CYBERSECURITY BREACHES IN INDIA'S ONLINE GAMING ECOSYSTEM

Maithly Jain, Law College Dehradun, Uttaranchal University

Ashok Dobhal, Law College Dehradun, Uttaranchal University

ABSTRACT

An exponential growth has occurred in the digital economy in India, making the online gaming segment one of the fastest-growing digital segments in the world. But it's grown faster than the lagging security protocols and statutory mechanisms in the country and caused a vastly larger and vulnerable attack surface. This paper explores the structural vulnerabilities of the Indian online gaming ecosystem, including the use of weak identity verification systems (KYC), vulnerable Application Programming Interfaces (APIs) and insecure third-party external payment mechanisms, as the major opportunities for malicious attacks. India's legal framework is rooted in the Information Technology (IT) Act 2000, and is rife with deep operational divisions in the statutes.[1] This study shows how the territorial approach of the old laws is not capable of countering automated and borderless digital threats like Remote Code Execution (RCE) and Distributed Denial-of-Service (DDoS) attacks through a critical legal analysis of them, namely Section 43A (negligent data protection standards), Section 66 (computer-related offenses), Section 79 (intermediary safe harbour immunity), and Section 85 (vicarious corporate liability). In addition, the paper identifies key systemic weaknesses, such as the fact that a lot of reports are still delayed after 72 hours, jurisdictional restrictions on jurisdiction over offshore servers, corporate implementation of safe harbour provisions and devastating capacity gaps in the local law enforcement cyber cells.[2]

The Indian courts have been filling a legislative void, especially due to a weak legislative framework. It charts a unique trajectory towards more aggressive judicial supervision as seen in the world-famous security audit decision in 2025 by the Delhi High Court, the enforcement of compliance by the Karnataka High Court and in individual cases by state consumer forums. It contends, however, that the less interventionist judicial response approach

[1] N. Pandey & S. Tarun, *Regulatory Progress and Challenges in India's Booming Online Gaming Market*, 2024 Online Gaming India 49, 49–61.

[2] S.T. Shrivastava, *Cyber-Security and Data Privacy Challenges in Online Gaming: Analyzing the Cyber-Security Risks and Challenges Faced by Online Gaming Platforms in India*, *in* Online Gaming in India 118, 118–25 (2024).

can never go far enough to prevent permanent, real-time exfiltration of data, and so will inevitably result in structural limits that expect Supreme Court cybersecurity directives.[3]

Lastly, the paper analyzes the paradigm shift in the world of online gaming, spurred by the two new sets of rules, namely, the Digital Personal Data Protection (DPDP) Rules, 2025 and the Promotion and Regulation of Online Gaming (PROG) Rules, 2026. This modern regime, led by the newly formed Online Gaming Authority of India, will have a new style of enforcement, kicking into the online arena, with the multi-crore fines being scaled and a strict distinction being made between banned online money games and online e-sports and social games. Finally, the study proposes a co-regulatory framework that will strike a balance between the need for innovation protections and an irrefutable user safety imperative and suggests embedding proactive, automated technical compliances into the very design of platforms to protect citizens' privacy in the digital era.

Keywords: Privacy Rights, Data Privacy, Online Gaming, Cybersecurity Breaches, Information Technology Laws, Intermediary Liability, Digital Personal Data Protection Act, PROG Rules 2026, India.

Introduction

Gambling is a $3.5 billion juggernaut in India taking over more than 500 million users of its more than 140 million gaming devices every day. The Indian gaming industry has however turned into a luring hotspot for cybercrimes due to the magnified volume of players/ users. Over 84,000 users had their gaming information breached last year and there is regular coordinated DDoS attacks being made on offline servers. New information technology rules race with the real-life threats.[4] This explosive growth is the result of the ease with which targets are created behind the backs of millions of users, who are adjusting their lifestyles to the platform for online gaming. The infrastructure is the one that causes high speed and ease of use and, now, it is under the burden of the constant threat to security. This industry is about working outside the privacy of the data, knowing who you are and how you spend your money and things. Indian government should take a closer look about their functioning to benefit the Indian citizens.[5]

