investment in esports will ramp up.

India funding. Ved "Beelzeboy" Bamb was the first Indian to become the World Champion of Pokemon GO in October 2025. It's a small-scale proof of concept, but a proof of concept. Indian players can play at the highest level in the world, with the institutions in place to help them do so.

Games in which there is no wagering, but rather a social, recreational or educational purpose, are known as social games, and PROGA mandates that platforms provide age verification, screen-time warnings and parental controls. These are consumer protection measures that are best practices around the world and a clear effort towards having a gaming ecosystem in India that is sustainable.

The question being raised is whether the esports-and-social-gaming model can replace the economic activity that RMG was able to generate. Of the 155 million paid users of RMG platforms, not everyone will move on to skill-based competitive gaming, making this an important user base. Some, as Reuters reports, may simply relocate to offshore platforms that are not regulated and, without the user protections required of domestically registered operators, cannot be held accountable for harm. This regulatory risk is genuine and is the strongest call for complementary measures of enforcement at the app store and payment gateway level.



The trajectory was already underway prior to PROGA. The Ministry of Youth Affairs and Sports officially included esports in the multi-sports events category in December 2023, giving competitive gamers access to the Sports Authority of India (SAI) for infrastructure provision and training, and Khelo

But the long-term logic still holds. Capital and talent that were otherwise diverted to the RMG platforms can now be channelled into the building of competitive gaming infrastructure, original intellectual property, and internationally-oriented studios.

CONCLUSION



At the end of the day, PROGA is about India's vision of creating a digital economy. The macro numbers – the 28% CAGR, the INR 33,243 crore projected market size – are real and represent true value creation. Economic growth based on the financial insecurity of the middle class and the susceptibility of young consumers is not the kind of growth that's responsible state should celebrate or be a part of. PROGA takes a strong and, in some ways, extreme position against that model. It's a global-first, innovative approach to confront what traditional domain blocks don't offer. The creation of the OGAI provides at least the skeleton of a mature regulatory authority. It's a formal acceptance of esports and social gaming, suggesting that India isn't looking to do less, but rather to do something different.



The Act is not without its flaws. The blanket prohibition on RMG, without a careful carveout for demonstrably skill-based formats, has caused collateral economic damage that is difficult to justify in purely consequentialist terms. The Supreme Court petitions pending against PROGA raise legitimate constitutional questions about proportionality and the right to practice lawful trade, and the risk of becoming addicted users toward offshore, unregulated platforms is a concern that enforcement alone may not be sufficient to address.



PROGA as a whole points to a regulatory stance that the Global South has yet to clearly articulate and has been even slower to act on: the Global South's story of the success of the digital economy is not to be measured by revenue numbers. Citizens' financial safety is an economic variable, as is access to it for young and economically vulnerable citizens -it impacts productivity, human capital development, and domestic demand in the long term. A game industry that profits off its users, but doesn't benefit them, is, at the end of the day, not an asset to a digital economy.



The success of PROGA will depend on the performance of OGAI, the enforcement of payment-layer restrictions, and the development of an evidence base to support an alternative licensing model to replace the blanket ban. If these conditions hold, India may well have produced the blueprint in a regulatory playbook for other Global South economies seeking similar solutions.



More than any one aspect of this debate, this demonstrates that innovation and protection are not mutually exclusive, and that a billion-dollar industry can be built on foundations that do not require the exploitation of the people it serves.



The regulation of real-money gaming sits at the intersection of consumer protection, economic growth, taxation, and public health. This article explores the potential consequences of restrictive regulatory approaches on industry development, employment, investment, and user behaviour.



ADDICTIVE GAME DESIGN AND CHILD SPENDING IN ONLINE GAMING

THE ECONOMIC IMPACT OF THE REAL-MONEY GAMING BAN



Dark Patterns in Gaming: Mapping the Existing Prohibitions

-RAHUL KUMAR, CIPPE AND
ISO/IEC 27001 AUDITOR

Issued by the Central Consumer Protection Authority (CCPA) under the Consumer Protection Act, 2019, the Guidelines for Prevention and Regulation of Dark Patterns, 2023 establish a regulatory framework aimed at curbing manipulative digital design practices. The Guidelines under Section 2(e) define dark patterns as "user interface designs that trick users into taking decisions contrary to their interests." Several enumerated categories are designed to limit the resale of online games to prevent monetisation under Annexure 1 of the Guidelines.



False Urgency operates through features such as countdown timers, limited-edition cosmetics, and seasonal battle passes. A documented 2021 case reported a Mumbai teenager who spent Rs 10 lakh from his mother's account on PUBG, driven primarily by time-limited exclusive skins and seasonal events; creating a circumstance of artificial scarcity pressure. This mechanism directly fits within the Guidelines' false urgency category.



Nagging manifests through persistent in-app purchase popups such as: "claim now" reward reminders, upgrade notifications, and other continuous prompts that are designed to effectuate transactions. These repetitive interactions constitute the obstruction mechanism that is outlined in the Guidelines.



Interface Interference includes misleading purchase flows, such as bright "Buy Now" buttons paired with hidden "Skip" options, ambiguous pricing, and streamlined payment pathways that reduce friction. In 2020, a Delhi teenager's Rs 2.23 lakh PUBG expenditure involved purchases that were facilitated by an opaque interface design, constituting a clear interface interference violation.



Drip Pricing potentially applies when games are initially presented as free, but progressively restrict meaningful gameplay behind mandatory payments. However, applicability of this design can become uncertain if the core gameplay remains accessible.



The interpretive challenge presented here is significant, i.e. whether Annexure 1's enumerated examples are exhaustive or illustrative, and whether Section 2(e)'s catch-all provision that states — "any practice" (impairing informed decision-making), extends to behavioural monetisation systems beyond the deceptive interface design.



THE DPDP GAP: DATA PROTECTION IS NOT BEHAVIOURAL PROTECTION



WHERE THE DARK PATTERNS FRAMEWORK FALLS SHORT

India's Digital Personal Data Protection Act, 2023 establishes critical safeguards for children: it mandates parental consent before games collect, process, or share children's personal data. However, this framework addresses only data protection, and not behavioural manipulation. Thus, a fundamental gap exists: the DPDP compliance does not prevent a game from employing dark patterns, even with verified parental consent.

Consider this practical mechanism: A parent consents to a game that collects their child's gameplay patterns, engagement metrics, and spending habits under the DPDP requirements. The game then uses this consented data to algorithmically personalise time-limited offers, matching spending psychology with individual engagement patterns. A teenager spending Rs 16 lakhs on PUBG demonstrates this dynamic: although parental consent on data collection may have been obtained, yet the game's algorithmic exploitation of behavioural vulnerabilities remained largely unaddressed.

The dark pattern operates at the behavioural manipulation layer, not at the data collection layer. Consequently, DPDP safeguards become functionally irrelevant to the actual harm mechanism. Regulators, therefore, cannot rely on the DPDP compliance as a proxy for dark pattern prevention. Although both frameworks must operate in tandem, yet neither fully addresses the point at which behaviour manipulation and data protection converge.

Although the Guidelines effectively address deceptive interface design, they remain insufficient for sophisticated behavioural monetisation systems. Modern game designs rely heavily on reward conditioning, algorithmic personalisation, and psychological engagement mechanisms that operate beneath interface transparency. These are not primarily UI (User Interface) tricks, but architectural choices that determine how reward systems, progression mechanics, and algorithmic targeting intersect to create an environment for compulsive spending.

The convergence of DPDP-compliant data processing and dark pattern design mechanics reveals the framework's limitations wherein behavioural architecture escapes current oversight.



“Protecting data is essential.
Protecting **behaviour** is the next frontier.”

