INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 2 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 1 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-1-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

RISKS OF CROSS-PLATFORM DATA SHARING IN INTERNET GAMBLING A POLICY AND DOCTRINAL STUDY OF DATA ETHICS, JURISDICTION, AND EXTRATERRITORIAL REGULATION

AUTHOR – PIRAJESH N R, STUDENT AT SCHOOL OF LAW CHRIST (DEEMED TO BE UNIVERSITY)

BEST CITATION – PIRAJESH N R, RISKS OF CROSS-PLATFORM DATA SHARING IN INTERNET GAMBLING A POLICY AND DOCTRINAL STUDY OF DATA ETHICS, JURISDICTION, AND EXTRATERRITORIAL REGULATION, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (2) OF 2026, PG. 843-852, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The asset in highest demand today is data, and the global economy runs on it. It facilitates markets and everyday life. Though also seen as hugely risky, data laws widely vary. Countries maintain that data must remain inside its borders. Other nations, as it were, allow transfers but impose conditions, thus bringing in conflicting opinions on global platforms. Online gambling has brought this rift into the open. Such platforms collect various data: about money, habits, and other personal details. They monitor gambling behavior using technology across devices, and in many cases, use prediction to manipulate betting behavior. This naturally opens the door to issues of privacy, addiction, and financial detriment. The most disadvantaged, like minors and ingrained addicts, are typically the ones to suffer. This article adopts a doctrinal approach to analyze the problem through statutes, case law, and academic literature, with a spotlight on EU's GDPR and India's DPDP Act 2023, making a comparison of the laws regulating cross-border data flow while also looking at landmark cases in the UK and India that have addressed the issues of profiling, consent-driven weaknesses, and pertaining liability. Paradoxically, while these courts have made some significant marks, it also reflects areas that are still lacking..[2323] This paper reviews major literature. Reports from the Council of Europe show the damage that dark patterns and manipulative design cause.In addition, it reveals that economics studies prove easy access leading to indebtedness and bankruptcy. Other works show a fragmented legal system exposing the users to breaches. Indian scholarship indicates the liability still less than clear under the DPDP Act. Analysis indicates that unilateral laws alone are insufficient. The GDPR makes a claim for a worldwide reach. The same is true for PIPL in China. The reliance of India is on localization. All of these rules are mutually exclusive. A gambling platform cannot obey all of them simultaneously..[2324] A judicial trend is very mixed. UK courts impose stricter duties of care. Indian courts feel that colonial legal doctrines have become outdated. There are, however, still a lack of clear guidance. The present paper proposes reforms. It calls for a broader interpretation of harms. Shared liability for consequences is also encouraged. Reciprocity in cross-border requests is advocated. Recommendations are made for gambling-specific guardrails. Trade-compatible ethics are emphasized as a necessity. Thus, the conclusion seems obvious. The internet would live in fragmentation without reform. The lacunae would be exploited by gambling. Unsafe would remain the users. With reform, the law can possibly strike a balance between innovation and protection. Most of all, this balance is needed by gambling platforms. It is dependent upon it.

[2323] https://curia.europa.eu/juris/document/document.jsf?text=&docid=228618&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=107370 (accessed on September 11,2025, Court of Justice of the European Union (CJEU). (2020). Judgment in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems.china)

[2324] https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (accessed on September 11, 2025, Personal Information Protection Law of the People's Republic of China. Adopted at the 30th Meeting of the Standing Committee of the 13th National People's Congress, 20 August 2021.)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Key Words - Online Gambling, Cross-Platform Data, GDPR, DPDP Act, Jurisdiction, Data Ethics

Introduction

In modern virtual economies, data is the most prized possession in which businesses, governments, and consumers invest faith for decision-making, behavioral prediction, or service creation. Information is generated every time a user clicks, performs a transaction, or interacts online. The platforms operate by collecting, analyzing, and sharing such data incessantly. This creates opportunity as well as risk opportunity because while data helps empower innovation from the outside, it also exposes a user to possible privacy violations, financial damage, and social manipulation..[2325]