[3] V. Singhania & P. Talukdar, *In Regulatory Purgatory: How Many Lives Left Before Mission Success for the Indian Gaming Industry?*, *in* Online Gaming in India 27, 27–37 (2024).
[4] V. Kumar, *Critical Analysis of the Promotion and Regulation of Online Gaming Act, 2025 in India: Constitutional and Stakeholder Perspectives* (2025).
[5] V. Rishiwal et al., *Blockchain-Secure Gaming Environments: A Comprehensive Survey*, 12 IEEE Access 183,466, 183,466–488 (2024).

Indian gaming is an extraordinary sector facing growth itself and still set to be buried by deep uncertainty in the law. As an effect, a need emerged for the government to step up to get control over this massive digital migration. The ministry of Electronics and Information Technology (e-I) is the nodal ministry that leads in the matters of Gaming oversight and thus, the Ministry of Electronics and Information Technology has come up with a set of Information Technology Amendment Rules to finally introduce some regulation, including in the online gaming domain, with the participation of intermediaries known as Online Gaming Intermediaries (OGIs) and the self-regulatory bodies (SRBs). As gatekeepers of their respective industries, they can only be made public once they have been reviewed and formally approved by the SRB, which has to be done in strict compliance with special rules. If the game is being utilized by users, the platforms are required to keep "due diligence" as per the IT Rules. This co-regulatory approach aims to strike a balance between fast changes and the need for legal frameworks to be structured.[6]

To tackle these different challenges, the Government has passed the "Promotion and Regulation of Online Gaming Act, 2025". The new act is geared toward the security of the gaming platforms. The current game industry, with its complexities (including server sabotage), is far too complicated to be addressed by the IT Act of 2000. As a matter of fact, we are still stuck running towards the traditional litigation system, which can only help afterwards, when the breach has already been occurred.[7]

The foremost objective of this study is to take a leap from critical analysis of the digital regulations, and to provide analysis of the failures in Indian law in the field of gaming. Secondly, to evaluate the efficiency of judicial action in order to react accordingly with remedies. Ultimately, the aim is to provide proactive reforms for converting our traditional litigation method towards a mandatory and resilient legal framework that can help in shielding the users across the gaming industry.

Gaming Ecosystem Vulnerabilities

The gaming industry is in transition to become a well-connected environment and this provides an environment where malicious attacks can occur. It is estimated that it will have 700 million

[6] J. Simser, *Dangerous Play: AML/CTF/CPF Risks in the Gaming Sector*, *in* The Financial War on Crime and Terrorism: Opportunities and Challenges 225, 225–44 (2026).
[7] A. Punia et al., *The Security and Vulnerability Issues of Blockchain Technology: A SWOC Analysis*, 18 Peer-to-Peer Networking & Applications 173, 173 (2025).

users by 2027 and malicious activity is growing accordingly, with roughly 37% of all the DDoS attacks over the past few years being malicious. Users of the online platforms rely on one another, and are always the subject of cybercriminals with a bad intent. Public cloud infrastructure is frequently used by developers to meet the demands of today's multiplayer video games, which can sometimes be lacking in a strong security system. In today's game systems, phishing links and trickery signals like embedded messaging in a game are now being used to trick users and encourage them to compromise their own data protection. Cheat downloads have malware to enable the installation of remote code execution (RCE) attacks. Such vulnerabilities can provide help to the attackers in compromising both the game server and the end user's device along with data privacy. [8]With the advantages in the minds of the users and with these vulnerabilities, cybercriminals can come up with their competitive advantages, which in turn can bring them to the 'grey market.' The proliferation of new forms of game and cryptocurrency have added new dimensions to financial terrorism. Often these sorts of websites are passed through via an compromised gaming account to hide where the money is coming from. There are other ways that the online platforms can be exploited by those with malicious intent, in addition to the classic technical exploits involving using artificially intelligent tools to analyze data and exploit game code or specific vulnerabilities in the game.[9]

