(JOINT JURIST)

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL] |
VOLUME 1 | ISSUE 1 | MAY 2026

ABOUT THE JOURNAL

The **Joint Jurist Journal (JJJ)** is a strictly law-focused national publication designed to bridge the gap between academic research and litigation expertise. We operate on a **Double-Blind Peer-Review** model, ensuring that every published work meets the highest standards of original scholarship and academic integrity. Our platform is dedicated to providing an openaccess environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **Dr. Seema Gupta**
- **Dr. Mohd Rafiq**
- **Dr. Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**

NAME	DESIGNATION	INSTITUTION/AFFILIATION	SPECIALIZATION & IMPACT
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	**High Court of Himachal Pradesh**	IPR Specialist, Courtroom Strategy & Legal Research.
Prof. (Dr.) Seema Gupta	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**	Constitutional Law, IPR, & Supreme Court Certified Mediator/ Interdisciplinary Legal Studies.

| VOLUME 1 | ISSUE 1 | MAY 2026

"INDIA'S ONLINE GAMING BILL 2025: DATA PROTECTION, VPN CIRCUMVENTION AND GLOBAL COMPLIANCE UNDER THE DPDP ACT AND GDPR"

AUTHOR: SUBHASREE BOSE | STUDENT (2ND YEAR), AMITY UNIVERSITY, NOIDA

ABTRACT

Global Online Gaming companies under scrutiny:The impact of India's Online Gaming Bill, 2025 on Data Protection, VPN Circumvention, and compliance with the DPDP Act and GDPR. The Global Growth of online Gaming has triggered complex debates on regulatory actions and data protection. India's Online Gaming Bill, 2025[1], provides a legal platform that blanket bans all forms of online money gaming on licensing as a necessity and provides blocking measures (Blocking rules) in compliance with these provisions. At the same h time, the strong enforcement of the DPDP Act (Digital Personal and Data Protection Act, 2023)[2] provides provisions, including children 's data, data processing, data retention policies, and restrictions on cross-border data flows. such provisions which remain the international data protection Regulations which remain the international data protection compliance standard. These regulatory Systems put the Global online gaming Platforms companies under different levels of scrutiny.

The widespread use of VPN (Virtual Private Networks), which allows Indian users to evade geo-blocking and access unlicensed on unregulated gaming, provides a formidable enforcement challenge. This scenario gives rise to unanswered accusations concerning the jurisdictions appointment of liability among platforms. Also, questioning the effectiveness of regulatory constraints in a borderless world, the VPN circumvention is explored as a distinctive element subverting both data governance and regulatory enforcement. the legal research work wants to approach a practical reality encountered by the international gaming business, all the while safeguarding users' privacy in an increasingly decentralized and vpn based online world.

INTRODUCTION AND BACKGROUND

One of the most rapidly expanding industries of the digital economy has been the internet games business with hundreds of web sites boasting of millions of gamers worldwide. It has also come with massive concerns on the regulatory, moral and data protection concerns on its growth. The world governments are faced with the Herculean task of ensuring that the economic potential of the online games is realized and protection against financial exploitation, misuse of information and addictive interfaces are provided. India has also seen a change in favour of Promotion and Regulation of Online Gaming Bill, 2025 ("Online Gaming Bill"), which is a proposed bill to introduce licensing requirements, prohibit games of chance, and give the authorities the right to access and block non-licensed sites. The Bill is a tectonic shift of the previous self-regulation model designed with the 2023 IT Rules, and it is also a move that testifies to the Indian intention to have more control over the gaming sector.

The connotations of regulation with regard to this Bill cannot be uncoupled. The Bill overlaps with the Digital Personal Data Protection Act, 2023 (DPDP Act), which is the first national data protection legislature in India. The DPDP Act stipulates on consent, data minimization, handling of data of children, and cross-border transfer of data, which play a significant role in online gambling websites, which traditionally handle sensitive personal and financial information of players. Meanwhile, foreign online gambling enterprises with European customers are covered by the General Data Protection Regulation (GDPR), the most powerful and significant data protection legislation globally. This point of regulatory intersection presents a complicated compliance challenge, where the questions of consistency, enforcement, and extraterritorial law are in play. The use of Virtual Private Networks (VPNs) by India is some of the causes of some of the issues of enforcement. Through a VPN an enduser can conceal their physical location and, thus, connect to a game platform that may be in a class that is prohibited or licensed under the Online Gaming Bill. This form of avoidance nullifies the effectiveness of geo-blocking strategies, confounds the distribution of liability between platform and user, and also presents major problems to the degree to which a state in an online borderless world can regulate.