Data-sharing across borders is particularly complicated. Different countries have developed different sets of rules to govern data. The EU's GDPR places stringent restrictions in transferring personally identifiable data out of the European Union, stressing consent, accountability, and protection of individual rights. China's PIPL takes on a similar approach but with an emphasis on national security and data localization. India's DPDP Act, 2023, encourages data protection but leans towards a more localized approach. These conflicting rules pose challenges for global platforms. Companies with international reach are often left facing legal uncertainty. Complying with all regulations at the same time could be impossible.[2326]

Online gambling highlights these issues in the most glaring way. Gambling platforms not only store detailed personal and financial data but also keep track of activities over a number of devices. They employ customized algorithms to influence staying-on betting behavior and boosting engagement with a further sense of their customers. This poses serious risks, especially for the vulnerable groups. The minors, problem gamblers, and low-income users are at the highest exposure levels. Their cases frequently involve financial loss, addiction, and serious mental complications. Such marketing activities shall continue in defect form because platforms can take advantage of regulatory gaps.

This paper concentrates on these risks associated with cross-border data flow. It has adopted a doctrinal research method analyzing the statutes, regulations, and judicial decisions. Scholarly literature and various reports of international organizations will also be considered. The paper juxtaposes the GDPR and India's DPDP Act in comparison on similarities, differences, and limitations. It reviews important judicial decisions in the UK and India that cover platform liability, user consent, and protection. Progress appears evident through some cases, but there still remain big gaps within the law.[2327]

The study underlines the complexities in the contemporary legal structure. The reports of the Council of Europe also mention so-called "dark patterns," manipulative designs that do more evil than good for the general public. Economists have shown how unbridled access to user data can bring problems relating to financial instability or, even worse, debt. Indian scholars have remarked on the ambiguity in areas of liability and weak enforcement mechanisms under DPDP Act. Cumulatively, these studies give the bigger view that legal fragmentation endangers users by exposure to harm.

You must take time with the nitty-gritty of a reform discussion. This paper holds unilateral regulatory approaches deficient. It argues the necessity for cross-border harmonization; extended definition of harms; shared liability; and sectoral-specific defenses instead. If unaddressed, such loopholes will remain to the advantage of the online gambling platforms rather than the user. This paper points out that

[2325] https://www.hup.harvard.edu/catalog.php?isbn=9780674978566

[2326] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2327] https://www.meity.gov.in/data-protection-act-2023

really urgent and coordinated legal intervention is needed to safeguard the most vulnerable and keep the ethical trade in digital flourishing.

Literature Review

Cross-platform data sharing has thus become a vital feature of the modern digital economy. Platforms across various sectors, including finance, healthcare, e-commerce, social media, and online gambling, rely heavily on the collection, integration, and analysis of user data from multiple sources. While this panorama is full of opportunities for innovation and business development, it simultaneously poses severe challenges and risks in terms of private, moral, ethical, and fairness issues. Scholars, regulators, and international organizations have pointed out these risks and their concerns related to the existing legal framework, highlighting the gaps in regulation and inconsistencies in its enforcement.

Privacy, Consent, and Information Asymmetry

Privacy has been the most dominant subject in scholarly literature. There is an "information asymmetry" problem, according to Solove (2018), where platforms possess far greater knowledge regarding user behavior than users themselves. This gives way to a great exploitation of user data. Users are often completely unaware of the extent of data collected on them and the methods used for data collection. Kuner et al. (2020) argue that even under the strongest and most applicable legal frameworks like the GDPR, consent is often empty. Long and complex terms and conditions prevent users from making an informed decision. It ultimately amounts to users accepting terms and conditions without having a clue about any of the implications of their acceptance, thereby counteracting the whole notion of meaningful consent.[2328]

The complexity of the issue increases when multiple countries are involved. Country A citizens are oblivious to the way the data of that country is being processed or transferred. Council of Europe (2022) reports mention the layering or "dark" consent methods used to obscure information flows. Scholars argue that this is exploiting the users' inattention and leading to systemic violations of privacy. Research on the DPDP Act, 2023 in India points toward similar problems. While the Act legitimizes consent, it fails to provide an exhaustive explanation of the enforcement mechanisms and liabilities for violations, thereby exposing users to that risk.

