International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 9, September 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos03092611691

Regulating Internet Addiction Crime under Cyber Law: A Critical Study

Amardeep Seth[1], Prof (Dr) Mukesh Kumar Sahu[2]
[1] *Research Scholar (Law) LNCT University, Bhopal (Madhya Pradesh) India*
[2] *Dean & Director of school of legal Studies, LNCT University, Bhopal (Madhya Pradesh) India.*

Article Info

Article History:
Published: 23 Sept 2026

Publication Issue:
Volume 3, Issue 9
September-2026

Page Number:
407-414

Corresponding Author:
Amardeep Seth

Abstract:

Think about how dramatically the Internet has changed our lives — the way we talk, learn, shop, play, and socialize. But every gift has a shadow. Alongside all this convenience, something troubling has crept in: excessive, uncontrolled Internet use. When someone can't stop scrolling, gaming, gambling, streaming, or shopping online — when it starts damaging their studies, work, relationships, or finances — we have a genuine social, psychological, and now legal problem on our hands.

And the legal problem gets even more tangled when this addictive behavior overlaps with actual cybercrime — financial fraud, online exploitation, privacy violations, obscene content, identity theft, harassment, and illegal gaming. So regulating Internet addiction can't simply be treated as an ordinary criminal-law question.

Here's a key fact students should note: India has no offence called "Internet addiction" under the Information Technology Act, 2000. Instead, we have a patchwork of laws — the IT Act itself, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, data-protection legislation, and the newly enacted Promotion and Regulation of Online Gaming Act, 2025 — each targeting a particular digital risk. The gaming law deserves special attention because it openly acknowledges the psychological, social, economic, and privacy harms of online money games and builds a specialized regulatory and enforcement machinery.

This article walks through the relationship between Internet addiction and Indian cyber law, and makes a central argument: criminalizing addiction itself makes no sense, because addiction is better understood as a health or behavioral condition, not criminal conduct. What we need instead is a preventive, rights-based, harm-oriented framework that combines criminal law, intermediary regulation, consumer protection, data protection, platform accountability, age safeguards, financial controls, digital literacy, and treatment. The article closes by proposing a balanced model that protects vulnerable users without crushing legitimate Internet use or fundamental freedoms.

Keywords: Internet addiction, cybercrime, cyber law, online gaming, gaming disorder, Information Technology Act, online money games, intermediary liability, digital addiction, India

1. Introduction

The Internet is no longer a luxury — it's woven into everything we do. Smartphones, social media, online games, streaming platforms, digital payments, virtual communities — all of these have fundamentally changed how we communicate and consume information. But here's the catch: the very features that make these platforms irresistible — they're always available, they personalize content for you, they offer social rewards, notifications, and sheer convenience — are the same features that can push people into compulsive overuse.

We use the term "Internet addiction" to describe a persistent, problematic pattern of Internet use that begins to damage a person's personal, educational, professional, social, or family life. But — and this distinction matters enormously for law — we must separate *intensive* Internet use from a genuine *clinical disorder*. The World Health Organization recognizes **gaming disorder** in ICD-11: it involves losing control over gaming, giving gaming priority over everything else, and continuing or escalating despite clear harm, with significant impairment normally visible for at least twelve months. Importantly, WHO stresses that only a *minority* of gamers develop this disorder.

Why does this matter legally? Because a person who spends five hours on social media or gaming has committed **no crime**. Criminal law demands a legally defined prohibited act plus the required elements of liability. So "Internet addiction" should never be automatically converted into a criminal category.

The real legal concern emerges when addictive digital environments *enable or fuel* unlawful conduct. Compulsive participation in online money games can lead to financial ruin or fraud; heavy social-media use can coexist with cyberstalking, impersonation, or the unlawful posting of intimate images; compulsive consumption of illegal content can involve obscenity or child sexual abuse material; and constant digital engagement raises exposure to scams, identity theft, and financial fraud.