Flaws in identity verification procedures, insecure API endpoints, and vulnerabilities in external payment processing systems are highlighted in the Indian industry. The following are platform-level security threats to blockchain security: blockchain platforms can have gaming platforms, vulnerable Application Programming Interfaces (APIs) can be integrated, and third-party payment providers can be integrated, creating 'endpoint vulnerabilities. A key factor that contributes to the attack surface is a weakness of the Know Your Customer (KYC) and APIs exposures. The weak component of a distributed ledger is third-party payments.[10] The gaps in the infrastructure mean that the gaming industry has operational and reputational risk factors from a business perspective. Regulatory review is a concern, and can adversely impact user trust, which can lead to data breaches. Furthermore, this also opened the possibility of financial liability, which could be a major hurdle for a safe development of the ecosystem as it would

[8] H. Ozalp et al., *Disruption in Platform-Based Ecosystems*, 55 J. Mgmt. Stud. 1203, 1203–41 (2018).
[9] A. Ibrahim, *Guarding the Future of Gaming: The Imperative of Cybersecurity*, *in* 2024 2nd International Conference on Cyber Resilience 1, 1–9 (2024).
[10] S. Chanda & A. Choudhary, *Blockchain in Online Gaming: Navigating the Legal Landscape for India and the World*, *in* Online Gaming in India 126, 126–41 (2024).

compromise the security of the platform.[11]

Most important today, both data breaches and personal data are found on the modern technological platforms, with financial credentials being used for microtransactions, and identity data being used for identification theft. Generally, it's those user accounts that are valuable in the real world that are attacked. Many years of creative work and technology creation are at stake if the internal development is not protected from cybercrimes. Cybersecurity focuses on equality of the experience. In some instances, aim-bots can be considered as a breach of the game logic as they are not supposed to be there. Cybersecurity could be considered the most critical element for making sure that the gaming spirit is as malicious free as you can.[12]

Legal Framework Analysis

Out of all of the legal support, the most basic law which is found in the medicine cabinet of the gaming industry is the Information Technology (IT) Act, 2000, otherwise known as a fundamental law which can be referred to as the standard base for Digital injuries. It's essential to have a critical analysis of strategies that are the backbone of how blockchain is used, data privacy and a clear legal framework to make working secure within the borderless technology. Gaming sector is rapidly moving towards the transparent use of digital ledger technology (DLT), powered by blockchain. This change from player to owner has been a complex legal landscape in the changing regulatory environment in India.[13]

The first information in the arsenal of every player whose information has been leaked is section 43A of the IT (Information Technology) Act, 2000. This section offers, "If you're being liberal with user data, but stingy with security, you are going to have to pay. The players use cheat codes which they learn and understand from the internet, not knowing that most of the such cheat-codes are manipulated by the deceptive malware which is created by cybercriminals with a malicious mind to make the players or users unaware of it and manipulate the workings of the same. When the same is being used, it is necessary to provide proper statutory legal

[11] P. Gulati & K. Pal, *The Notion of Privacy Rights in the Metaverse: Examining Legal Hemispheres in India's Digital Era*, *in* Metaverse Driven Intelligent Information Systems: Emerging Trends and Future Directions 159, 159–76 (2024).
[12] B. Rajput, Cyber Economic Crime in India 9–10 (2020).
[13] U. Pareek & N.A. Sole, *Seizing the Networked Crime: Legal Framework for the Governance of Social Media Crimes in India*, *in* Big Data Analytics in Cognitive Social Media and Literary Texts: Theory and Praxis 165, 165–82 (2021).

framework as if it is allowed to run freely in the computer, it will certainly infringe upon the privacy of the users as it is clearly a Virus in the computer so what are the limits? [14]

