Page 305 - 313 **DOI:** *https://doij.org/10.10000/IJLMH.1111498*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Cyber Threats and Privacy Concerns in Online Gaming Landscape

S SIREESHA[1] AND BAWANKAR BHUVANESH PRABHAKAR[2]

ABSTRACT

Online gaming is a place where people interact with electronic devices such as computer systems, mobile phones, and tablets through the Internet for gaming purposes. Owing to advancements and access to the Internet, these gaming platforms provide many benefits, such as entertainment, accessibility, and education. Apart from the benefits, it also poses the risk of privacy concerns along with cyber threats. Information technology plays a major role in the online gaming landscape by providing infrastructure for gamers. By using artificial intelligence in gaming platforms, the participants are provided with advanced versions of games, which leads to an enhanced experience for gamers. In addition to the advancements, there are several security and privacy issues may often experience by the players and developers. This study deals with the laws relating to cyber threats, which are often encountered in online gaming environments, and provides measures to protect the privacy of gamers.

Keywords: *Online Gaming, Privacy Concerns, Cyber Threats, Artificial Intelligence, Information Technology*

I. INTRODUCTION

The concept of the online gaming industry in India has been expanding over the past few years, and this expansion has indeed negatively impacted the players due to a lack of protection at the initial stages. The significant growth occurred in online gaming with the adoption of new economic reforms in 1991, which led to the rise of internet cafes, which provide the space for players. Following the economic reforms, due to the rapid growth of technology, everyone can get access the smartphones with cheaper mobile data, placing the online gaming industry in a dominant position. Some of the games, like Candy Crush, PUBG, etc., attract the youth population at large; other than the younger people, older people also may be attracted to the gaming industry. By knowing the pulse of gamers, the developers focus on creating content based on the choices of gamers, which leads to the development of this section.

[1] Author is an Assistant Professor at Vignan Institute of Law, VFSTR, Vadlamudi, Andhra Pradesh & Research Scholar (PT) at SPMVV, Tirupati, Andhra Pradesh, India.
[2] Author is an Assistant Professor at Vignan Institute of Law, VIGNAN's Foundation for Science, Technology & Research (Deemed to be) University, Vadlamudi, Andhra Pradesh, India.

 [ISSN 2581-5369]

To begin with, the involvement of the legal framework in the online gaming industry started with the Information Technology Act, 2000. There are several provisions of the IT Act, 2000, providing the regulations for online games to protect the players, which help to maintain privacy and also mitigate the risk of cyber threats. The Government of India is also taking initiatives to promote online gaming, making India one of the gaming hubs in the country. The Promotion and Regulation of Online Gaming Act, 2025, also helps to strengthen the gaming industry by providing the regulations of online money games, customer protection, and promotion of e-sports, etc. Apart from these legislations, there are many laws such as the Information Technology (intermediary guidelines and online media ethics code) Rules, 2021, online gaming rules, 2023, and the Online Personal Data Protection Act, 2023.

The terms cybercrime or cyber threat are not explicitly defined under the IT Act, 2000, and any other legislation. The crimes/offences are defined under the Indian Penal Code, 1860 (now BNS), and it also prescribes the punishment for defined offences. However, the term online game is defined as follows: "*any game, which is played on an electronic or an online device and is managed and operated as software through the internet or any other kind of technology facilitating electronic communication".* [3]

A cyber threat is a malicious action that occurs through the computer system. it creates a negative impact by carrying off the sensitive information relating to both the users and developers. Cyber threats may occur in several forms, such as identity theft, DDoS attacks, malware, and ransomware etc., resulting in financial loss, and the families of the users are also at stake. Privacy is one of the major concerns in this online era. At the same time, using the mobile computer system tabs for games allows players to provide their personal information to access a login for a better gaming experience, which can result in misuse by hackers and third parties.