2. Understanding Internet Addiction vs. Cybercrime

"Internet addiction" is an umbrella term covering many different behaviors: compulsive social-media use, problematic gaming, online gambling or money gaming, compulsive pornography consumption, endless video streaming, compulsive online shopping, obsessive participation in online communities, bingeing on short-form content, and other repetitive online activities.

Here's my advice as a teacher: don't lump these together. Each has different motivations, different degrees of harm, different economic consequences, and different potential for criminality.

Cybercrime, on the other hand, is a strictly legal concept — unlawful conduct involving computers, networks, devices, or digital information. The IT Act, 2000 contains offences covering computer-related misconduct, identity theft, cheating by personation, privacy violations, cyber terrorism, obscene electronic material, and more. Sections 65 to 67B, for instance, deal with offences against computer systems and prohibited electronic content; Section 67C imposes preservation and retention duties on intermediaries; and Sections 69 and 69A provide for interception and blocking in defined circumstances.

A person can be addicted without committing any crime. A cybercriminal can commit serious offences without being addicted at all. The two sometimes overlap — but only sometimes.

3. The "Criminogenic Digital Environment"

Let me introduce a useful concept: the **criminogenic digital environment**. Some online spaces raise a person's exposure to illegal activity simply by making harmful conduct easy, repetitive, and financially rewarding.

Think about how social-media algorithms, recommendation engines, virtual rewards, gamification, and persuasive design keep you hooked. Now, that doesn't mean every platform using these tools is a crime facilitator. The legal question is narrower and sharper: **do particular design practices create foreseeable risks of exploitation, or open the door to unlawful conduct?**

The Promotion and Regulation of Online Gaming Act, 2025 gives us a striking contemporary example. The Act explicitly voices concern about social, economic, psychological, and privacy harms from online money games, and its framework points to manipulative design features, addictive algorithms, and aggressive advertising as factors behind these risks. The Act defines an "online money game" broadly — any online game involving payment of fees, deposits, or stakes in expectation of winning money or other enrichment, whether based on skill, chance, or both, subject to statutory exclusions.

Notice the bigger shift this represents in Indian cyber regulation: instead of merely punishing what an individual user *does*, the law is now examining the **architecture of the digital service itself**.

4. India's Existing Cyber-Law Framework

4.1 The Information Technology Act, 2000

The IT Act remains the backbone of Indian cybercrime law. It contains no specific offence of Internet addiction — and that's a good thing. What it does is criminalize particular *conducts* that may occur in digital spaces:

- **Section 66:** computer-related offences
- **Section 66C:** identity theft
- **Section 66D:** cheating by personation using computer resources
- **Section 66E:** violation of privacy
- **Section 66F:** cyber terrorism
- **Sections 67, 67A, 67B:** prohibited obscene or sexually explicit electronic material
- **Section 67C:** preservation and retention obligations of intermediaries
- **Section 69:** interception, monitoring, decryption under statutory conditions
- **Section 69A:** blocking of public access to specified information
- **Section 79:** conditional safe-harbour protection for intermediaries

These provisions deal well with crimes that may accompany excessive Internet use. But none of them punishes a person merely for spending "too much time" online — and from a criminal-law theory standpoint, that's exactly right. Liability should attach to a defined prohibited act, not to a person's psychological condition or consumption habits.

4.2 Intermediary Regulation

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 add another regulatory layer, and MeitY continues to maintain them as part of India's statutory digital framework. This matters because Internet addiction isn't just a user problem — **platforms shape how content is recommended, displayed, monetized, and amplified.** Platform governance through these rules covers grievance redressal, unlawful content, user safety, and compliance with government directions — potentially reducing harmful exposure *without* criminalizing ordinary Internet use.

4.3 Blocking and Cybersecurity Powers

Sections 69A and 69B provide blocking and monitoring mechanisms for specified statutory purposes. These become relevant when websites or apps facilitate serious unlawful activity. But blocking always raises hard questions: Is it proportionate? Transparent? Procedurally fair? Does it respect freedom of expression?

Here, every student should know the Supreme Court's landmark decision in ***Shreya Singhal v. Union of India*** (decided 24 March 2015), which struck down Section 66A of the IT Act. The lesson is enduring: technological regulation must remain compatible with constitutional guarantees — we cannot criminalize our way out of every undesirable online behavior.