The other field, which directs the State regulatory approach in India, is the parents patriae doctrine of the State, commonly known as the doctrine of the State as parent or father. This principle of judicial gives to the State a paternal, custodial role in respect of its citizenry-particularly weaker groups like children, orphans, and persons incapable of self-protection. Providing itself as a guardian to their safety, the State can step in even beyond natural guardianship in order to protect interests standing vulnerable to exploitation. Applied to online gambling, the doctrine defends the government in its argument of strict licensing, real-money gaming prohibition and the additional protection of children data and web usage which can be seen as a defense of the State as a protector and not a regulator.

Nonetheless, even though parens patriae further increases consumer protection, the State is subjected to colossal risks in an internet economy. Too much augmentation of the paternal position of the State may smother agency of individual, constrain rightful online behavior, and enable unproportional surveillance in the name of security. Overindulgence in paternalism may also put a freeze on creativity and the freedom of choice by adults in legal entertainment. Without open checks and judicial oversight, the doctrine can serve as a convenient shroud around an over-accumulation of data, censorship and over-governance, and it also thwarts the privacy and freedom that it claims to defend.

The constitutional basis on which the data protection regime in India is founded is in the identification of the fundamental right to privacy as enunciated in K.S. Puttaswamy v. Union of India (2017). In the landmark case, the Supreme Court decided that informational privacy is an accessory and complement of the right to life and liberty under Article 21. Then, the DPDP Act, as well as personal regulation, e.g., the Online Gaming Bill, will have to be reviewed within the prism of such constitutional guarantee. The privacy rights engagement, regulatory authority, and global compliance regimes such as the GDPR are sensitive as they show the delicate tug-and-pull between personal freedom and government control within cyberspace. This thesis places the Online Gaming Bill in the broader scope of data protection laws, and examines its impacts on online gaming platforms across borders. The relationship between the Bill, DPDP Act, and the GDPR is discussed in a bid to evaluate the shifting of the compliance obligations in response to the claims of sovereignty, borderless transfer of data, and

technological evasive mechanisms like VPNs. Moreover, it raises a question of whether the regulatory policy of India is addressing legitimate problems of user protection and data sovereignty appropriately or it may create disjointed burdens that may hamper global interoperability. Lastly, the research will be able to add insight into better understanding how borderless states can regulate digital markets without infringing on fundamental privacy rights

.SCOPE AND OBJECTIVES

The purpose of the study in particular is to examine the impact of Online Gaming Bill, 2025 on the foreign online gaming websites, particularly in the sphere of data protection, circumvention via VPN and its compliance with the international regulations such as the Digital Personal Data Protection Act, 2023 (DPDP Act) and the General Data Protection Regulation of the European Union (GDPR). It looks at the interlocking of the Bill blocking and licensing regime with these data protection regimes, such as consents, data minimization, children data regulation and cross-border data transfer, and evaluates the costs of compliance to global gaming companies. The study also reviews the issue of the widespread use of Virtual Private Networks (VPNs) that bypass geo-blocking and licensing requirements and are hard to enforce. Moreover, it examines the tension between the regulative power and the constitutional right to privacy in Article 21 of the Indian Constitution as set out in K.S. Puttaswamy v. Union of India (2017) and whether the policy in India is sufficient in balancing the protection of the users with the creation of innovations or poses a threat of breaking the international interoperability. Finally, the study will provide pragmatic regulatory or self-regulatory suggestions to balance out data protection standards, seal enforcement loopholes, and maintain user privacy in an open-digitized world.