II. TYPES OF CYBERCRIME IN MONEY-RELATED ONLINE GAMING

As per the Indian Cybercrime Coordination Centre (I4C), cybercrimes in India are broadly categorized under the following: Cryptocurrency Crime, Cyber Terrorism, Hacking/ Damage to Computer Systems, Online and social media-related Crime, Online Financial Fraud, Publishing or Transmitting of Explicit Material in Electronic Form, Ransomware, and Child Pornography/ Child Sexual Abuse Material. Cybercrime in money-related online gaming comes under the heads of Online Financial Fraud and Online & social media-related Crime,

[3] The Promotion and Regulation of Online Gaming Act 2025, s 2(f).

 [ISSN 2581-5369]

respectively. These crimes are further subdivided under different subtypes such as –

a. Phishing

Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc., through emails that appear to be from a legitimate source.[4] In pushing the online gaming websites, stealing the banking details of gamers, like Credit/Debit Card numbers, along with Expiry date and CVV for validating the gaming account. Due to the non-compliance, the gaming websites are threatening to the gamer and also selling the banking details on the black market, as a result, they are using the banking details for financial purchases from the gamer's account without knowing to the gamer.

b. Account Takeover and Identity Theft

During the account takeover, the attacker unauthorised accessed the gamer's account and stole the personal information of gamer along with the wallet amount (Virtual currency) or game assets. As a result of this, some gamers lose their dollars of gaming earnings because of account takeover. In Identity theft, cybercriminals theft the individual's information by various methods, such as personal details, and use the same information for opening new financial accounts or for financial fraud.

c. Malware and Ransomware

Malware and Ransomware are kinds of malware or kinds of malicious software programs that damage the computer program or steal the personal information, login details, and monitor the activities. This has happened with gamers because of unauthorised downloading of games or cracked versions of games.

d. Money Laundering

In money laundering, the real money gaming (RMG) platforms like fantasy sports, poker, and skill-based contests allow users to use that money for online gaming. In this type, they are converting illicit money into the online gaming platforms.

e. Scams and Fraud

In gaming scams and fraud, gamers are spending their virtual currency to purchase gaming assets or gaming items, but they never receive that things to the gamer. This opens the door to

[4] Indian Cybercrime Coordination Centre, CrimeCatDes.aspx (National Cybercrime Reporting Portal) https://cybercrime.gov.in/Webform/CrimeCatDes.aspx accessed 2 December 2025.

 [ISSN 2581-5369]

in-game scams and marketplace fraud.[5]

f. Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) Attacks are the most common kind of attack in which an attacker attacks the game's server with fake traffic, which leads to the game crashing and the computer altogether.

III. LEGAL FRAMEWORK OF ONLINE GAMING

In India, there are several laws to protect online users from different kinds of cybercrimes, such as identity theft, privacy concerns, and financial fraud, specifically in the online gaming landscape, as follows –

a. Information Technology Act, 2000

It is a comprehensive legal framework for regulating online gaming by addressing various cybercrimes, including unauthorized access to computers and fraudulent activities related to computer systems. To protect the users, there are several provisions under the IT Act, 2000, regarding the responsibility of intermediaries for online gaming platforms. These provisions are helping to prevent identity theft and address privacy concerns, which are largely prevalent in our society.

The intermediaries of online gaming platforms have an exemption from liability as a safe harbour according to the provisions provided by the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. Intermediaries have a responsibility to maintain the privacy and safety concerns of the users. As a part of this, the intermediaries have to adopt the rules as follows –

- Intermediaries should develop clear policies on real-time money games in terms of withdrawal process, KYC authentication, and fees to maintain the immunity of safe harbour and create safe gaming practices.
- To prevent financial fraud and maintain accountability in real money games that are permitted by legislation, while accepting the deposits from the users, intermediaries have a responsibility to verify the user identity, like banks.
- As per the rules, intermediaries shall maintain the user information for a period of 180 days even after cancellation of registration and also take reasonable measures to protect

[5] Cyber Management Alliance, 'Game Over: 5 Types of Cyber Attacks Threatening the Gaming World' (Cyber Management Alliance Blog) <https://www.cybermanagementalliance.com\> accessed 30 October 2025.

 [ISSN 2581-5369]

the information stored in the computer resource.