5. Online Gaming Addiction and the New Framework

Online gaming is where the addiction–cyber law intersection is most visible. WHO recognizes gaming disorder as a disorder due to addictive behaviors — impaired control, escalating priority, continued play despite harm, with significant impairment.

India's response has moved well beyond old gambling statutes. The **Promotion and Regulation of Online Gaming Act, 2025** creates a national framework for online gaming and expressly *prohibits* online money games and associated services, along with their advertising and fund transfers. It establishes the **Online Gaming Authority of India**, creates offences and penalties, and provides blocking powers and investigation mechanisms.

One feature deserves your close attention: the Act applies not just within India but also to online money-gaming services offered in India **even when operated from outside India**. That's a big deal, because addiction-related harms often flow from offshore platforms with no physical presence here.

The framework became operational in 2026 — MeitY notified the constitution of the Online Gaming Authority of India on 22 April 2026 — and the rules mandate safeguards like age verification or age-gating, time restrictions, parental controls, user reporting, grievance redressal, counselling support, and fair-play monitoring. The Centre has also authorized designated cyber-cell and nodal cyber-cell officers to investigate offences under the Act. The significance? This framework joins **preventive regulation, user protection, and criminal enforcement** — instead of waiting to punish after harm occurs.

6. The Critical Question: Should Internet Addiction Itself Be a Crime?

Let's stress-test the idea of criminalizing addiction, and watch it fall apart.

First, addiction is tied to a health condition, not deliberate criminal intent. Criminal law has always distinguished between prohibited *conduct* and personal *conditions*.

Second, where would you draw the line? How many hours online equals "addiction"? Would the same number apply to a software engineer, an online student, a professional gamer, and a social-media influencer? Time alone tells us nothing about impairment.

Third, diagnosis is a medical, behavioural exercise. WHO's gaming-disorder criteria require significant functional impairment, normally over at least twelve months — that's a clinical judgment, not something a police officer can apply.

Fourth, criminalizing addiction would stigmatize sufferers and frighten them away from seeking treatment — the exact opposite of what we want.

Fifth, overcriminalization would collide with legitimate digital life. Today, education, jobs, banking, healthcare, government services, and professional communication all run on digital platforms.

7. Addiction, Cybercrime, and Criminal Responsibility

To be clear: saying addiction shouldn't be a crime doesn't mean it never matters in criminal law. It matters as *context*.

Picture someone who gambles compulsively on online money games and then commits identity theft to fund the habit. The crime is identity theft — not addiction. If someone impersonates another on social media to defraud victims, the law targets the fraud, not the screen time.

The principle is simple: criminal responsibility attaches to the legally prohibited act. But addiction can still be relevant in victim-risk assessment, juvenile justice, rehabilitation, sentencing where the law permits, diversion programmes, mental-health interventions, parental and educational measures, and prevention policy.

So let's reject the false binary of "criminal versus medical." A person may *need treatment* and *still be legally responsible* for an independent criminal act. Both things can be true at once.

8. Privacy and Surveillance: The Regulation Paradox

Here's a genuine dilemma. To prevent addiction effectively, platforms may need to detect excessive usage, abnormal spending, age-related risks, or repeated participation in harmful activities. But that very monitoring creates a new danger: **surveillance of citizens' online lives**.

The IT Act already contains powers for interception, monitoring, decryption, and blocking, and modern regulation increasingly pushes platform-level compliance. So regulators must answer hard questions:

1. What data may be collected?
2. For what purpose?
3. For how long?
4. Who can access it?
5. Can automated decisions be made on it?
6. Can users challenge those decisions?
7. What safeguards exist against misuse?

A system built to prevent addiction must never become a backdoor for unrestricted behavioural surveillance. That would cure a smaller harm by inflicting a larger one.

9. Children and Vulnerable Users

Children deserve special protection because they're least equipped to understand commercial incentives, persuasive design, and privacy risks. That's why age verification, parental controls, spending limits, default safety settings, and easy complaint mechanisms matter so much as *preventive* tools.