CLOSING THE INTERPRETIVE GAP: REGULATORY CLARITY, NOT NEW LEGISLATION

“

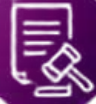
Rather than new regulations, three clarification mechanisms would substantially strengthen enforcement.



01

EXPLICIT GUIDANCE ON BEHAVIOUR ARCHITECTURE.

The Ministry should issue advisory guidance clarifying that the dark pattern definition extends beyond interface deception to encompass sophisticated behavioural monetisation systems, including algorithmic personalisation of offers, reward conditioning, and engagement-driven architecture.



02

INTERPRETATION OF SECTION 2(E).

Regulators should confirm that the catch-all provision extends to behavioural design patterns that fall outside the enumerated categories. Such a clarification would address the existing uncertainty regarding whether Annexure 1 is intended to be exhaustive or merely illustrative.



BALANCED ASSESSMENT

The Guidelines do possess sufficient conceptual scope which is required to address gaming-related dark patterns. Multiple prohibited categories demonstrably operate within gaming monetisation, as illustrated by documented cases. The practice is known as regulatory absence. Instead, it pertains to enforcement ambiguity and the interpret relationship between interface-level deception (clearly consistent with behavioural level administration (less clearly addressed)).

Critically, DPDP and the dark patterns framework operate on separate tracks, as data protection compliance does not guarantee behavioural protection. Accordingly, regulators must coordinate these frameworks in order to prevent games from exploiting parental-consentive data and misusing it for dark pattern manipulation.



CONCLUSION

India's dark pattern framework contains adequate tools to address addictive game design. The path forward does not require new legislation; instead it demands regulatory clarity on how existing frameworks are to be coordinated between DPDP and dark pattern enforcement. Early enforcement precedent of Ministry advisory guidelines was established in 2000, and the appropriate regulatory tools exist between data protection consent and behavioural protection.

The question before policymakers is: whether to actively interpret and apply existing frameworks to the behavioural architectures that are responsible for shaping India's rapidly growing gaming sector.



DID YOU KNOW?

Several countries now require disclosure of loot-box odds or have restricted their use for minors.

Source: [Global review of assessments of online video gaming policies affecting young people: Loot boxes, age ratings, gameplay time restrictions, and beyond - ScienceDirect](#)



COMPLIANCE CHECKLIST

FOR ONLINE GAMING

PLATFORMS

WHAT COMPANIES NEED TO
BUILD, MONITOR, AND MAINTAIN

-ISHARTH KUMAR,
NLIU BHOPAL



India has ushered in a new era for online gaming. The Act for Promotion and Regulation of Online Gaming (PROG) 2025, passed by Parliament in August 2025, along with the PROG Rules, 2026, came into force from 1 May 2026, and it establishes India's first national regulatory regime for online gaming. The new, centralised body, the Online Gaming Authority of India (OGAI), functioning as an attached office under MeitY, now serves as the only regulator in the gaming sector.



Operators, whether online gaming platforms or hybrid formats, can no longer sideline compliance, as it is now a condition precedent for registration. The five-pillar checklist below discusses the foundations each platform will need to sustain its business with the best industry practices.



As regulatory expectations grow, compliance is becoming a core business function rather than a legal afterthought. This article provides a practical overview of governance, user safety, grievance redressal, payments compliance, and platform accountability requirements.



ISO 31000 BEST PRACTICES

These are principles that must be followed while integrating compliance obligations across the whole value chain avoid becoming a requirement. In the context of enterprise risk management, in the context of the online gaming industry, these principles emerge:



RISK IDENTIFICATION BEFORE LAUNCH:

A systematic risk assessment of every new game feature, payment feature, or other customer-facing change is to be carried out before launch.



PROPORTIONALITY:

The level of controls deployed is to match the level of risk exposure



CONTINUAL IMPROVEMENT:

Regular review periods to be functionised



INFORMATION SECURITY GOVERNANCE:

The OGAI could seek to implement controls covered by ISO/IEC 27001. This should assure OGAI and other stakeholders that practices have been assessed to the highest standard.



ACCOUNTABILITY:

The PROG Rules, 2026, designate a Grievance Officer to operationalise accountability



DOCUMENTED TREATMENT PLANS:

All identified risks need to have a clearly documented treatment plan (avoid, reduce, transfer, or accept), including the ownership and review date of the identified risks.



KEY PILLARS

PILLAR A: USER SAFETY FEATURES

"User safety features" have been defined by Rule 2(1)(i) of the PROG Rules, 2026 to mean "a mechanism that relates to the technological, procedural, operational, behavioural or systems aspect of the game and is commensurate with the risks posed by each game".



Key elements to build:

	Age verification & age-gating	▶ Rigorous KYC at onboarding is an absolute must. The Gambling Commission in the UK has made age verification mandatory prior to play and it's likely India will move towards a similar direction.
	Parental Controls	▶ Parents or guardians should be empowered with easy-to-use tools to be able to block, monitor, or disable access to a child.
	Time Restrictions & Usage Limits	▶ Set up session time caps, cooling-off reminders, or daily limit tools as mandatory provisions. Australian regulators, under the South Australian Gambling Commissioner's Licensee Checklist , mandate self-exclusion and spending limit tools as basic requirements.
	In-app user reporting tools	▶ Players should be empowered to report bad content, dubious activity, or behaviour directly from the platform's interface and not rely on email channels.
	Counselling Support Integration	▶ The rules make it imperative that at-risk users be provided with access to counselling support services.
	Fair Play and Integrity Monitoring	▶ Ensure the installation of automated systems capable of detecting bot activity, collusions, and match-fixing for the purpose of fair play in esports platforms. Ensure your platform installs dedicated anti-cheat software, such as kernel-level or server-side detection engines, and get third-party annual verification
	Accessibility	▶ Platforms must comply with WCAG 2.1 Level AA for users with impairments. This will provide easier access to the reporting, grievance redressal, and safety mechanisms without any barriers for those users with visual, motor, or cognitive impairments.



What to monitor: Audit these features quarterly. Verify that age-gating has not been bypassed, that time-limit tools are functioning, and that reporting flows are operational end-to-end.

PILLAR B:

GRIEVANCE REDRESSAL MECHANISMS



PROG Rules 2026 provides a two-tier grievance structure where a user is given the right to escalate their complaint within 30 days (from resolution/non-resolution) to the platform. Should the platform's outcome be unsatisfactory to the user, Tier 2 allows the user to appeal to the OGAI, which must deliver a response within a further 30 days. The UK's Online Safety Act 2023 outlines similar requirements for accessible and transparent user complaint systems with clear turnaround times, a two-tier model that is very much analogous to India's.



KEY ELEMENTS TO BUILD:



DESIGNATED GRIEVANCE OFFICER



A clearly designated and contactable officer must be in place at each platform to receive and investigate complaints from users. This officer's name and contact information should be readily available for public viewing within the platform. The company must not use a general email inbox to manage complaints (Rule 23 of PROG Rules 2026).



IN-PLATFORM COMPLAINT SYSTEM



Users must be given the facility to submit, monitor, and receive decisions on their complaints from within the platform itself.



CLEAR TURNAROUND TIMES



Develop internal Service Legal Agreements (SLAs) that fall comfortably within the regulated timeframe—e.g., Acknowledgement within 48 hours, resolution within 15 days, and outcome communicated within 21 days.



TRANSPARENCY ON THE COMPLAINT ESCALATION ROUTE



Users must be informed at the point a complaint is concluded (or non-concluded) of their right to appeal to the OGAI. An email response from the platform stating "no further action" without indicating the appeal path would constitute a lack of disclosure.