[3]India's online gaming sector has developed very quickly, with famous firms such as Nazara Technologies, Dream11, MPL, Games24x7, and Paytm First Games drawing millions of gamers. The platforms deal with a great deal of personal and money-related information, so they have to abide by strict guidelines. The upcoming Online Gaming Bill, 2025 requires all real-money games to be licensed and enables the government to block non-licensed sites. Meanwhile, the Digital Personal Data Protection Act, 2023 (DPDP Act) enforces norms on consent, child data protection, restricting data collection, and cross-boundary data transmission, as in the case of global standards such as GDPR.

The new legislation has posed significant issues for Indian online gaming businesses. Several businesses, such as Dream11, MPL, and WinZO, have shut down real-money gaming and are revising their business models. Venture capitalists, who invested around $2 billion in Indian online gaming startups worth around $15 billion, now worry about the returns. To add to that, most of the users make use of VPNs to circumvent geo-blocking and play unauthorized games, which makes it all the more challenging for corporations and regulators to comply with the law.

Due to such issues, Indian gaming businesses need to tread the fine line between ensuring regulatory compliance, maintaining user privacy, and keeping their finances afloat. With this, the following research questions are concerned with how the Online Gaming Bill, 2025, affects Indian online gaming companies in terms of data protection, VPNs, privacy, and compliance.

How does India's Online Gaming Bill, 2025, interact with the Digital Personal Data Protection Act, 2023 (DPDP Act), and to what compliance issues does this pose for Indian online gaming businesses such as Nazara, MPL, and Dream11?

India's Online Gaming Act, 2025, which came into effect on October 1, puts a straight ban on real-money gaming, including skill-based game money participation. The act criminalizes the providing, arranging, promoting, or sponsorship of such games, with imprisonment for up to three years and a fine of up to ₹1 crore. Indian gaming firms like MPL, Dream11, and Nazara have thus been compelled to suspend their real-money operations. MPL, for instance, intended to lay off some 60% of its employees in India, or about 300 employees, as a consequence of shutting down paid gaming services. Nazara Technologies too suffered heavily, with its share price plummeting by 6.73%, indicative of market uncertainty and investor apprehension regarding changes in regulations.

Concurrently, the Digital Personal Data Protection Act, 2023 (DPDP Act) places stringent data protection responsibilities, labeling gaming platforms as 'Data Fiduciaries' and liable for the privacy and security of users' data. Data processing requires direct consent from users, having strong data protection systems, careful cross-border data transfers, reporting data breaches within 72 hours, and ensuring the data of young users through verifiable parental consent mechanisms. The conflict between the DPDP Act and the Gaming Bill generates a twin regulatory burden: whereas the Gaming Bill limits money transactions, the DPDP Act regulates the collection and usage of financial and personal information, so that companies have to juggle criminal risk and data protection duties. Breach of either statute can lead to draconian sanctions, such as fines, imprisonment, or reputation loss, which make operational adjustment both illegally and economically burdensome.

Together, the legislations have compelled Indian gaming firms to restructure their business models into gaming experiences that are not monetary with emphasis on alternative sources of income like sponsorship and advertisement. Dream11, for example, leverages its 10 million daily active consumers to generate revenues through brand collaborations such as Swiggy, Astrotalk, and Tata Neu targeting a predominantly youthful population of approximately 70% aged between 18 and 35 years.. But the shift brings in challenges like reduced profitability, increased operation costs to manage data, and rebuilding user interaction in a competitive landscape. In general, the regulatory landscape requires Indian gaming companies to walk along the thin line of compliance and innovation so that they are at par with the law and yet sustain their operations and growth. For more details, see "Dream11 eyes advertising revenue with 10 million daily active users after RMG ban" and "Legal experts weigh in on DPDP Act's impact on online gaming sector"

To what extent is the extensive popularity of VPNs in India weakening the enforcement of the Online Gaming Bill, 2025, and how should liability be divided between users and platforms in a borderless digital world?