- Grievance redressal mechanism has to be established by the intermediaries to address the complaints, which have to be resolved within a period of 15 days.
- Intermediaries also monitor the content shared by the users to prevent the prohibited content from circulating in online sources, and if that cases occur, intermediaries take necessary steps to remove the content that is harmful to other users.

b. Promotion and regulation of online gaming bill, 2025

The Promotion and Regulation of Online Gaming Bill, 2025, was introduced by the Parliament on 21st August, 2025, with the main objective to regulate online games, consumer protection, and ensure transparency. The central government has the authority to make the rules for the regulation of online gaming platforms, and it has jurisdiction all over India, and is also applicable to online gaming services provided in India or from outside India. This bill restricts the real money games in the nature of skill, chance, or both, and also prohibits banks and other financial platforms from transacting financial transactions regarding online gaming platforms. To investigate the offences, the central government appointed officers having the power of search and seizure of the computer sources provided by the criminal procedure code.

The Central Online Gaming Regulatory Authority (COGRA) was proposed by this bill to monitor the gaming platforms, issuing licenses, facilitating the guidelines for users and protecting the consumer interest. This bill also introduces the licensing process to register games like skill-based, educational, cultural, and social games. It plays a major role in impacting society by expanding the opportunities and encouraging youth to participate in skill-based games, which help to create employment opportunities along with economic growth. This bill also proposed a stringent punishment for non-compliance with the rules, including providing a platform for prohibited online games and encouraging financial transactions related to them.[6]

c. Digital Personal Data Protection Act, 2023

This Act was enacted by the parliament on 7th August 2023 to protect personal data collected and processed in digital form. This Act playing a significant role in addressing privacy concerns in online gaming through making companies mandating to obtain consent for data collection, access and removing data from online landscape. This Act only deals with the data which is collected and maintaining in digital format or converted into digital form in India. The main

[6] Promotion and Regulation of Online Gaming Bill, 2025 (Backgrounders, Press Information Bureau, Government of India).

 [ISSN 2581-5369]

provisions of this Act are as follows –

- This Act provides for the provision of data fiduciaries, which help to collect and maintain the data.
- It makes fiduciaries mandatory to obtain free consent without any compulsion and misrepresentation from the individuals during their personal data collection and processing to maintain transparency. Individuals also have the right to withdraw their consent at any time.[7]
- As per the provisions of this Act, any person under the age of 18 years and persons with disability need to provide parental consent for data processing, and fiduciaries also have a right to advertise the prohibited norms for children's data collection without their parents' consent.[8]
- This Act provides several rights to individuals concerning their data maintained by the fiduciaries, such as the right to ask summary of data, nominate a representative in case of death to deal with their data rights, approach the board to address the disputes, and request corrections, if necessary, etc.
- The Data Protection Board of India (DPBI) was established by the central government to address the grievances regarding data protection, data breaches, and imposing penalties. The decision given by the board is also appealable to the Telecom dispute settlement and Appellate Tribunal.

IV. LANDMARK JUDICIAL PRONOUNCEMENT

A. Shreya Singhal v. Union of India*, (2015) 5 SCC 1*[9]

In this case, the Honourable Supreme Court has Section 66A of the Information Technology Act, 2000 and read down Section 79 (intermediary liability), because of this, social media platforms or any e-commerce platforms are not responsible for the users' created content, but these platforms are responsible if they did not remove that content even after being notified by the government. In relation to online gaming platforms and privacy concerns, many times these platforms play a dual role as like communication or content platform. Because of this judgement online platforms cannot arbitrarily force to censor or compile the user to block the content. It is

[7] Digital Personal Data Protection Act 2023, s 4 (India).
[8] ibid s 9.
[9] Shreya Singhal v Union of India (2015) 5 SCC 1 (SC).

 [ISSN 2581-5369]

relevant because now, as the technology develops, and according to the user's requirement may gaming apps may play a dual role like a social media chatbot and a gaming content platform.

B. Puttaswamy v. Union of India (2017)[10]

In this case, the Hon'ble Supreme Court adjudicates the privacy concern of an Individual when private parties or state authorities require the personal data, like Aadhar KYC details of users. SC, in this case, held that as per Articles 14, 19, and 21, "Right to Privacy" is the fundamental right. With regards to online gaming or personal data protection, this judgement provides the user's information protection from private parties or state authorities from personal data like Aadhar KYC details.