DETAILED COMPLAINT LOG



Each platform must maintain a comprehensive log detailing every complaint received, categorising it based on issue type, the time taken for its resolution, and the overall outcome. This contributes directly to Pillar E compliance documentation.

PILLAR C:

PAYMENTS AND FINANCIAL COMPLIANCE

While the PROG Act, 2025, banned money games in their entirety, financial compliance for permitted platforms (e-sports and notified social games) becomes limited but highly scrutinized. Furthermore, Australia's Gambling Commissioner Licensee Checklist can be used to get a reference to detailed AML policies and procedures.



Key elements to build:



Payment gateway compliance and disclosure

A platform must adhere to payment facilitation directives issued as part of its licence. The platform's entire payment integration should be aligned with the RBI directives and its financial model, disclosed at the time of application, in addition to PCI DSS-12 principles, which are globally the basic requirement.



KYC/AML procedures

Since most non-money-game platforms may require entry fees, prize money, or in-game purchases, they are bound to the KYC procedures outlined under PMLA.



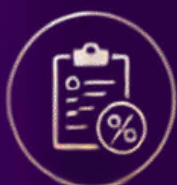
Revenue model transparency

A platform operator needs to disclose their revenue model to OGAI at the time of applying for a licence. All significant changes in revenue models must be revealed and possibly reassessed.



Review of in-game asset monetisation

The Determination Test under the Rules considers in-game asset monetisation when assessing if a game is a prohibited money game. Thus, pre-launch review of virtual currencies or any tradable item on the platform would be advisable.



GST compliance

The 28% GST applicable to certain categories of online games from October 2023 shall remain effective. Platforms need to ensure their invoicing, TDS, and filing of returns are up-to-date.

PILLAR D:

CONTENT MODERATION AND PLATFORM GOVERNANCE

PROG registration is not a one-off process; it is an ongoing governance relationship with the OGAI. Platforms have an affirmative obligation to maintain the circumstances under which they are registered.



KEY ELEMENTS TO



Determination Test Readiness



A new **objective “Determination Test”** defined in the PROG Rules measures whether any aspect of a game constitutes a prohibited money game. Your organisation should maintain an in-house legal/product review system whereby every new game mode, feature, or update is tested according to this protocol prior to launch.



Game Classification Governance



The **PROG Act categorises games as e-sports, social games, or prohibited money games**. Each of these classifications carries different compliance obligations. If your platform supports games across more than one of these categories, you'll need a classification matrix which outlines the relevant category for each supported title.



Advertising and Promotion Standards



The PROG Act proscribes the advertisement of prohibited online money games. For even permitted platforms, promotional material can not create false impressions in the eyes of the consumer about game mechanics, prize structures, or competition. (E.g. An e-sports platform promoting "guaranteed cash prizes for tournament participation" without the fine print clarifying conditions for entry, consumer protection and PROG Act risks.)



Platform Architecture Disclosure to OGAI



The OGAI may inspect the underlying mechanics of game play, payment systems and the overall architecture of the platform prior to issuing registration. For any gameplay element with a random component, an OGAI will expect to see proof of current RNG (Random Number Generator) certification from an accredited testing lab (e.g. BMM, GLI, iTech Labs). This is international best practice and is key to the OGAI scrutinizing mechanics.



Foreign Operator Responsibilities



If your company is not an Indian domestic company and supports services to Indian consumers, it will be bound by India's requirements on registration, user safety, financial transactions, and grievance resolution. A well-tested and audited geo-IP compliance system will be mandatory.

PILLAR E:

RECORDKEEPING AND COMPLIANCE DOCUMENTATION



The key connection to each pillar is the importance of documentation. Data retention orders of the OGAI must be adhered to as per PROG Rules, 2026. Penalties are scaled according to recurrence, user loss, and user remediation efforts; all to be evidenced through documentation, according to the Act.



KEY ELEMENTS TO BUILD:



COMPLIANCE REGISTER



A living document recording all relevant regulatory obligations, the status of implementation, and how the platform ensures ongoing compliance.



USER SAFETY FEATURE DISCLOSURES



Every platform applying for a determination or registration must disclose user safety features and response mechanisms clearly.



CERTIFICATE OF REGISTRATION



Every issued **Certificate of Registration** (valid for a maximum of 10 years) must be displayed prominently on a platform interface.



AUDIT TRAILS FOR AGE VERIFICATION/KYC



All age verification checks and KYC records must be retained in a form that will stand scrutiny by a regulator.



COMPLAINT LOGS



As explained under pillar B, logs, which are time-stamped, categorised, and have a recorded outcome, are a necessity, not a feature.



COMPLIANCE AUDIT SCHEDULE



As industry experts emphasise, compliance is an ongoing process. Conduct formal internal audits at least semi-annually that span all 5 pillars. Document findings and track them to closure. Obtaining SOC II Type 2 attestation to verify that the platform's controls around security, availability, and confidentiality are operating effectively will be an added benefit in proving operational trustworthiness. Use data pipelines compliant with ISO/IEC 5259 (Data Quality for Analytics and ML) when building tools that use AI for fraud detection, user analytics, moderation, etc.



CONCLUSION

The PROG Act, 2025 and PROG Rules, 2026, represent a significant turning point in Indian regulation of online gaming by bringing in transparency, safety, and responsibility as central elements. For operators, compliance is integral to business success going forward, and for platforms to develop responsible and user-friendly compliance structures is crucial.

A NOTE ON PENALTY CALIBRATION

Under the PROG Act, 2025, the punishments are proportionate and are assessed by the OGAI depending upon the level of non-compliance, benefits reaped by the infraction, user damage, repeated offenses, and the remediation applied. The single most effective mitigating factor in any regulatory action is a documented, functioning compliance program. It must be built before it is needed.



THE GAMING LEXICON

DECODING THE JARGON OF ONLINE PLAY

-HITHIKA KOHLI

In recent years, advances in immersive graphics and persistent online networks have transformed online gaming into sprawling virtual ecosystems. The gaming model today has gone far beyond recreation and has instead turned into a multifaceted digital industry, influenced by cultural trends, commercial interests and regulatory frameworks.

Like any complex ecosystem, online gaming has developed its own vocabulary. These are everyday terms used by digital players as they socially compete, transact and construct identities in real time. This 'Gaming Lexicon' section scans through some of the important terms that shape the viscera of online gaming. As governments aim to regulate online gaming in consonance with data protection and consumer rights, it becomes imperative to get a basic understanding of these terms and as well as their implications. The goal is not to make readers fluent in gamer slang, but to give policymakers, educators and professionals a 'shared reference point'.

“
Understanding gaming
governance begins with
understanding gaming
language.
”



SOCIALISE



COMPETE



TRANSACTION



CONSTRUCT
IDENTITIES



MULTIPLAYER GAMING GENRES



Online gaming offers diverse multiplayer experiences that bring players together in unique and engaging ways. Here are the key genres shaping the multiplayer landscape.

1. MMORPG (MASSIVELY MULTIPLAYER ONLINE ROLE-PLAYING GAME)



OVERVIEW:

A large online role-playing game where thousands of players share a constant virtual world. MMORPGs behave like small networked societies wherein players build identities, form groups and indulge in trade. Players develop reputations, informal rules and shared group cultures, making the game feel like a tangible social infrastructure.

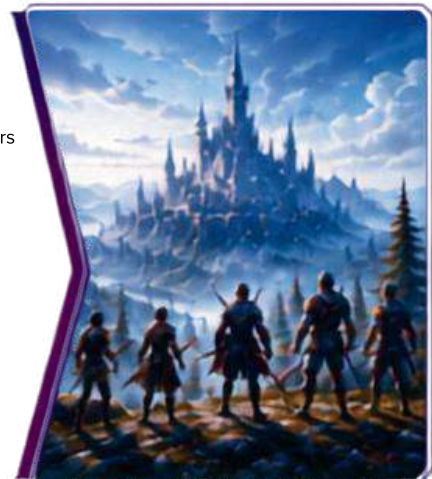
REGULATORY INSIGHT:



MMORPGs pose tough questions for policymakers about virtual property, dispute resolution, cross-border rules and citizenship/rights as no single offline law is capable of fully encompassing these aspects.