The widespread use of Virtual Private Networks (VPNs) across India has a significant impact on the implementation of the Online Gaming Bill, 2025, particularly regarding the prohibition of real-money gaming. VPNs enable users to mask their geographical location so that they may access and participate in online gaming platforms that otherwise would be prohibited within the country.. Such bypassing of geo-blocking technology negates the success of the law since users can readily evade national firewalls and access foreign gambling websitesVenturThe problem of enforcement from the excessive application of Virtual Private Networks (VPNs) in India is critical, particularly from the view of the Online Gaming Bill, 2025. While the Indian government has attempted to regulate the application of VPNs, for example, by requiring

providers to keep users' data for extended periods, such controls are largely targeting service providers and not end-users. Therefore, users will still be able to access censored content, like web-based gaming sites, with VPNs without being legally confronted immediately.

India's cyber regulator, the Indian Computer Emergency Response Team (CERT-In), issued new guidelines in April 2022 that require VPN service providers, cloud service providers, and data center, to store users' data for at least five years. This includes names, e-mail addresses, contact information, and IP addresses. The goal of the regulations is to improve cybersecurity and fight cybercrime. Obligations like this apply directly to service providers only and not users.. Therefore, users are free to use VPNs to conceal their location and access online gaming websites that otherwise remain banned in India.

The applicability of the Online Gaming Bill, 2025, is also made tougher by the technological advancement of VPN services. Although the government has made VPN operators keep records of users, the operators are not bound to censor or block users' actions. Users are still able to access VPN servers in nations where online gaming is not prohibited, thus avoiding national prohibitions. This puts the enforcement of the Online Gaming Bill provisions in a difficult situation, as it is hard to differentiate between legal users and those seeking to evade legal prohibition.

In this global free zone, liability is elusive. Although users who deliberately circumvent national restrictions through VPNs can be said to go against the intent of the law, they are not directly violating its letter. On the flip side, platforms that enable access to their services from jurisdictions where they are banned could be argued to be complicit in promoting illegal activity. However, enforcement of Indian laws against foreign platforms is problematic on issues of jurisdiction and enforceability.

To address such issues, there must be a balanced response to liability. Users need to be educated about the legal implications and the risks of avoiding national controls, including the risk of fraud and addiction. Websites, especially those which are licensed in other jurisdictions than India, should be endowed with robust geo-blocking mechanisms and adhere to international norms of responsible gaming to prevent their services from being accessed in prohibited zones. Secondly, international cooperation between regulators is essential in formulating an overarching framework that can address the challenges posed by the application of VPNs and provide proper enforcement of online gambling laws. In such a context, establishing responsibility in an extraterritorial cyber world is complicated. Those users who purposefully circumvent national bans through the use of VPNs can be held to have broken the spirit of the law, although not necessarily its letter. Conversely, sites that enable access to their websites from jurisdictions under which they are banned can be said to be complicit in facilitating illicit activity. Yet, the application of Indian laws outside India to foreign websites creates concerns regarding jurisdiction and enforceability.

For these purposes, a balanced approach to liability is called for. Users should be made aware of the legal implications and risks entailed in avoiding national controls, including exposure to fraud and addiction. Sites, especially those operating in jurisdictions outside India, will need to implement efficient geo-blocking technology and global norms of responsible gaming to prevent their services from being accessed within areas banned. There also needs to be international cooperation between regulators to develop an integrated framework for dealing with the difficulties presented by VPN use and enforcing online gaming regulations.

Is the Online Gaming Bill, 2025, when construed with the DPDP Act, sufficient to safeguard users' constitutional right to privacy under Article 21 of the Indian Constitution (K.S. Puttaswamy v. Union of India), or is it in danger of overreach and regulatory fragmentation?

The K.S. Puttaswamy v. Union of India (2017) Supreme Court judgment sanctioned that the right to privacy is a constitutional right under Article 21 of the Constitution. The court held that any such state action infringing upon such a right must pass three tests: legality, necessity, and proportionality. Thus, while examining the Online Gaming Bill, 2025 and the DPDP Act, one has to ascertain whether their provisions satisfy such tests or unreasonably intrude into privacy.

DPDP Act establishes a statutory regime for data protection in India. It prescribes obligations for data fiduciaries -- such as gaming platforms -- to procure consent, provides notice, provides rights of access, rectification, and erasure of personal data, and governs cross-border transfers. These are substantial legislative protections to safeguard informational privacy under Article 21

[4]The DPDP Act requires processing of personal data to be for a particular lawful purpose and notice to be given. These elements conform with the proportionality requirement of Puttaswamy. The Act also offers procedural safeguards and outlines categories of processing and risk, thus planning to curb excesses.