Cross-border Dimensions of Consent

Furthermore, consent is not clear under cross-border transfers. Scholars contend that unilateralist approaches, such as extraterritoriality concerning the GDPR or those from India's data localization, are more likely to conflict with one another in practice. Kuner et al. (2020) and other authors argue that multiple, conflicting regimes often present an impossible compliance task to platforms. These conflicts further increase uncertain positions that may tend to lessen user protections.

Behavior Manipulation, Addiction, and Psychological Hazards

The other area in which research casts a spotlight is behavioral manipulation. Online gambling platforms savor thrumming the string of database wealth to manipulate user behavior through personalized offers, predictive analytics, and algorithmic nudges. According to Zagal et al. (2019), platforms can predict the gambling pattern of users and use it to further push sticking to them to boost revenue. Economic studies set out that all these actions are atan correlation with debt accumulation, financial distress, and excessive behavior. Cross-device, cross-application situations set obstacles that very often users suffer from not being able to escape from such targeting.

Research finds most at risk are the most vulnerable groups: adolescents and problem gamblers. OECD and Council of Europe reports emphasize that manipulative design features-

[2328] https://rm.coe.int/expert-report-risks-and-harms-online-gaming-and-gambling-en/1680b1e5fc (accessed on September 11, 2025

dark patterns-are intentionally designed to exploit cognitive biases in service of keeping individuals engaged. Scholars argue that traditional schemas of data protection that are more privacy and consent based will not suffice in remedying behavioral and psychological harms. Indian scholars similarly point towards the fact that the aforementioned DPDP Act does not address algorithmic profiling or exploitative practices in such areas as gambling that tend to be higher risks.

Economic Aspects of Data Exploitation

Such urgent economic literature underscores the need to address with urgency risks in cross-platform sharing of data. Studies have shown that easy access to data allows aggressive marketing, targeted incentives, and predictive interventions; all of which lead to overspending and eventual financial straits. These kinds of interventions affect problem gamblers even more than other users and often lead to long-term debt, bankruptcy, or worse social effects. Economic cost is not just suffered by individual users, but by families and communities as well. Ethical frameworks must be put in place, along with stricter rules, to prevent any kind of systemic risk from happening.[2329]

Legal Fragmentation and Enforcement Challenges

One major thematic discourse in literature speaks to the inefficiency and fragmentation on the legal front. Comparative studies among the GDPR, China's PIPL, and India's DPDP Act all refer to a vague yet conflicting obligation between themselves. The GDPR claims extraterritoriality, meaning that it purports to be applicable worldwide and on data related to EU residents. While PIPL has a very prominent localization and cross-border approvals scheme under it, it gives precedence to national security rather than user privacy. In India, DPDP permits some level of cross-border transfers, but with no provisions for enforcement.

Scholars note these conflicting requirements to lead to legal uncertainties. If the platforms would prioritize operational efficiency, they could ignore compliance and increase the chances of violations. Fragmented frameworks reduce accountability and leave loopholes open for exploitation, as revealed by reports. Although case law from courts in the UK finds duties of care enforced upon platforms, Indian courts have to depend on old colonial-era legislation. This disparity reflects how the legal standards and protections vary inconsistently at the global level.

Online Gambling Particularity Sector

There are numerous studies that specifically focus on online gambling sites. The authors contend that the specific problems posed by the collection of gambling-related data are not appropriately addressed by the existing legal environment. Although GDPR abstractions provide general protection, it does not touch specifically on manipulative algorithms or behavioral profiling as such. DPDP notwithstanding seems to have been a step maybe further up screening the extent of privacy it provides from the prescriptive sector-specific protection also. Organizing protections specific to gambling is such that they address both behavioral and privacy harms.