EXAMPLE:

A fantasy MMORPG where players join factions, manage housing, trade crafting goods and attend in-game festivals or protests organised entirely by players. Over time, the virtual world may split, merge or create their own codes of conduct and emulate real world organisational dynamics.



2. BATTLE ROYALE



OVERVIEW:

A gaming format where a large number of players enter one match and fight until one player or one team is left. These games come under collaboration, so players can present combat in decreasing play zone and high stakes produce fast and spectator friendly matches that draw huge live audiences, especially among the youth.

REGULATORY INSIGHT:



Battle Royale matches double up as mass live events which makes the game more accessible to public. Some players may only have to attend one event, while others may attend multiple events at a time. This practice is also required to gauge whether microtransactions, battle passes and virtual currencies meet consumer protections standards or not.

EXAMPLE:

Fortnite Battle Royale: About a hundred players drop onto an island, search for loot and an encroaching storm until only one player is left. Others may also host certain "viewer games" in this mode, turning ordinary matches into semi-public events that could be viewed by thousands at a time.



3. PVP (PLAYER VERSUS PLAYER)

OVERVIEW:

A gaming mode where human players directly contest against each other instead of fighting against system-controlled or automated opponents. The real test lies in the rival's skill or decision-making ability as there is no scripted enemy behaviour or predictable AI pattern here.

EXAMPLE:

League of Legends: Two teams compete to destroy the enemy using different strategies. Players may choose to livestream these matches.

REGULATORY INSIGHT: PvP is where the facets of cheating, targeted harassment and competitive pressure emerge, making it significant for discussions that circle around fair play, sanctions and mental health. Therefore, regulators and platforms need to understand the PvP dynamics while assessing harms such as: bullying, abuse, racism, etc. Policy retorts and online safety regulations can reflect in the form of chat monitoring, end-to-end reporting systems and identity verification. In PvP esports, regulation can be achieved by keeping a check on cheats, match-fixing, doping and enforcing rules through software systems (built in anti-cheat tools) and integrity codes.

4. MOBA (MULTIPLAYER ONLINE BATTLE ARENA)



OVERVIEW:

A team-based competitive game where players control distant heroes on a fixed map and aim to destroy the opponent's base. MOBAs demand tight coordination and deep strategic knowledge, which makes them ideal for professional leagues and structured competition.



EXAMPLE:

Dota 2: Two teams battle alongside, pick 5 distinct heroes, coordinate abilities, contest neutral objectives and time their abilities to win team fights, until they can take down the enemy.



REGULATORY INSIGHT: MOBAs illustrate how a game can become a full-fledged ecosystem of pro players, team sponsors, bettors, and broadcasters. The main issues that policymakers might grapple with are: labour rights, match fixing, gambling and youth exposure within a sector that behaves both as a sports and a media industry at the same time.



5. LIVE SERVICE GAME



OVERVIEW:

A game that runs as an ongoing service with regular updates and events, instead of a static product (which is released once). Features include live service that run seasonal events, crossovers and limited time offers.



EXAMPLE:

Destiny 2: An online shooter game that is constantly updated with new seasons, events and rotating item shops. The game runs as an ongoing live service.



REGULATORY INSIGHT: The main business goal with live service games is to keep players engaged over long periods of time, turning the game into a recurring revenue system. As this game never finishes, concerns may arise around long term safety, data retention and a change in the rights of players (when features change/disappear). Policymakers and consumer bodies can question companies if they end up withdrawing paid content or shutting down services without any reimbursement.

6. LOOT BOXES



OVERVIEW:

These are paid-in-game mechanisms that grant random rewards, usually without the revelation of fully transparent odds. Visual, flair, excitement and scarcity is used to encourage repeat purchases (especially in games that are popular with the youth).

EXAMPLE:

Overwatch is a useful example of how loot boxes work in practice. Players earn or purchase loot boxes that contain a random bundle of cosmetic items such as skins, emotes, sprays and voice lines. Every box is a surprise or a gamble.

REGULATORY INSIGHT: This feature offers a blend of luck, eye-catching animations and plenty of opportunities to open multiple boxes throughout a season. Conversely, regulators scrutinise the loot-box style monetisation due to the uncertainty regarding the items that players receive, combined with paid access to more boxes. Research also links heavy loot box spending to gambling addictions. Loot boxes have prompted inquiries, reports and regulatory actions in multiple jurisdictions, resulting in odds disclosure or even outright bans.



FREEMIUM MODEL



OVERVIEW:

In this model, the basic access of a game/app is free. However, the advanced features, content or conveniences require a certain amount of payment. Most of the revenue is generated from an enthralled minority who tend to spend recurrently to finish off levels. The design is built in such a way that it nudges players towards repeat purchases.



EXAMPLE:

A puzzle game that offers endless free levels and simultaneously sells extra lives, hint packs and cosmetic themes to impatient or devoted players. Also, advertisement/promotional videos appear in between levels for the users who choose not to pay.



REGULATORY INSIGHT:

Freemium models keep entry barriers low, which makes the games more accessible to players across diverse income levels/regions. These models also complicate the perception of affordability, fairness and informed consent in digital markets. Consequently, the onus lies on the regulators and consumer rights groups to be on the lookout for any manipulative designs or user exploitation.



In October 2022, the Competition Commission of India (CCI), held that Google had abused its dominance by forcing app developers to use its own billing system for in-app purchases (which included freemium titles). Penalties were imposed and Google was pushed to provide for a more flexible user choice for billing.



SKIN ECONOMY



OVERVIEW:

Skin economy encapsulates all the cosmetic aspects (skins) of gaming characters such as appearances, weapons or even interfaces. Skins act as means for playing androgynous, fashion and status markers, which also gives them visual modes to signal individuality or accomplishment.



EXAMPLE:

Cosmetic items in the skin economy tend to behave like real digital assets, especially when their value becomes comparable to a real-world product. For instance, a limited-edition skin related to a real-world event eventually becomes a symbol of prestige. As a result, digital players trade it on external marketplaces for higher values.



REGULATORY INSIGHT:

Trading of rare skins can result in people getting misled, scammed due to fraud, or money laundering. Policymakers claim that game companies should face regulations similar to the ones that are applied to banks/payment apps. Stronger rules can improve consumer protection, transparency and child safety.

In 2016, the Washington State Gambling Commission told Valve (a US based video game company) to stop third-party sites from using CS:GO (Counter Strike: Global Offensive) weapon skins as de-facto gambling chips. They warned that skin betting on esports was operating as an unlicensed and unregulated gambling market. As a result, Valve sent formal cease-and-desist notices to dozens of skin-betting sites, tightening its compliance and enforcement rules.



9. REAL MONEY GAMING (RMG)

OVERVIEW:

These are online games where players stake real money (or translatable credits) and win or lose money based on the outcomes. These games can range from casino-style playoffs to skill-based contests (that usually fall within the gambling ambit).

EXAMPLE:

RummyCulture/Classic Rummy: A game where players deposit real money, join rummy tables and win cash prizes (that can be withdrawn to their bank accounts).



REGULATORY INSIGHT: RMG as a concept can lead to loss of money, addiction, fraud and amplify consumer protection risks. To combat this, regulators focus on licensing, age checks and transparency.