The 2026 gaming rules explicitly include age verification or age-gating, time restrictions, parental controls, user reporting, grievance mechanisms, and counselling support among their safeguards. But notice the irony: age verification itself creates privacy risks — collecting identity documents or biometrics from children could open new vulnerabilities. The answer is a proportionate system using the *least intrusive* method that achieves the protective goal.

The guiding philosophy should be **safety by design** — building protection into the platform itself, rather than dumping the entire burden on parents and children.

10. Financial Crime and Internet Addiction

The money connection is where addiction meets crime most brutally. Compulsive digital spending creates financial vulnerability, and fraudulent platforms are only too happy to exploit it. Online money gaming can also intertwine with unlawful fund transfers, fraud, and money laundering.

The 2025 Act tackles this head-on: it prohibits online money games along with their advertising and fund transfers, and its legislative statement flags financial fraud, money laundering, and tax evasion as risks of unlawful online money gaming — though, students, note the careful framing: these are legislative concerns, **not** a finding that every platform or player is a criminal.

The right response demands cooperation among cybercrime agencies, banks, payment intermediaries, and regulators. No single institution can solve this alone.

11. Constitutional Dimensions

Every Internet regulation sits inside India's constitutional framework. Article 19(1)(a) protects speech and expression; Article 21, as interpreted by the Supreme Court, protects privacy and personal liberty. Restrictions on online communication therefore need legal authority *and* must satisfy constitutional standards of proportionality.

Shreya Singhal proved how vital precise drafting is in the digital sphere — vague, overbroad prohibitions will not survive. Likewise, "this is harmful" cannot, by itself, justify a restriction. The law must identify the *specific harm*, the *statutory authority*, the *procedural safeguards*, and the *proportionality* of the measure. A blanket war on digital addiction could easily trample legitimate communication, association, recreation, and access to information — and that would be constitutionally indefensible.

12. The Gaps in the Current Framework

Honest scholarship means naming what's missing. Here are the major deficiencies:

12.1 No general legal definition — There is no comprehensive statutory definition of Internet addiction spanning social media, gaming, pornography, streaming, and other online activities.

12.2 Fragmented regulation — Cybercrime, financial fraud, gaming, consumer protection, privacy, and mental health each sit under different statutes and different authorities, with little coordination.

12.3 Treatment deficit — Criminal statutes punish unlawful conduct; they build no treatment infrastructure for people suffering from problematic Internet use.

12.4 Weak algorithmic accountability — The law is waking up to platform responsibility, but questions linger over recommendation systems, engagement-maximizing design, and algorithmic amplification.

12.5 Cross-border enforcement — Offshore platforms create thorny problems of jurisdiction, evidence collection, operator identification, and enforcement of blocking or investigative orders.

12.6 Evidentiary challenges — Digital evidence can be deleted, altered, or moved in seconds; preserving and authenticating it is a serious investigative hurdle.

12.7 Risk of overcriminalization — Broad prohibitions on digital behavior will inevitably capture legitimate conduct and impose disproportionate restrictions.

13. A Proposed Five-Layer Regulatory Model

What would a smarter Indian approach look like? I propose five layers working together.

Layer I — Identification and Prevention. High-risk platforms should adopt age-appropriate design, conduct risk assessments, and provide spending controls, time-management tools, and transparent user warnings.

Layer II — Platform Accountability. Platforms must identify and mitigate demonstrable risks created by their own design, with transparency about how recommendation and monetization systems work.

Layer III — Criminal Enforcement. Criminal law should target specific unlawful conduct — fraud, identity theft, cyberstalking, unlawful sexual content, hacking, financial crimes, prohibited online money gaming — **not addiction itself**.

Layer IV — Treatment and Rehabilitation. People showing clinically significant problematic digital behavior need access to counselling, psychological treatment, family intervention, and digital-dependency programmes.

Layer V — Rights Protection. Every intervention must embed privacy, due process, transparency, proportionality, grievance redressal, and meaningful appeal.