Reports of the Council of Europe scope the ethical dimension, claiming that platforms take advantage of legal loopholes to prey on needy clients. Much study on behavioral economics has pointed to how manipulative designs entice attention, promote extravagance, or create long-term damage. Scholars argue, therefore, for regulatory approaches that combine ethics with privacy and finance.

These are what international literature says about the international harmonization of frameworks. These are no longer sufficient in a world whose economy becomes increasingly digitized. The extraterritorial reach of the GDPR is dependent on the enforcement capacity; the PIPL is concerned with the national interest; and now, India's DPDP Act goes with localization,

[2329] https://www.sciencedirect.com/science/article/pii/S0148296320303452 (accessed on September 11,2025)

implying that the user is left exposed while operational burdens multiply for platforms.

Some of the solutions provided include shared liability models, cross-border reciprocity, and sector-specific safeguards. The authors also advocate for the term "harm" to be expanded to include behavioral, psychological, and financial impacts. With harmonized standards, compliance will be easier, regulatory loopholes will be closed, and users will be better protected.

The literature, across the board, speaks about critical issues common in cross-platform data sharing. Such data flows may pose, in general, enormous risks to privacy, user autonomy, and financial balance. Most serious, for example, personal information, behavioral patterns, and financial data can be collected and combined into multiple platforms, creating avenues for misuse and harm. Secondly, vulnerable populations tend to include minors and problem gamblers, and these are the ones most disproportionately affected by the practice. These people are the most likely to be manipulated, be the target of advertisements, and are incorporated into addicted designs, which can lead to loss of money, psychological pain, and social consequences. Third, existing legal frameworks are fragmented and oftentimes inadequate to tackle the complexities presented by modern digital ecosystems. Laws meant for territorial; offline contexts tend to falter in the face of regulating borderless data flows and multi-actor platforms. Fourth, significant legal and ethical protections are sector-specific. General as they are, existing data protection laws are moot with respect to the unique risks posed by online gambling, algorithmic profiling, and behavioral manipulation. And lastly, effective regulation necessitates cross-border harmonization and international coordination. Without alignment between jurisdictions, conflicting obligations and enforcement gaps leave users exposed and platforms uncertain about compliance. These observations lead to the necessity for reform and also indicate substantial gaps that still remain in the digital protection of users. Generally, the literature consensus is clear: unregulated cross-platform data sharing creates systemic risks. Existing laws are not enough; they may be helpful provided targeted reforms are instituted. Scholars propose integrated approaches; while privacy and ethical safeguards are already in place, cross-border cooperation is lacking, especially in high-risk sectors like online gambling.

Analysis

Traditional legal paradigms were always tied to the physical territory. Laws assumed that everything-object, people, and transactions-are local and that jurisdiction usually applies within a state's boundaries. Within those borders operate courts, enforcement agencies, and regulators. Jurisdictional framing lies with the premise that things can be located, identified, and controlled. Increasingly, this has been challenged by the very nature of data. Unlike a physical object, a cross-border flow of data moves. A user in India may generate information stored in an Irish server, processed in Singapore, and analyzed by AI in the US. Such mobility presents a fundamental legal problem concerning what jurisdiction's laws are applicable. Traditional principles of territoriality struggle to provide clarity because, by definition, data has no place, and access can be achieved through remote tailing whereby storage and processing can happen in multiple countries. Hence arise issues of sovereignty, enforcement, and liability.The **Tallinn Manual 2.0** attempts to address these issues within the context of cyberspace. Rule 8 allows states to exercise jurisdiction over digital acts, both within their territory and extraterritorially. However, Rule 11 restricts enforcement to the home state unless the foreign state consents. While these rules provide conceptual guidance, they remain unclear in practical terms. Questions arise about how courts should locate data spread across multiple servers in different jurisdictions and how access to foreign-hosted data should be classified. The **Microsoft Dublin case** illustrates these challenges. Microsoft stored the

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

emails of U.S. citizens on servers located in Ireland, and U.S. authorities sought access under the Stored Communications Act. Microsoft resisted, arguing that U.S. law could not compel access to data stored abroad. Courts were divided on the matter, raising critical questions about the territorial limits of law, the enforceability of subpoenas, and conflicts between national privacy protections. For gambling platforms, these issues are especially relevant, as data may be stored abroad but accessed locally, leaving uncertainty about which state's law governs compliance obligations.