[5]The Online Gaming Bill's prohibition on real-money gaming, through prohibitions and sanctions, can be argued to be directed towards legitimate state aims: averting financial exploitation, safeguarding vulnerable groups (particularly children), avoiding fraud and gambling-addiction. State control in such areas has been sustained in the past as permissible under Article 21 (albeit subject to challenge). The Madras High Court in recent times upheld gambling restrictions such as the minors' ban and time bans, saying the right to privacy is not absolute and public health/public order considerations justify regulation.

The The DPDP Act establishes a statutory paradigm for data protection in India. It enunciates duties for data fiduciaries -- such as gaming platforms -- to seek consent, guarantees notice, provides rights of access, correction, and erasure of personal data, and controls cross-border transfers. These are substantial legislative protections aimed at safeguarding informational privacy under Article 21.

The DPDP Act imposes that processing of personal data shall be for a predefined lawful purpose and notice shall be given. These are adopted in the proportionality requirement of Puttaswamy. The Act also prescribes procedural means and determines types of processing and risk, thus aiming to curb overreach.

The Online Gaming Bill's real-money gaming restrictions, such as its prohibitions and fines, may be viewed to be directed at proper state purposes: avoiding financial exploitation, safeguarding vulnerable groups (particularly children), avoiding fraud and gambling-addiction. State control in these areas has been accepted in the past to be within Article 21 (albeit subject to judicial review). The Madras High Court in a recent judgment upheld gaming prohibitions such as minors' prohibition and time prohibitions, holding the right of privacy is not absolute and public health/public order grounds vindicate regulation. In spite of these positives, there are various material risks and gaps that endanger proper protection for privacy and pose risks for regulatory overreach or fragmentation.

The DPDP Act provides broad exemptions under Section 17 to state instrumentalities on grounds like national security, friendly foreign relations, public order etc. These are extremely wide, and critics have raised that they could breach the proportionality test: permitting excessive government access to personal data in the absence of stringent safeguards.

The Rules of the Act (DPDP Rules) have been faulted by the civil society (e.g., Internet Freedom Foundation) as being imprecise: words such as "reasonable safeguards", "appropriate measures", or "necessary purposes" are employed but not precisely defined. Such imprecision could enable arbitrary exercise of power, which is in tension with Puttaswamy's calls for narrowly drawn constraints.

The structural framework for enforcement (Data Protection Board, etc.) has been faulted as too dependent or ineffective. For instance, worries have been expressed regarding executive control over appointments, absence of judicial oversight over some data access or processing operations, and lack of effective or timely redress and review mechanisms.

The Bill prohibits all real-money gaming (even skill games) instead of making a distinction between games of skill versus chance. It has the potential to infringe upon the right to livelihood (part of Article 21 / Article 19(1)(g)) of professional gamers, and could be perceived as disproportionate if there are less prohibitory alternatives available (licenses, regulation instead of outright ban). Such a blanket ban can be argued by critics as potentially failing the proportionality test under Puttaswamy.

[6]Since the Gaming Bill governs economic activity, financial bets, and licenses, and the DPDP Act governs data, there is possibility of duplication and ambiguity. For example, stringent blocking / licensing under the Gaming Bill could encourage companies to gather more user information or impose stricter identification checks, which is a privacy risk. Conversely, loose data protection laws could enable state access in most situations under exemptions, compromising user trust.

Overall, while the DPDP Act and Online Gaming Bill do contain provisions aimed at safeguarding privacy and do tackle some of Puttaswamy's tests of legality, necessity, and proportionality, there is very real risk of overregulation and regulatory dispersal. Some of the main issues are sweeping government exemptions, imprecise statutory/regulatory language, inadequate supervision, and disproportionate regulation (e.g., blanket prohibitions rather than finessed regulation).

Therefore, as drafted today, the laws partially safeguard privacy but fail to completely meet what Puttaswamy requires. There is a requirement for greater design in control, clearer definitions, judicial checks, and adherence to the least restrictive means to prevent privacy violations and facilitate constitutional validity.