When a criminal prosecution under the IT Act, 2000 section 66 is conducted with intent, it becomes a failure of cyber security, turning negligence into intent. Under this law, punishment is provided for the hackers in its section 66. If it is determined that any violation of Section 43 is made dishonestly or fraudulently, the penalties outlined above are also applicable. A hacker who accesses the data without permission, injects malware, or does any other sort of damage to a data base, for example, may be subjected to prosecution. Under this law, the hacker being convicted will face imprisonment of up to three years or a fine of up to Rs 5,00,000 or both. Many of the structures of the application of Section 66 in online gaming reveal that there are many problems in its application in this field. The law also uses the same criminal intent tests when it comes to data theft as it does when it comes to the theft of physical data. These tests are easy to conduct for conventional data thievery, but are not very clear in the current complicated use of automated exploits. For example, Remote Code Execution (RCE) and Distributed Denial of Service (DDoS) attacks can be used to disrupt the operation of a game. However, these activities could be some sort of taking of a physical asset. Hackers could be filling thousands of API endpoints and disrupting operations on the server without gaining access to any assets or they could be making memory buffers. The law doesn't define what constitutes server sabotage, or automated botnets and manipulation of game code. This void requires outdated definitions for prosecuting and adjudicating cutting-edge technologies. As a result, prosecutions under Section 66 in gaming are rare. A greater deterrent effect by the law is the only protection that players actually have as there are no means of protection in place.[15]

According to the provision of Section 67C of the IT Act, the intermediary shall keep the following information for a certain period of time: Logs of the traffic and user's information. This section is the legal requirement for cyber-forensics that is responsible for keeping the server "black box" and not wiping off IP addresses, session history and access logs from the time of the exploit.

[14] A. Roy et al., *Deepfakes: Navigating Ethical Concerns and Legal Frameworks*, *in* International Ethical Hacking Conference 337, 337–55 (2025).
[15] N. Sun et al., *Data-Driven Cybersecurity Incident Prediction: A Survey*, 21 IEEE Comm. Surveys & Tutorials 1744, 1744–72 (2018).

The gaming industry is a very fast paced environment with millions of pings of API's and micro-transactions per day, and a huge resource cost to keep this information available. The platform uses poor data hygiene methods to save storage costs, this will have a negative impact on the preservation of exact forensic evidence and will not have the necessary logs to recreate the breach.[16]

One of the most controversial measures in digital laws is Section 79, "Safe Harbour for Intermediaries". This section will exempt any gaming platform from any liability for any data, links to third parties or harmful files hosted on their platform. This section is designed to encourage innovation in digital games and the unequal nature of the Safe Harbour has resulted in many gaming platforms not taking compliance seriously. Platforms can choose to see Section 79 as a full-blown barrier to structural accountability. For example, in a global tournament, a malicious user might post a link to malware in a chat, or use an unsecured API. Platforms will often claim a lack of prior knowledge of the act. This has resulted in a very reactive security culture, making the players very vulnerable in 'Real-Time'.[17]

What is required now is to have a new paradigm of accountability by establishing a 'Vicarious Corporate Liability' under Section 85 of the IT Act and merge cybersecurity with IT. This provision provides that if a corporation commits an offence in relation to the IT Act, the law deems each of its directors, managers and executive officers, who supervise and manage the affairs of the company to have committed the offence. The executive(s) responsible for running their company's information security policies and procedures should not pass the buck because of the company's name and say that they can't be held accountable if a data breach occurred due to poor KYC processes or "cutting corners" with regards to encryption. Specifically, the executives in charge of the management of gaming companies must take the protection of an individual player's digital identity and financial resources (wallet) as seriously as the financial success of the gaming company.[18]

In our country, there have been occurrences. When PUBG was banned in 2020, under Section

[16] S.A. Bagul, *Guarding the Digital Gateway: An In-Depth Analysis of Cybersecurity Challenges in India*, *in* Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics 67, 67–92 (2025).
[17] S.N. Mohanty et al., *A Study on Building Awareness in Cyber Security for Educational System in India Using Interpretive Structural Modellings*, 15 Int'l J. Sys. Assurance Eng'g & Mgmt. 2518, 2518–28 (2024).
[18] A.P. Sai, *Cross-Border Challenges in Combatting Digital Piracy on OTT Platforms: Legal Frameworks and Enforcement Gaps in the Global Media Landscape*, *in* 2025 International Conference on Sustainability, Innovation & Technology 1, 1–6 (2025).