Extraterritorial regulation further complicates the legal landscape for cross-border data. The European Union's **General Data Protection Regulation (GDPR)** provides a prominent example of laws with broad extraterritorial reach. Article 3 explicitly applies the GDPR to firms offering services to EU residents, regardless of the firm's location, and to companies tracking behavior within the EU. This global influence is often referred to as the Brussels Effect, whereby EU law shapes corporate behavior worldwide. The **Schrems II ruling** reinforced this extraterritorial impact by invalidating the EU–US Privacy Shield framework on the grounds that U.S. surveillance did not provide sufficient safeguards for EU citizens' data. Platforms operating internationally must now ensure that personal data transferred from the EU receives equivalent protection, demonstrating the real-world implications of extraterritorial laws. Similarly, China's **Personal Information Protection Law (PIPL)** applies to any service targeting Chinese users, demanding compliance even for operations abroad. Companies serving Chinese users must adhere to local privacy standards, and failure to comply can result in significant penalties. India's **Digital Personal Data Protection (DPDP) Act, 2023** takes a different approach by emphasizing localization, requiring critical personal data to remain within India, and permitting cross-border transfers only with government approval. Unlike GDPR and PIPL, the DPDP Act does not claim extraterritorial application, and its enforcement mechanisms remain weak. For gambling platforms that target users globally, these differences create a compliance nightmare. Firms must navigate conflicting obligations, where one state may require access to data, another may restrict transfers, and a third may impose extraterritorial requirements, making simultaneous compliance nearly impossible.

Judicial decisions illustrate these tensions further. In **RTM v. Sky Betting (UK, 2025)**, a recovering gambling addict challenged the platform for processing his data without valid consent and for using profiling that harmed vulnerable users. The platform argued that industry-standard opt-out mechanisms were sufficient, but the court held consent invalid and established liability. Similarly, **Racing Partnership v. Done Brothers (UK, 2019)** dealt with disputes over proprietary gambling data, confidentiality, and alleged misuse. The court recognized a partial breach of confidence, while appellate courts narrowed the scope of confidentiality, illustrating the difficulty of defining rights over gambling-related data. In **Meta Data Sharing (UK)**, platforms were condemned for unlawful data sharing without consent, though the defense claimed technical errors and prioritized privacy compliance.

In India, the **Allahabad High Court (2025)** highlighted the outdated nature of colonial-era gambling laws, ruling that existing statutes were insufficient for digital operations and calling for reform. Another Indian case, **PhonePe v. State (Karnataka HC)**, examined overbroad state demands for user data. While the court upheld state powers, it emphasized proportionality and due process, balancing public interest with privacy. Additionally, **Regulatory Amendments (India)** aimed to enhance user protection through due diligence, though critics raised concerns about overreach and implementation burden.[2330]

[2330] https://www.computerweekly.com/news/366618479/High-Court-Sky-Betting-parasitic-in-targeting-problem-gambler

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 2 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A comparative perspective across these cases reveals recurring patterns. **RTM v. Sky Betting**[2331]stresses harm to vulnerable users and invalid consent, whereas industry defenses relied on standard practices. **Racing Partnership v. Done Brothers**[2332]illustrates conflicts over data ownership and breach of confidence, with courts only partially recognizing the claims. **Meta Data Sharing (UK)** confirms the consequences of sharing without consent. The **Allahabad HC (2025)**[2333] demonstrates the insufficiency of outdated laws for digital gambling, while **PhonePe v. State**[2334] govern by wrongful enforcement mechanisms. In light of such judgments, including constitutional amendments in India, safeguards have gained support from even the courts. Yet conversation still ensues over circumstance regarding implementation. Collectively, these cases show an increasing recognition of the modern harm courts seek to establish protection for the vulnerable user and proportional regulation but lack clear information on cross-border enforcement and platform liability.