In India, the legal discourse around gaming used to focus mainly on deciphering whether a game was skill-based or chance-based. Chance-based formats were typically treated as gambling. However, The Promotion and Regulation of Online Gaming Act, 2025 has now created a wider category known as 'online money games'. Under this 2025 framework, once a game is categorised as an online money game, it can be subjected to tighter rules such as licensing, bans, KYC requirements, payment-gateway obligations and strict advertising norms.

10. ONLINE BETTING

OVERVIEW:

Players place wagers on online game outcomes, esports matches, specific in-game achievements and other events.

EXAMPLE:

A viewer bets on the result of an esports livestream through an online betting platform and uses a digital wallet to complete the transaction.

REGULATORY INSIGHT: Online betting platforms bridge sports and gaming audiences with gambling markets, resulting in frequent integration of betting features into livestreams, online tournaments and digital sports broadcasts. This links gaming directly to gambling regulation, including oversight around match integrity, age verification and anti-money laundering compliance.



SECURITY RISKS IN GAMING



11. ACCOUNT TAKEOVER (ATO)



OVERVIEW:

An account takeover happens when an attacker gains control of a player's account without permission. ATO usually starts due to stolen credentials, phishing or automated attacks that use a large collection of stolen/breached passwords.



EXAMPLE:

An online gamer clicks on a fake login link and ends up taking access to his account. The attacker then uses the stored payment details or steals the in-game items.



REGULATORY INSIGHT:

In India, account takeover is a regulatory concern since it can cause consumer harm and financial fraud. It is usually covered by the IT Act, 2000, the Consumer Protection Act, 2019, the RBI payment security rules and customer liability norms. Gaming platforms are expected to protect user accounts, detect suspicious activity and provide quick grievance redressal, especially when it comes to real money games.

12. CHEAT SOFTWARE/CHEATS



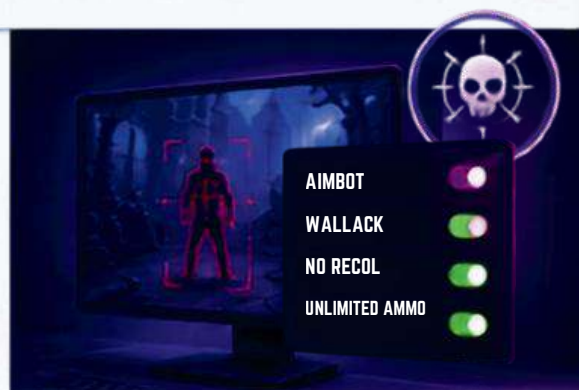
OVERVIEW:

These are unauthorised tools that give players unfair advantages by breaking in or bypassing the game's rules. This software is sold as subscriptions on cheat websites. They may even be promoted on gaming chats, suspicious sites and social media DM's under the gimmicks of 'cheat codes'.



EXAMPLE:

Aimbot and Wallhack are the most commonly used cheats in online shooter games. Aimbot automatically aims and shoots at enemies without the player aiming manually at the target. Through Wallhack, players can see through walls/solid objects, revealing enemy positions and ambushing hidden players.



REGULATORY INSIGHT:

Cheating software erodes trust in rankings, casual play and esports. In India, using or selling such cheats invokes unauthorised access and fraud risks. Platforms are expected to use anti-cheat systems and enforce suspensions/bans when detected. However, these systems might become too invasive as they tend to collect deep system data in the process, resulting in an invasion of user privacy. Therefore, during the regulatory process, policymakers have to create a balance between ensuring fair play and safeguarding the user's right to privacy.

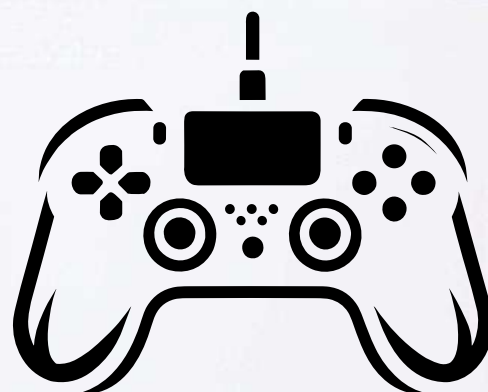
13. BOTTING

OVERVIEW:

Botting is a process which uses automated programs (software bots) to perform recurring in-game tasks. Large bot networks can feign in-game economies and run multiple accounts at a given time. This can inflate a player's resources much faster than that of a legitimate player.

EXAMPLE:

In an MMORPG (like RuneScape or World of Warcraft), a player can use a software to automatically kill enemies or gather resources 24/7, without employing any human effort. This gives an unfair advantage to players who play manually.



REGULATORY INSIGHT:

Botting turns games into a base for unregulated digital labour and money movements. This raises questions about enforcement priorities and latent financial crime ramifications.

In India, botting can be considered as fraud, unfair trade practice and money laundering. In late 2025/early 2026, the Enforcement Directorate charged the WinZO gaming app under the Prevention of Money Laundering Act (PMLA), 2002. The app was accused of rigging games with bots, AI and algorithm-based profiles (instead of pairing players with real humans).



VIRTUAL ASSET THEFT



OVERVIEW:

Virtual asset theft is a cross-border cybercrime that involves theft of in-game items, currency or accounts that have either real or perceived monetary value. Victims can lose out on investments pertaining to both time and money.



EXAMPLE:

Attackers can compromise multiple high-value accounts and move the player's rare items to mule accounts. They can then cash them out through another external trading site.



REGULATORY INSIGHT:

In virtual asset theft, redressal and restitution can get difficult if platform policies treat such assets as non property. Authorities and courts might have to first ponder over how they would consider the ownership and theft of digital items.



Researchers are now focusing on strengthening asset recovery mechanisms for stolen virtual assets. Emphasis is also being laid on international cooperation since jurisdictional gaps can create global vulnerabilities. The Financial Action Task Force (FATF), established in 1989, requires countries to implement AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) standards for virtual assets.

15. TOXICITY



OVERVIEW:

Toxicity in online gaming means any harmful, hostile, insulting or degrading player behaviour in the form of text, voice or other in-game actions. As per research and surveys, women and minority groups are frequently subjected to harassment, abuse and hate in online games.



EXAMPLE:

A player is singled out in a voice chat with derogatory slurs and threats due to his performance. This person feels mentally harassed, is forced to mute everyone and eventually ends up leaving the game.



REGULATORY INSIGHT:

Toxicity undermines inclusion, tolerance and wellbeing. It isn't something that is just a part of the gaming culture, but something that should be treated as a safety and equality issue. Globally, regulators expect platforms to moderate, report and sanction toxic behaviour. In India, under the IT Act, 2000, IT Rules, 2021 and Promotion and Regulation of Online Gaming Act, 2025, platforms must ensure safe environments, remove unlawful content and address grievances, especially with regards to minors.

16. DOXING



OVERVIEW:

Doxing in online gaming is a malicious practice where players' real identity and private details (like name, address, contact details) are posted online to harass, intimidate or harm them. The attacker may use social media, IP (Internet Protocol) logging, hacking or social engineering to uncover this data.



EXAMPLE:

An argument between two players during a match results in one of them posting the other's real address and phone number online. Subsequently, the victim player gets hundreds of threatening calls and is compelled to leave the game.

REGULATORY INSIGHT:

In India, currently there is no specific law that directly criminalises doxing. However, it can be treated as cyber harassment, stalking, defamation or a privacy violation under the IT Act, 2000 and Bharatiya Nyaya Sanhita, 2023. Gaming platforms are obligated to remove doxing content and provide grievance redressal under the IT Rules, 2021 and the Online Gaming Act, 2025. Regulators are presently deliberating on explicitly criminalising doxing under the upcoming Digital India Act.