What law and policy frameworks could India implement to align its online gaming regulation with global data protection norms, simplify compliance requirements, and enhance interoperability across borders while protecting the users?

India should take two major steps first will be , reform and harmonize domestic rules so they conform to global standards, and establish useful, cooperative mechanisms to facilitate compliant cross-border activity by gaming platforms.

[7]First, on domestic law and rulemaking: India needs more lucid, precise DPDP implementing rules and guidance that reflect internationally accepted safeguards. The DPDP Act presently establishes fundamental principles (consent, purpose limitation, rights of data subjects) but there are lacunae on cross-border adequacy, operational specificity, and wide exemptions that leave uncertainty for businesses and foreign partners. Tightening DPIA rules(Data Protection Impact Assessment), making technical and organisational measures precise, and confining state exemptions would eliminate legal risk and make India a more reliable partner for the EU and other regulators The Data Protection Board and every gaming regulator should be endowed with clear powers, transparent rulemaking, and robust appeals/judicial review. Avoiding duplicative enforcement (multiple regulators with conflicting powers) reduces fragmentation that increases compliance cost and litigation risk. India should publish authoritative guidance (FAQ, DPIA templates, parental-consent process) specifically for gaming businesses to address particular issues such as children's data, behavioural profiling for monetisation within the game, and anti-fraud .India can manage VPN usage and rule-violation intelligently and equitably. Extremely rigorous measures such as prohibiting VPNs outright or compelling all VPNs to retain detailed user information can damage individuals' privacy and prompt them to lose faith in the system. Rather, the government can:

(a) Request game platforms to employ simple instruments to bar players from regions where the games are prohibited and verify the location genuinely.

(b) Establish clear guidelines on how to warn off or block unlicensed gaming services.

(c) Collaborate with other nations' authorities to take down illicit games, exchange blacklists, and act against recidivists.

Meanwhile, VPNs and encryption must continue to be permitted for secure and legitimate applications. Regulations cannot become so broad as to jeopardize individuals' right to privacy.

The industry itself must also establish some good-practice guidelines. These can range from age verification, safer play elements, equitable adverts, and obtaining as little personal data as possible. Independent audits or monitoring can help ensure companies do live up to these undertakings, and sanctions should be used if they do not. Public education through government-private business cooperation can also help with educating people about secure gaming, creating better parental controls, and running secure-gaming labs for reducing harms and the need for stringent regulation.

Lastly, the transition to new rules must be gradual and planned. The government should provide explicit timelines, user-friendly guides, and even tax or research incentives to assist gaming platforms in changing their systems (e.g., shifting to esports, skill-based tournaments, or advertising models). This gradual process prevents shock that chases away investors or leads to job losses. It also enables companies to plan more effectively and regain trust.

CRITICAL ANALYSIS

The recent prohibition of real-money gaming under India's Online Gaming Bill, 2025 has set a hotly debated issue ablaze. It has nothing to do with games of skill or gambling. It is about controlling the fast-growing digital economy without damaging privacy, innovation, or international competitiveness. Three key tensions define the argument: privacy against enforcement, innovation against restriction, and domestic versus international norms. The government's agenda is clear: stem gambling addiction, protect children, and eliminate money