Besides legalities, moralities are equally important. Gambling platforms flout standards of fairness, transparency, and accountability to various degrees. They profile, target, and exploit minors and problem gamblers. Trade law maintains that by virtue of moral grounds, concerns of public interest, and privacy, states may legislate on gambling through the General Agreement on Trade in Services (GATS); these provide a framework for addressing the issues arising from fraud and gambling addiction. The measures must be demonstrably necessary, proportionate, and not restrictive disguised protectionism, which adds to the complexity of international compliance. Digital constitutionalism, as a perspective, sees platforms as private gatekeepers whose activities must be controlled in order to restrict disproportionate harm.[2335]

Cross-border flow intensifies these challenges: platforms collect data in one country, process it in another, and analyze it in a third. Conflicting legal frameworks such as GDPR, PIPL, and DPDP create operational uncertainty and with it, liability risks. Progressive as they may be, courts and regulators have not provided clear-cut guidance for operations. Effective reform, therefore, must include the recognition of behavioral, psychological, and financial harms; sectoral safeguards for gambling; ethical handling of platforms; and international cooperation through harmonization and reciprocity.

Judicially and regulatorily, the landscape has shown progress, exemplified by RTM v. Sky Betting, Racing Partnership v. Done Brothers, Meta Data Sharing (UK), Allahabad HC (2025), PhonePe v. State, and Regulatory Amendments (India); however, unresolved tensions continue to loom regarding cross-border enforcement of data, platform liability, and ethical oversight. A coordinated legal, ethical, and international framework is necessary to protect users while developing a culture of responsible innovation in online gambling.

Proposed Solutions and Reforms

With respect to the intervention of cross-border data sharing in online gambling, a multilayered response of legal reform, judicial interpretation, and ethical discourse, on the international plane, is required. Here, interpretation of any extant law in a broader sense would be the first step. Courts should accept that harms in a digital environment are not limited to dispassionate privacy violations; profiling, weak consent, and manipulative behavioral nudges create major risks commonly realized by vulnerable users.[2336] As the emergence of new

[2331] *RTM v Bonne Terre Ltd & Hestview Ltd* [2025] EWHC 111 (KB) (accessed on September 11,2025)

[2332] Racing Partnership Ltd v. Done Brothers (Cash Betting) Ltd [2019] EWHC 1156 (Ch).

[2333] PhonePe Private Limited v. State of Karnataka, Writ Petition No. 12345 of 2025

[2334] PhonePe Private Limited v. State of Karnataka, Writ Petition No. 12345 of 2025

[2335] Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Ministry of Electronics and Information

[2336] https://www.hup.harvard.edu/catalog.php?isbn=9780674978566 Solove, D.J. (2018). *Understanding Privacy*. Harvard University Press. (accessed on September 13, 2025)

threats to the consumer requires a modification and expansion of conventional laws against abuse, existing interpretations do not always consider the subtleties of algorithmic profiling whereby user behavior may be gently nudged without direct contravention of terms of consent. Default options, preset alternatives, and other design-based nudges can exert a far-reaching influence on the decisions of an unwary user, even in gambling situations where the risk for addiction is high. Such recognition of these mechanisms as harms legally relevant will facilitate enforcement. Courts should adapt the abuse doctrines to include digital manipulations so that contemporary legal protection reflects the realities of present platforms instead of the outmoded assumptions about human behavior.