GAMING SAFETY & GOVERNANCE

17. AGE VERIFICATION

OVERVIEW:

For online gaming, certain processes are used to assess whether a user is a child, teenager or an adult before access is granted. Methods include simple in-app self-declarations, ID upload, third-party checks or AI-based estimation.

REGULATORY INSIGHT: Many new online gaming and safety frameworks now pivot around protecting minors. Age-checks have undoubtedly become crucial but are still somehow technically challenging when it comes to enforcement.

In India, under the Promotion and Regulation of Online Gaming Act, 2025 and the new Online Gaming Rules, 2026, age verification and age-gating have become core user safety features. These are non-negotiables which platforms are expected to implement, especially where games involve high stakes. In fact, platforms that are unable to show credible age-verification and age-restriction mechanisms, risk losing out on registrations, can face transaction blocks and can be treated as non-compliant.

EXAMPLE:

A platform that requires verification of age before enabling real-money wagers, paid loot boxes or 18+ channels. Parents may also be presented with dashboards to review and approve access.

18. CONSUMER PROTECTION IN GAMING

OVERVIEW:

Processes that apply general consumer rights principles (such as safety, fairness, transparency) to online games, in-app purchase and subscriptions. It stems from the rationale that digital goods/services should be treated like any other product that comes with the prospects of redressal and recourse.

EXAMPLE:

A regulator may mandate that an online game should indicate real-currency prices alongside virtual currency and also uphold refund rights for accidental purchases by minors. Platforms can even be directed to add compliant channels/ independent dispute resolution for billing concerns.



REGULATORY INSIGHT: As online gaming evolves into service-based platform models, regulators now expect them to comply with the same standards that apply to other online marketplaces. In India currently, consumer protection in gaming is overseen by the Consumer Protection Act, 2019, the E-Commerce Rules, 2020, the IT Act Rules, 2021 and the new Promotion and Regulation of Online Gaming Act, 2025 read with the Online Gaming Rules, 2026. Under these, gaming consumer protection focuses on clear pricing, honest ads and easy refunds (especially for freemium and real-money games). The 2025 gaming law and the 2026 rules also push platforms to add KYC, grievance redressal and user-safety features.





19. CONTENT MODERATION



OVERVIEW:

This term is used for the processes that systems/teams undertake to detect, review and respond to harmful or rule-breaking behaviour. These processes monitor, filter and enforce rules on user-generated content to keep the virtual environment safe, fair and compliant.



EXAMPLE:

A flagged conversation on a gaming platform triggers an automated analysis. It is then escalated to a reviewer who either mutes, suspends or bans the defaulter.



REGULATORY INSIGHT:

REGULATORY Insight: As online games are now being considered as key digital spaces of interaction and communication, moderation practices are gaining significant momentum. The best approach followed by platforms is a hybrid one, which means combining both AI models as well as human review to enforce moderation standards.

20. PLAYER REPORTING SYSTEMS



OVERVIEW:

These are in-game tools for users to flag any bad behaviour to the platform (such as abuse, cheating or rule-breaking). A report goes to the game's moderation team along with chat logs or gameplay data. Based on the evidence received, an offender may get a warning, suspension, or a total ban.



EXAMPLE:

A post-match portal where players can report others, attach clips or screenshots as proof of any misconduct, and later receive a notification when adequate action has been taken.



REGULATORY INSIGHT:

REGULATORY Insight: Player reporting systems help platforms quickly detect acts such as doxing, harassment or hate speech. Reporting systems also help platforms to comply with safety obligations and avoid penalties. Timely action and transparency on how reports are handled, are both important aspects of these systems.



CONCLUSION



As gaming communities continue to grow, familiarity with these terms and concepts will become increasingly important for anyone who seeks to understand the modern gaming landscape. These terms and their explanations illustrate and reflect the evolving realities of digital societies, virtual economies and online interactions that define the gaming experience of today.

GAMING AS A THIRD SPACE

HOW VIRTUAL WORLDS ARE BECOMING SOCIAL SPACES FOR A GENERATION

For many young people, gaming platforms have become more than entertainment spaces. They function as digital communities where friendships are formed, identities are explored, and social life increasingly unfolds.



For many parents, online gaming is often seen as a form of entertainment, or at worst, a distraction. Yet for millions of young people around the world, gaming has evolved into something far more significant. It is increasingly becoming a social space a place where friendships are formed, communities are built, and identities are explored.



Sociologist Ray Oldenburg famously described "third places" as places outside home (the first place) and work or school (the second place) where people gather, share stories, build communities, and community centres. Today, for a growing generation of digital natives, many of these interactions are taking place in virtual worlds.



Online games such as Fortnite, Minecraft, Roblox, Valorant, and PUBG Mobile are no longer simply games. They function as social environments where players spend time together, communicate through voice and text, and share shared goals, and entertainment. During the COVID-19 pandemic, when physical interaction became limited, these digital spaces became even more important as avenues for connection and social engagement.



Research has increasingly highlighted this social dimension of gaming. A report by the Pew Research Centre found that many teenagers view gaming as an important way to spend time with friends and maintain social relationships. Similarly, studies published by the Oxford Internet Institute suggest that gaming can become a key source of motivation and when used in moderation and within healthy contexts.



The rise of gaming as a social space is particularly relevant in countries such as India. Rapid smartphone technology has also become popular, and the growth of multiplayer mobile gaming have enabled millions of young people to participate in digital communities regardless of location. For students living in hostels, young professionals in new cities, or senior executives in corporate digital infrastructure, online gaming often provides a sense of belonging and companionship that may be difficult to find elsewhere.



At the same time, these virtual communities are not without challenges. Online spaces can also expose users to harassment, toxic behaviour, misinformation, privacy risks,

and financial exploitation through manipulative monetisation practices. Questions of moderation, platform accountability, child safety, and digital well-being therefore become increasingly important as gaming platforms take on functions traditionally associated with social networks and community spaces.



This shift raises an important governance question: if online games are becoming social infrastructure, should they be viewed solely through the lens of entertainment regulation? Policymakers are increasingly being asked to consider broader issues such as user safety, content moderation, data governance, accessibility, and community standards. The conversation moves beyond what games people play to how digital environments shape social interactions and public life.



Understanding gaming as a social phenomenon does not mean ignoring legitimate concerns around excessive use, harmful content, or exploitative design. Rather, it requires recognising that gaming occupies a more complex place in contemporary society than is often acknowledged. For many young people, logging into online environments is a key source of motivation and when used in moderation and within healthy contexts.



As digital societies continue to evolve, online games are likely to play an increasingly important role in shaping how communities are formed, how relationships are maintained, and how individuals expand their belonging. In contrast, online gaming challenges for policymakers, platforms, educators, and parents is not merely to understand gaming as a space where digital citizenship is increasingly being practiced.



FURTHER READING

- **Pew Research Centre, Teens and Friendship**
<https://www.pewresearch.org/internet/2015/08/06/teens-technology-and-friendships/>
- **Oxford Internet Institute, Gaming and Wellbeing Research**
<https://www.ox.ac.uk/research/projects/understanding-video-game-play-and-mental-health/>

THE OTHER SIDE OF THE SCREEN

Through the story of one individual, this article explores how gaming, academic pressure, influencer culture, and mental health can interact. It highlights the importance of understanding gaming habits within broader social and psychological contexts.

The global online gaming market is expected to grow at an annual rate of 10.5 percent starting in 2025, reaching around USD 350 billion by 2030. This figure reveals a contradiction: an industry that brings real community, creativity, and entertainment to millions, while also exposing a significant minority to risks like addiction, academic setbacks, and financial problems. In April 2026, a case from Delhi highlighted the extreme end of this issue. A nineteen-year-old, who had previously scored ninety percent in his Class 12 exam, committed a violent crime due to online gaming debt. Although this case was exceptional, it was not completely isolated. It stemmed from an environment where financial risk and psychological compulsion are often built into platforms available to people of all ages.