69A of the IT Act, it was a clear demonstration of the threats to the country and its control as our users' personal data were being sent to servers of other countries. The same was the case with Dream11 – first where the real gaming accounts of people were more vulnerable to attackers using the stolen information of the players and secondly, where the definition of "good enough security" under the IT Act under section 43 A was open to interpretation. In the same way, other games such as BGMI have also encountered the same kind of issues with their servers that hindered the running of large-scale events. Although the competition has been significantly harmed, it is very difficult to trace back and determine the source of these attacks, due to its server in other country, showing that our law is not ready to deal with these transnational attacks. The games will continue to face such issues.[19]

Core Legal Challenges

Financial issues are hampering the first layer of defense in gaming against cyber threats. If there is to be a data breach, it's a matter of being transparent. But, most of our country's gaming sites are not prompt to inform users about such hacks, in most cases it takes 72 hours. Players usually don't know that their database is being hacked during the hack. These platforms would usually patch up the problem and deal with reputational consequences. If this information is for sale on dark web forums, millions of players are at risk of falling victim to Identity theft. Another challenge is the legislation is not adequate to prevent this, the cyber-attack fee for 5 lakhs is not sufficient to make major companies and cyber criminals think twice. For these groups it merely translates to a cost of doing business, rather than being serious about a high-level of security. There's a need to own up to the gaming industry.[20]

For a cybercriminal, 'national boundaries' do not exist. But for India this is a huge drawback as the laws applied are based on India. India is also able to deal with computer related offences that are perpetrated outside its borders, under the IT Act. In fact, most of the servers aren't in India and so cannot be reached by the law. The hurdle for Indian police is that they come across a wall when they need to obtain any data from another country's server to conduct any investigation into cybercrime occurring from a foreign server. For implementation of the laws, India will have to enter into bilateral treaties with the countries to obtain information that will

[19] K. Singh & K. Rizvi, *Responsible and Ethical Framework for Online Gaming: A Shared Responsibility*, *in* Online Gaming in India 242, 242–55 (2024).
[20] S. Siddamsetty et al., *Designing Cybersecurity Ecosystems: Lessons from the Kyiv Breach and the ECLIPSE Economic Model*, *in* 2025 International Conference on Intelligent and Secure Engineering Solutions 857, 857–62 (2025).

help it catch cybercrime offenders. It seems to be a breach of the legislation. A lot of the companies exploit a law which states that they are not responsible for any occurrence on their platforms. The companies cite being intermediaries between the users and the networks, claiming their lack of knowledge. Indeed, the companies do know but are choosing not to take a step to do anything about it. They are leaving their systems vulnerable for criminals to be able to easily steal from them. The Government is giving these companies immunity for anything that takes place on their systems, unless they're told by them of any action. This is detrimental to the issue of cybercrimes as the cyber criminals would not be apprehended and are free to exploit Indian cyber space in any manner, since the companies would continue to allow it by not taking preventive measures. It would only be the cyber criminals who would take advantage and the cyber space of India is becoming unsafe.[21]

Judicial Remedies Examined

When IT Act machinery breaks down or is unable to respond it falls upon the courts to ensure that individual's rights are maintained. In online gaming courts are stepping outside the role of merely adjudicating private disputes between companies and becoming part of the regulatory landscape. With the increasing incidents of data breaches and platforms not taking responsibility, the Indian cyber laws are being interpreted and altered by judges.