C. Play Games 24x7 Private Limited & Anr. v. State of Tamil Nadu & Ors. (2025)[11]

The Madras High Court upheld the validity of the Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act, 2022, and the associated regulations (2025), which mandate Aadhaar-based KYC for online real-money games (RMG), impose a "blank hours" ban (midnight to early morning), and other restrictions.[12]

In this case court held that privacy is not an absolute, public interest, and social well-being is also important may also be necessary, as the reason the court permits KYC or Aadhar verification in this case.

D. Directorate General of Goods and Services Tax Intelligence (HQS) & Ors. v. Gameskraft Technologies Pvt. Ltd. & Ors. (2025)[13]

In this case, the Hon'ble Supreme Court stayed the notices issued by the GST Department on 49 online gaming companies regarding the demand of 1 Lakh Crore rupees Tax. In the same decision Supreme Court said that regarding the online gaming platform, there is a lot of fraud and privacy concerns. For this reason, it is legitimate to incorporate clear legislation regarding online gaming rather than a blanket crackdown.

V. CHALLENGES OF PRIVACY CONCERNS IN ONLINE GAMING

Due to the development of technology, mobile phone usage increases in every age group for the entertainment purpose and many peoples are using the social media platform and gaming

[10] Shreya Singhal v Union of India (2015) 5 SCC 1 (Supreme Court of India).
[11] Play Games 24x7 Private Limited & Anr v State of Tamil Nadu & Ors [2025] Madras HC WPs Nos 6784, 6794, 6799, 6970, 8832 & 13158.
[12] Play Games 24x7 Pvt Ltd and another v State of Tamil Nadu and others (Madras High Court, 2025) LiveLaw (Mad) 185.
[13] Directorate General of Goods and Services Tax Intelligence (Hqs) & Ors v Gameskraft Technologies Pvt Ltd & Ors [2024] SLP (Civ) Nos 19366–19369/2023 (SC).

platform like fantasy gaming, e-sports, Candy Crush, PUBG. For using this online platform, gamers are giving various permissions by default which resulted into many socio-legal privacy concern happened which are mentioned as follows –

i. Gaming companies taking personal data from the individuals with consent, even though they are not aware of the information on which they have given consent.

ii. While online gaming using voice chat or face recognition by minor's leads to create fake identity which can be used in crime.

iii. Theft in the gaming account leads to financial and emotional losses to gamer.

iv. In online gaming children are often providing the personal information which is not known by the parents leading to privacy features or term and conditions of online gaming platforms.

v. In online gaming users are unaware of their legal rights under Digital Personal Data Protection Act, 2023 (DPDP Act).

vi. Many gaming platforms are allowing the minors for online gaming without any KYC details or personal information.

vii. Many online gaming platforms are located outside the India it leads to cross border data transfer.

viii. Misuse of financial information by online gaming platform it leads to financial losses.

ix. Weak enforcement of Digital Personal Data Protection Act, 2023 (DPDP Act) which leads to lack of jurisdiction, and lack of child specific safeguards under the law.

x. Legislation regards on cyberstalking, identity theft, data breach exist but no specific online gaming standards in India.

xi. In India lack of gaming related privacy concern and consumer protection in online gaming.

VI. Conclusion

Privacy is an essential element in every individual's life. Because it protects the personal dignity of individual and promote the human rights. Due to rapid growth of technology, this privacy concern is at stake. Specifically, in online gaming landscape this privacy is playing a significant role by protecting from identity theft, phishing, malware, ransom ware and misuse the data collected by the fiduciaries etc. To curb these cyber issues, legislations provided stringent rules through the punishments and penalties. In this concern, judiciary also taking initiative to protect

 [ISSN 2581-5369]

the privacy of individuals through the judicial pronouncements which are directly related to addressing the privacy issues in cyber space. However, there are several challenges often faced by the users as well as the fiduciaries such as lack of transparency, strict implementation of laws and lack of awareness on cyber issues etc.

*****

 [ISSN 2581-5369]