Broad data tells one part of the story. Personal experiences provide another. What follows is a first-person account from an interview with a recovering gaming addict — referred to as Rohan here, at his request — as part of this magazine's wider exploration of India's gaming culture.

THE KOTA YEARS: FROM RELIEF TO DEPENDENCY

For the first time away from home, in high-pressure academic setting with little social support, Rohan found community in PUBG — just like many of his friends and family. In the days of livestreaming before PUBG, he recalled, "It introduced something completely new." For isolated students, coping with the stress of competitive gaming, the need for connection and identity in a demanding environment.

At first, gaming was just a way to unwind from academic stress. But as the gap between his performance expectations and actual results grew, Rohan started taking more time gaming and less time watching TV shows. By the time of academic performance led to more gaming as a way to cope, which in turn worsened performance and deepened the need to escape. Within months, he was gaming all night and sleeping all day.

• ANUPMA PRAKASH SRIVASTAVA

A PROMISING BEGINNING

Rohan is twenty-eight years old and currently works for a multinational company in Gurgaon. When we met, he spoke calmly, reflecting on his past. "Not where I should have been," he said about his current situation. "but definitely somewhere — despite everything."

His early life showed little sign of what lay ahead. A passionate reader with insightful observations, Rohan was considered an exceptional student. Strong Class 10 board results got him into a coaching institute in Kota to prepare for the IIT-JEE entrance exam. He was just sixteen at the time. PUBG had just launched in India.



"I simply couldn't follow the subjects anymore," he said. "Gaming was a break from the boredom of lectures I had stopped understanding." Six months into this, he returned home. His parents attributed his withdrawal from Kota to the intensity of the environment. The deeper issues went unexamined."

A PROMISING BEGINNING

Rohan openly discussed the structural factors that made his addiction possible. He noted that gaming had traditionally been a middle-class pastime limited by the costs of consoles and equipment. The rise of affordable smartphones and cheap mobile data removed those barriers entirely, making PUBG and similar games accessible to anyone with a device and connection, regardless of income.

Importantly, the game imposed no time limits. Unlike earlier mobile games that included cooldown periods to manage playtime, PUBG allowed continuous gaming. “You could play all night,” Rohan said. “And many did.” The lack of restrictions, combined with social features that made lengthy sessions feel productive and community-focused, made it hard to stop.

For Rohan, physical sports — an area where he had genuine talent — were not a viable option. His neighbourhood had no parks or sports facilities, and his family couldn’t justify the cost of private or academy. PUBG was, in his words, “a low-cost, curated, independent world” that filled the gaps left by unavailable social and physical activities.



FREE

THE PHYSICAL AND PSYCHOLOGICAL TOLL

➤ The long hours of gaming took a cumulative toll on Rohan’s daily life, eventually becoming severe. He mostly relied on packaged snacks near his device, as getting up for meals disrupted gaming sessions. He was known to train in his skills, focusing on schedule and then in quality. Physical symptoms emerged: trembling fingers, constant headaches, fatigue, and a general decline in his engagement with the outside world.

➤ In December 2022, Rohan was diagnosed with Attention Deficit Hyperactivity Disorder (ADHD). Research from the National Library of Medicine shows ADHD can be linked to gaming disorders. For Rohan, the diagnosis clarified patterns he had struggled to understand — the difficulty in focusing on tasks, the need for social support, and the importance of immediate feedback, and the intensity of his addiction compared to peers who played without similar issues. “In mathematics, I would zone out twenty times in an hour. Gaming gave my mind somewhere definite to go.”





THE ROLE OF ENVIRONMENT: FAMILY, SCHOOL, AND INFLUENCER CULTURE

Rohan reflected on the external factors that increased his vulnerability. His father, absorbed in work, had little knowledge of his son's daily life. His mother, not well-versed in digital technology, couldn't tell the difference between productive and harmful screen time. "I told her I was studying on my phone," Rohan said, lacking any pride. "She had no way of knowing otherwise." This situation, he noted, is common in many Indian households — especially in cities where both parents work long hours and digital skills vary widely.



At school, Rohan faced what many students in similar situations describe: a tendency to categorise students early and provide attention accordingly. Once placed in the "average" group, he received little guidance in adjusting to more challenging course material. With neither family nor school supporting him in a way that matched his struggles, gaming filled the void where mentorship and structured help should have been.



He also considered the impact of gaming content creators. The rags-to-riches stories prevalent in gaming culture during his formative years painted success as quick and glamorous. "The messaging was constant," and the stories that he created never explained the investment behind those stories or what happens when you lose." For a teenager already facing academic failure and social isolation, these narratives held a strong appeal that came with real costs.



The online gaming industry's profit motives are not necessarily harmful, but they are not neutral either. Game design, progression mechanics, and social features aim to increase the time users spend on the platform. For most users, this creates an enjoyable and positive impact on the community. Moreover, for a minority, one that considering the size of the industry, includes millions of people worldwide, these same features can lead to dependency.



RECOVERY: THE SLOW WORK OF REBUILDING

Rohan's path to recovery was neither simple nor straightforward. He received medication for sleep issues, but the treatment required a consistent routine that his lifestyle at the time made impossible. Therapy brought out long-term treatments. Eventually, in 2020, he developed a slow recovery. He moved Mumbai with a promise to return only after he had established some independence.



What the city offered was not a cure, but an environment where the conditions that fueled his addiction could no longer exist. Managing housing, work, meals, and finances in a busy urban setting left no room for long gaming sessions. "Survival mode," he simply stated, "had no time for bad habits." The addition that had structured his life for years and quickly ones the supportive conditions were removed.



Rohan is open about what he has lost. "Years of educational and job opportunities, strained relationships, due to withdrawal, and a path that did not match the potential others had recognised in him early on. He has switched jobs and cities multiple times in four years, but he has made peace with this instability. He still plays games, as many people his age do, but now he knows when to stop.

WHAT ROHAN'S STORY TELLS US



Individual accounts can risk oversimplifying complex issues. Rohan's journey through the game industry was not easy. He spent years learning the rules, getting certified, and mastering the game. These elements will not apply equally to all players. His story does not argue against gaming. Instead, it shows what can happen when a platform designed for engagement meets a young person with fewer options, in an environment that lacks understanding or resources to help.



The online gaming industry's profit motives are not necessarily harmful, but they are not neutral either. Game design, progression mechanics, and social features aim to increase the time users spend on the platform. For most users, this creates an enjoyable and positive impact on the community. Moreover, for a minority, one that considering the size of the industry, includes millions of people worldwide, these same features can lead to dependency.



India's Promotion and Regulation of Online Gaming Act, 2025, along with the PROG Rules of 2026, attempts to bring accountability to this landscape. Age verification, parental controls, management tools, and access to counseling are potential supports that could have helped someone like Rohan. The key question is whether these measures will be implemented effectively and independently.

“

Rohan has thought about sharing his experience. "Maybe a book," he said, "on influencer culture and its impact on young minds." He spoke about it calmly and without urgency, as if the idea would reveal itself when the time was right.

#

AUTHOR'S NOTE

This story reflects one individual's lived experience and should not be interpreted as representative of all gamers or gaming experiences.

MARCH–MAY 2026

CYBERPEACE IN ACTION

BUILDING CYBER RESILIENCE ACROSS COMMUNITIES

A quarterly roundup of CyberPeace Foundation's awareness campaigns, capacity-building programmes, law-enforcement engagements, industry trainings, and youth outreach initiatives across India.