laundering. In order to that, the Bill and attendant rules require blocking unlicensed apps, strict geolocation verification, and Know-Your-Customer (KYC) authentication. These same measures, however, imply gathering sensitive information—IDs, addresses, financial information, device locations—and storing it for years in many cases. This goes against India's Digital Personal Data Protection Act (DPDP), 2023, that mandates purpose limitation and data minimisation. Practically speaking, sites now over-collect data to play safe from fines. This expands state surveillance powers and increases the potential for breaches. As legal academic Vrinda Bhandari has pointed out in the Indian Express (2024), "broad exemptions without oversight" leave privacy rights vulnerable. The question is whether such intrusive surveillance is actually necessary in order to get enforcement, or if less intensive privacy-respecting solutions would be as effective.India created a successful skill-gaming and fantasy sports ecosystem between 2015 and 2023. Makers of these games like MPL, Dream11, Nazara and Head Digital Works received investment from Sequoia, Tiger Global, and international gaming companies. As per the ban, MPL has let go of around 300 of its 500 Indian employees (India Today, Aug 2025), Head Digital Works has dismissed approximately 500 employees (Moneycontrol, Sept 2025), and Gameskraft has let go of approximately 120 employees (Business Standard, Sept 2025). In total, that works out to around 1,300–1,400 employees laid off in a span of a few months. Flutter, the owner of Junglee, has threatened to lose USD 200 million in revenue from India (Reuters, Aug 2025). This illustrates the economic price of a blanket ban. More permissive models—licensing, age-restriction, stakes limits—might have safeguarded users while keeping companies and jobs intact. And it poses the broader question of whether we are protecting citizens from harm or merely shoving them onto unregulated offshore platforms that provide zero protection.India's strategy will also need to sit within the international privacy and gambling regulatory framework. Under the EU's General Data Protection Regulation (GDPR), data minimisation and severe retention restrictions are applicable even to gambling operators, and state exemptions are strictly limited. The UK Gambling Commission demands age and affordability checks but restricts intrusive profiling and demands encryption. Singapore's Remote Gambling Act denies access to unlicensed operators but is consistent with its Personal Data Protection Act, having transparent datahandling provisions and cross-border transfer channels. India, by contrast, has broad government exemptions under the DPDP Act and no adequacy frameworks for data flows. This raises compliance costs and deters global firms, which must adapt to conflicting requirements.Two key assumptions underpin the current approach. First, that banning realmoney gaming will protect users. Yet evidence from Europe and the US shows that strict bans tend to push users to black markets (Reuters, Aug 2025). Second, that KYC duties do not compromise privacy. In practice, KYC may be extremely invasive, particularly if operators hold entire documents rather than minimal tokens or hashes. Privacy threats increase where such sensitive information are kept for extended durations or insecurely stored. KYC may also discourage involvement in legitimate non-monetary games or ban users lacking common identity documents. VPN infiltration provides an easy indicator of enforcement boundaries. Reports put the use of VPNs by Indians at 43% or an estimated 600 million people, perhaps reaching 700 million by 2026 (Grab On, 2025). This defeats geo-blocking and indicates how simple it is for users to circumvent bans. Loss of jobs, as mentioned earlier, amounts to 1,300–1,400 redundancies. Investment flight comes in the shape of Flutter and other companies reducing their India budgets. These statistics indicate that the price tag on a blanket ban is tangible and quantifiable.Many gaps exist. The first is broad state exemptions under the DPDP

Act, which can be triggered without judicial oversight or independent review. The second is a weakened Data Protection Board, which is inadequately staffed and less independent than EU regulators. The third is ambiguous liability for VPN circumvention: it is not clear whether it is the user's or platform's liability if a blocked game is accessed using a VPN. The fourth is not providing any transition support to impacted workers or new businesses. A more balanced solution is available. Rather than a total ban, India might establish phased licensing of realmoney games with rigorous age checks, spending limits and harm tracking. Current platforms might be allowed six to twelve months to comply, which would keep tax revenues and jobs in place while improving consumer protection. State exemptions under the DPDP Act may be restricted through independent or judicial approval and transparency reporting every time an exemption is applied. KYC may be re-designed as privacy-preserving, for instance through the use of age-verification tokens or hashes rather than the storage of full IDs, and through pseudonymous play in non-monetary games. Transparent rules of liability could be made regarding VPN evasion, defining good-faith geo-blocking by platforms and what notice needs to be provided to users, and safe Harbor where applicable if platforms abide. The Data Protection Board could be beefed up with additional staff, technical expertise and independent appointments.

India too should establish a cross-border data transfer framework—like Standard Contractual Clauses—and negotiate an EU adequacy decision. These would reduce compliance hurdles for Indian companies and facilitate easier foreign investment attraction. Transparency can be enhanced by mandating large gaming platforms to disclose yearly reports on blocking measures, data requests and data protection impact assessments, with independent audits to promote trust. Government assistance could lastly be provided to laid-off workers, through tax credits, retraining grants and startup support. This would moderate the impact of the regulatory change and demonstrate that the state assumes responsibility for transition costs.