In 2025, court involvement in corporate negligence in relation to cyber security was the order of the day. The Delhi HC had to make a judgment in the PUBG Hack Case 2025. The large data exposure exposed user information and even their bank details to threat actors and hackers around the world. Instead of giving a warning the court had ordered a security audit of the platforms network, more specifically focusing on API endpoints and payment gateways, along with ordering an award of Rs 2 crore in damages. This made it easier to generate profit using user data leakages than to updating systems. The Karnataka High Court followed suit in a case that saw a real-money gaming platform refusing to accept its liability for allowing a data breach and not reporting it within the specified period. The platform had to go through CERT-In compliance verification and the 6-hour period of breach notification was a must for any company that wishes to operate in the country, according to the court. With their decisions in

[21] K. Priyanka et al., *Strengthening Cybersecurity in India's FinTech: E-Governance and Financial Literacy Against Digital Fraud*, *in* International Conference on Information and Communication Technology for Competitive Strategies 401, 401–10 (2024).

favour of the people's rights and imposing such kinds of penalties, the courts are doing an excellent job in tackling cyber threats from the organizations operating in India.

In the event a cyber challenge impacts the people citizens are resorting to a unique provision in the structure referred to as Article 226 Writ Jurisdiction. In case of any cyber challenge impacting the people citizens are turning to a unique provision of the structure known as Article 226 Writ Jurisdiction. This is the authority that will enable a person or persons to go to a state High Court without having to take matters to a lower court, and state that the security concerns on the platforms violate their right to privacy. The Right to Privacy can be found in the Constitution under Article 21. The advantage of an Article 226 writ is that it is general in nature. A High Court can compel the bodies such as MeitY/CERT-In to perform its duties and investigate platforms that are not performing well. It also will prevent an application from operating while they work on fixing the issues. This has resulted in Public Interest Litigations (PILs) directed towards addressing cyber issues. No, activists and legal groups are not waiting for a problem to occur. They are using PILs to take parts of the gaming industry to court. This means that judges will consider the points they take, such as unreliability of verification or unsafe payment methods. These PILs are putting High Courts in the shoes of tech regulators. They fill in where the states leaders have failed. The courts are doing so to safeguard citizenry against cyber threats. [22]

No one in India can unite and act to combat cybercrime. Attempt to go to law to get help – difficult. This takes many years. Requires a lot of paperwork, including individual notices and establishing like interests. As a result, when a platform leaks millions of records it only has to deal with a people who can afford to take them to court. Most people affected simply have to get over it. They have no means to make resistance as a group. Long as India doesn't have a better system for people to join together and take action it will be hard for people to hold companies accountable, for cybercrimes. The existing system will continue to safeguard business and not people. India must have a mechanism which will facilitate people to act in concert. This system should be designed to deal with the challenges of cybercrimes.

Conclusion

Blockchain technology has the potential to transform India's digital economy, as it meets the

[22] M.K. Brar et al., *Balancing Play and Protection: Public Health Risks and Regulatory Measures in India's Online Gaming Landscape*, 57 Simulation & Gaming 299, 299–327 (2026).

advanced metrics and online gaming. However, the current law does not sufficiently reflect the particular needs and concerns of this emerging sector. In fact, the old IT Act, 2000 is not adequate to meet these changes. But this is a legislation that leaves much room for interpretation, ambiguity as to data security, and trivial punishments for hackers, and which has left companies complacent and more interested in building up their user base than in developing adequate security.

The good news is that India's attitude towards regulation is changing quickly. The recently implemented Digital Personal Data Protection Rules 2025 are a new development from the previous era. These rules suggest the creation of a Data Protection Board that will oversee the data protection practices and harsh penalties will be imposed on companies that do not ensure that their user's data is properly safeguarded. The balance between regulation and a less rigid interpretation of innovation will be crucial to the future of the gaming industry in India. Excessive regulation can hinder innovative concepts and compel Indian game developers to migrate, and insufficient rules can compromise users' privacy and security.

Henceforth, it is imperative for the government to collaborate with gaming and blockchain firms to ensure compliance. It can implement measures like leveraging technologies, such as blockchain, that help ensure company compliance. The Digital Personal Data Protection Rules, 2025, and relevant laws should be called into action to safeguard users' privacy and security. Creating such an environment will enable India to establish a niche where gaming industry can thrive while blockchain technology remains robust without sacrificing user safety and data protection.