Over the past quarter, CyberPeace continued its capacity-building and public awareness efforts across educational institutions, law enforcement agencies, industry stakeholders, community groups, and security personnel.

Through workshops, awareness sessions, legal literacy initiatives, and specialized technical training, the organisation engaged diverse audiences on emerging cyber risks, digital safety, fraud prevention, cyber law, and responsible technology use.



Quarterly Snapshot:

40 Sessions | 2000+ Participants | 25+ Partners



KEY FOCUS AREA



SECTORAL READINESS

Cybersecurity preparedness for specific industries.



OSINT CAPACITY

Building skills in open-source intelligence and investigation.



CYBER LAW

Understanding cyber laws and reporting mechanisms.



CYBER FRAUD AWARENESS

Training on identifying and preventing cyber fraud.



CYBERPEACE RESPONDER

Programme for first responders in cyber incidents.



AI SAFETY

Responsible use of artificial intelligence in technology.

FEATURED ENGAGEMENTS

STRENGTHENING DIGITAL INVESTIGATIONS: OSINT TRAINING FOR ODISHA POLICE



CyberPeace conducted a Two-day Open-Source Intelligence (OSINT) training programme for approximately 200 police personnel in partnership with Odisha Police.



The programme focused on strengthening investigative and digital intelligence capabilities through practical exposure to:



- ▶ Social media investigations
- ▶ Geolocation analysis
- ▶ Digital identity tracking
- ▶ Publicly available intelligence gathering
- ▶ Ethical investigation practices
- ▶ Infosec analysis and emerging investigative tools



Participants engaged in hands-on exercises designed around real-world investigative scenarios, supporting evidence-based policing in increasingly digital environments.



WHY IT MATTERS:

As cybercrime, misinformation, and digital threats evolve, strengthening OSINT capabilities has become critical for modern law enforcement.



CYBER DEFENCE

FOR

SMART AVIATION

PROTECTING CRITICAL INFRASTRUCTURE

CyberPeace delivered a specialized session titled “Cyber Defence for Smart Aviation” for aviation personnel associated with the Jewar Airport, Greater Noida with **Source Integreta**.

Led by **Anindita Mishra**, the programme explored cybersecurity challenges unique to smart aviation ecosystems, including:

-  Protection of aviation infrastructure
-  Ransomware preparedness
-  Phishing defence
-  Cyber risks in connected systems
-  Supply-chain vulnerabilities
-  Incident response readiness

Participants were also introduced to the CyberPeace First Responder framework as a proactive approach to cyber incident detection, response, and recovery.

WHY IT MATTERS:



As critical infrastructure becomes increasingly connected, sector-specific cyber resilience is becoming an operational necessity.



“ SECURE SKIES. RESILIENT SYSTEMS. **TRUSTED AVIATION** ”



UNDERSTANDING CYBER LAW

REPORTING MECHANISMS & DIGITAL RIGHTS

Advocate Muskan Sharma conducted a session on "Legal Frameworks & Reporting Mechanisms for Cyber Crimes" for approximately 350 participants, including students, educators, professionals, and community members.

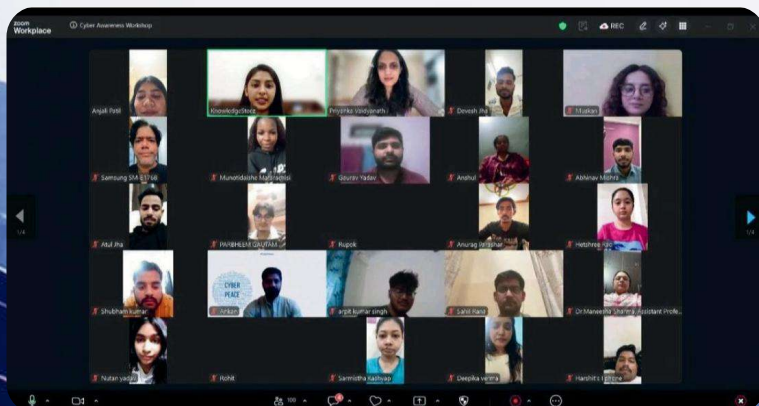
THE SESSION UNPACKED INDIA'S CYBER SAFETY ECOSYSTEM, COVERING:

- ✓ Cybercrime reporting procedures
- ✓ National Cyber Crime Reporting Portal (NCRP)
- ✓ Emergency helpline 1930 for financial fraud
- ✓ Documentation requirements for complaints
- ✓ Roles of cyber cells and law enforcement agencies
- ✓ Victim rights and legal protections

Interactive discussions focused on practical response mechanisms for phishing, fraud, and online harms.

WHY IT MATTERS:

Digital safety requires not only awareness of threats, but also knowledge of legal remedies and reporting pathways.



YOUTH CYBER AWARENESS AND DIGITAL SAFETY

Throughout the quarter, CyberPeace continued large-scale youth outreach through awareness sessions delivered across schools, universities, military education institutions, and student communities.



SELECTED ENGAGEMENTS INCLUDED:

- **Sri Venkateswar International School, Delhi** — 468 students reached
- **KLE School** — 250 students reached
- **NSHM Knowledge Campus, Durgapur** — 250 students reached
- **Sister Nivedita University, Kolkata** — multiple sessions engaging university students
- **Sainik School programme** through **USI collaborations**
- **NCC outreach** initiatives in Delhi and Ferozpur



SESSIONS FOCUSED ON:



financial and payment fraud



social media and messaging scams



cyber hygiene practices



responsible technology use



identifying and responding to digital threats

WHY IT MATTERS:



Building cyber resilience among youth remains central to creating safer and more informed digital communities.



FROM THE FIELD: QUARTERLY ROUND-UP



Additional engagements during the quarter included collaborations with educational institutions, security organizations, corporate stakeholders, and community groups across India.



Programmes were conducted in partnership with:

USI | CISF | Odisha Police | DELNET | Tata Cummins | NCC | Techno India Group | Mount Abu School | Maheshwari Community | Sainik Schools | Universities and Schools across multiple states |



These sessions covered themes ranging from cyber fraud awareness and AI safety to digital literacy, community resilience, and responsible technology adoption.



CyberPeace



DELNET
Developing Library Network

BY THE NUMBERS



29

Educational Institutions



4

Security / Law Enforcement Engagements



3

Industry & Workforce Trainings



4

Community Awareness Sessions

STATES REACHED

- Delhi
- Odisha
- Jharkhand
- West Bengal
- Uttar Pradesh
- Punjab
- Uttarakhand
- Andhra Pradesh

MOST COVERED THEMES



Cyber
Fraud



AI
Safety



Cyber
Law



Digital
Hygiene



Cyber First
Reporter



Investigation
Capacity
Building



BY THE NUMBERS



29

EDUCATIONAL
INSTITUTIONS



4

SECURITY / LAW
ENFORCEMENT
ENGAGEMENTS



3

INDUSTRY &
WORKFORCE
TRAININGS



4

COMMUNITY
AWARENESS
SESSIONS

MOST COVERED THEMES



CYBER FRAUD



CYBER FIRST
RESPONDER



AI SAFETY



INVESTIGATIVE
CAPACITY BUILDING



CYBER LAW



DIGITAL HYGIENE

STATES REACHED



Delhi



Odisha



Jharkhand



West Bengal



Uttar Pradesh



Punjab



uttarakhand



Andhra Pradesh

Volume 02 | Issue 02 | June 2026 | Quarterly



CyberPeace

CYBERPEACE

M A G A Z I N E

Shaping a **safer**
digital future
through trust, laws,
governance, and
innovation.



FREE DIGITAL EDITION



<https://magazine.cyberpeace.click/>



CYBERPEACE
MAGAZINE