This model recognizes a simple truth: Internet addiction is simultaneously a **public-health issue, a consumer-protection issue, a technology-governance issue, and — in some situations — a cybercrime-related issue**. No single legal tool can address it.

14. Critical Evaluation

The deepest flaw in today's debate is the habit of treating Internet addiction and cybercrime as the same thing. They are not. The Internet can be addictive without being criminal; cybercrime can flourish without any addiction. The law must avoid two opposite errors: **medicalizing criminality** and **criminalizing illness**.

The new gaming framework shows a more mature direction — instead of asking only "has this person become addicted?", the law examines the service's characteristics: the financial stakes, the advertising, the platform's operations, registration, blocking, enforcement. It regulates the *system*, not just the *symptom*.

But regulation must stay evidence-based. WHO itself reminds us that gaming disorder affects only a small proportion of gamers, and we must distinguish healthy gaming, hazardous gaming, and actual disorder. The same discipline should govern cyber law generally: excessive Internet use must never become an excuse for indiscriminate surveillance or criminalization. Intervention must be proportionate to *demonstrable* harm.

And keep your eye on the horizon: artificial intelligence and personalized recommendation systems are growing more powerful by the day. Algorithms learn your preferences and optimize engagement relentlessly. Where systems are *deliberately* engineered to exploit vulnerability, platform responsibility will become one of the defining legal questions of the coming decade — but the law must set evidence-based standards, not assume every recommendation algorithm is inherently evil.

15. Conclusion

Internet addiction is a genuinely new challenge for cyber law because it lives at the crossroads of technology, psychology, public health, consumer protection, and criminal justice. The cardinal error would be treating addiction itself as a cybercrime. Using the Internet — even using it a lot — is not automatically unlawful conduct.

Indian cyber law has traditionally targeted specific prohibited acts: unauthorized access, identity theft, cheating by personation, privacy violations, unlawful electronic content. The IT Act gives us an important criminal-law foundation, but it is not — and was never meant to be — a comprehensive framework for behavioral addiction.

The landscape, however, is evolving fast. The IT Rules regulate intermediaries; the Promotion and Regulation of Online Gaming Act, 2025 builds a specialized regime for online gaming — prohibiting online money games, regulating their advertising and fund transfers, establishing the Online Gaming Authority, and creating investigation and blocking machinery. The 2026 rules add age verification, time restrictions, parental controls, reporting, grievance redressal, and counselling support.

So the path forward is clear: move from a **punishment-centred model to a harm-reduction and accountability model**. Criminal law should target identifiable unlawful conduct; regulatory law should address harmful platform practices; data-protection principles should fence in intrusive monitoring; and health policy should treat people with clinically significant behavioral problems.

A balanced framework ultimately pursues three goals together: **protect the individual, regulate the digital environment, and preserve legitimate digital freedom.** India's challenge is not to ban the Internet because it *can* be addictive — it is to build a legal system wise enough to recognize when digital design, commercial greed, or unlawful conduct turns ordinary Internet use into a source of serious, legally cognizable harm.

References

1. The Information Technology Act, 2000 (India), ss. 65–67B, 67C, 69, 69A, 69B, 79.
2. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Ministry of Electronics and Information Technology (MeitY), Government of India.
3. The Promotion and Regulation of Online Gaming Act, 2025 (India), including provisions on prohibition of online money games, the Online Gaming Authority of India, and associated rules notified in 2026.
4. World Health Organization, *International Classification of Diseases (ICD-11): Gaming Disorder*, WHO, Geneva (2019).
5. World Health Organization, "Gaming Disorder" (Fact Sheet), WHO, Geneva.
6. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (Supreme Court of India, decided 24 March 2015).
7. The Industrial Disputes Act, 1947; The Consumer Protection Act, 2019 (for related consumer and regulatory contexts).
8. NITI Aayog, *Designing the Future of Dispute Resolution: The ODR Policy Plan for India*, Government of India (2021).
9. Ethan Katsh & Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace*, Jossey-Bass (2001).
10. Ministry of Electronics and Information Technology (MeitY), notifications and official releases concerning the Online Gaming Authority of India (2026).