CONCLUSION AND SUGGESTIONS

Internet gaming web sites celebrity endorsements (particularly real-money or high-stakes games) should be eliminated. Popular personalities have massive power over vulnerable groups such as children and can become a source of normalisation or glorification of harmful gaming behaviour. India has the potential to borrow a code such as the Advertising Standards Council of India (ASCI) guidelines to gambling and betting advertisements with the help of legislation. This should:Ban Celebrities should not advertise real-money or probability games, particularly where money changes are involved, or loot boxes are involved.

Paste demand warnings and risk warnings on all gaming advertisements, stating that loss of finances and data gathering are pitfalls of using it.

The regulators, civil society and gaming platforms should embark on a sustained awareness campaigns to educate the users about their rights and responsibilities. Terms and Conditions (T&Cs), privacy policies, and consent forms should be highly encouraged to be read and understood by the users before signing up and transacting financial transactions. In order to do this possible:

Obtain key-facts or privacy nutrition labels that give an overview of the important aspects of T&Cs in simple terms. Give automatic in-app notifications or dashboard warning of permission, budget constraints, and data-sharing practices. Introduce cooling-off periods and

convenient self-exclusion options allowing users to exit/quit games safely. Financial penalties on misleading or non-compliant advertising and endorsers ought to be held jointly and severally liable to misrepresentative or exaggerating statements. Platforms must be encouraged to adopt privacy enhancing technology -age-verification tokens, low-KYC data, encryption and anonymisation, to advance regulatory objectives without excessive gathering of sensitive information. The government can offer compliance sandboxes to test out such initiatives. Laws and regulations should unmistakably outline the respective roles of platforms and users. Good faith sites that have effective geo-blocking and age-checking in place should enjoy safeharbour protection; users who deliberately circumvent local restrictions must be made aware of the legal consequences in plain English. Any gambling regulator and the Data Protection Board must be adequately funded and independent, including with clear appointments and judicial review of their power. India must also conclude international data-transfer accords and mutually beneficial takedown processes with other governments to reduce compliance hassle and increase enforcement consistency.India should not have outright prohibitions, but should implement gradual licensings, spending caps, and harm-tracing. This allows firms a time to make the transition, protects jobs and creates a continuous investment. The government can facilitate this by offering re-training or by the tax rebate on innovation to the affected workers.

REFERENCES

https://prsindia.org/files/bills_acts/bills_parliament/2025/Bill_TextOnline_Gaming_Bill_2025.pdf https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

https://link.springer.com/article/10.1007/s42979-025-04269-7?utm_

https://www.scconline.com/blog/post/2025/09/25/rethinking-online-gaming-regulationindia/amp/?utm_source

https://www.mondaq.com/india/gaming/1650648/the-state-reasonably-controls-the-appsmadras-hc-upholds-real-money-gaming-restriction?utm_source

https://timesofindia.indiatimes.com/business/india-business/online-gaming-bill-2025-gamingregulation-shake-up-puts-billions-in-vc-investment-at-risk-investors-to-figure-out-what-canbe-done-next/articleshow/123500416.cms?utm_source

[1] https://prsindia.org/files/bills_acts/bills_parliament/2025/Bill_Text-Online_Gaming_Bill_2025.pdf

[2] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[3] https://timesofindia.indiatimes.com/business/india-business/online-gaming-bill-2025gaming-regulation-shake-up-puts-billions-in-vc-investment-at-risk-investors-to-figure-outwhat-can-be-done-next/articleshow/123500416.cms?utm_source

[4] https://www.juwiss.de/32-2025/?utm

[5] https://www.mondaq.com/india/gaming/1650648/the-state-reasonably-controls-the-appsmadras-hc-upholds-real-money-gaming-restriction?utm_source

[6] https://www.scconline.com/blog/post/2025/09/25/rethinking-online-gaming-regulationindia/amp/?utm_source

[7] https://link.springer.com/article/10.1007/s42979-025-04269-7?utm_

OFFICIAL CHANNELS

- **Website:** www.jointjuristjournal.com
- **E-mail:** publisher@jointjuristjournal.com
- **Instagram:** @jointjuristjournal
- **YouTube:** Joint Jurist Journal Official