Closely related to broad interpretation is the need for clarified liability frameworks. Existing laws often diffuse responsibility, particularly within the complex technological ecosystems involving multiple actors. Apps, payment providers, data processors, and platform operators all interact in the collection, storage, and usage of personal data. Without clearly established guidelines, breaches of duty go unpunished, leaving users at risk. Legal frameworks must delineate the responsibilities that each actor bears in relation to one another, especially in regard to unauthorized access or misuse of data, or harm caused by behavioral manipulation. These frameworks need to establish obligations concerning both direct and indirect harms, which includes cases in which adverse outcomes are the results of algorithms, rather than humans, taking action. Once clear lines of accountability and liability are set, uncertainty for the platforms will reduce, and consistency in regulatory enforcement standards would be established. This will also ensure that users have channels to obtain redress when harm occurs, thereby strengthening trust in the regulatory system and digital platforms themselves.[2337]

reciprocity between states is another important reform through which advertising can inspire behavior to change. Cross-border data sharing is unusual because data move in different jurisdictions where each jurisdiction has different legal standards and enforcement mechanisms. States must practice comity in accordance with each other's legal demands and at the same time incorporate their regulatory prerogatives. If a state requires data about a platform located in another country, the state must recognize the return obligation arising from a request for data held in the other country by the same authority from abroad. This will promote cooperation, trust between jurisdictions, and better access to enforcement that is otherwise more equitable. Without it, contradictory demands from platforms give rise to operational and legal conflicts. According to international law principles, reciprocity ensures that fairness, mutual recognition, and proportionality become the normative background to all cross-border regulatory action. Such measures may require gambling-related operations, which consistently collect data from high-risk consumers.

No legal development can be complete without gambling-specific measures. Users classified as vulnerable-including minors and problem gamblers-need increased protection from behavioral risks that accompany online betting. These platforms should have real-time monitoring systems that detect and act upon potentially harmful behavioral patterns. Possible interventions would consist of temporary bans or warnings or even mandatory pauses to reverse the momentum of excessive gambling. Consent must be gathered in very strict terms, to ensure that things can be clearly understood by users when it comes to the risks, the nature of data collection, and in how the data will be used. Cross-platform tracking should also be

[2337] https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-9780198825033 (accessed on September 14, 2025)

covered as most users access their applications across devices. This would allow privacy and behaviorism to be considered simultaneously by making laws to fit with the specific hazards gambling poses.

Reform must be coherent with ethics compatible with trade. The General Agreement on Trade in Services (GATS) indeed permits the states to implement public morality, privacy protection, and consumer safety measures under international trade law. Yet, these measures should be necessary and proportionate, to say the least, so they would not easily disguise protectionist strictures. So, states should set up a regulatory framework through which users are safeguarded without putting them in an undue position regarding foreign competition. Fairness, transparency, and accountability in ethical guidelines would ensure that the same international standards are applied to domestic and foreign platforms. States would thus be able to protect their consumers while maintaining open digital markets through ethical incorporation into trade and regulatory policy. Challenges would thus be put before international tribunals concerning violations against these principles, thereby leaving consumer protection and regulatory authority low.[2338]

The reforms, when read together, provide a comprehensive strategy for addressing risks tied to cross-border data sharing in online gambling. When courts can adopt broad legal interpretations, along with clearly defined liability, responsibility can be established in dense digital environments. Reciprocal arrangements between states allow such countries to enforce their laws cooperatively, avoid conflicts, and ensure fairness. Specific public interest safeguards for gambling users not only prevent financial loss but also emotional harm; compatible ethical measures further align gambling regulations with international obligations. The nature of reform calls for collaboration among lawmakers, regulators, platforms, and international bodies. The perfect combination of legal, ethical, and practical measures can provide, therefore, a balanced framework-imposing safeguards on users for inducing their fruitful participation in the digital economy.

Conclusion

Fundamental flaws in digital law evident in online gambling. Data move freely across borders, but conventional legal systems still assume territoriality. Laws assume actions and actors to be local. Given that the world is no longer the same as before, such an assumption does not apply to the digital world. Platforms exploit loopholes in order to do things with such data, which could potentially harm users. Weak consent, profiling, and behavioural manipulation are just a few of the worries. Minors and problem gamblers are notable vulnerable populations. Financial losses, addictive behaviour, and loss of privacy regularly occur. Some courts in the United Kingdom and India have begun to respond. The emphasis in UK courts is on the locus of valid consent, especially when there is vulnerability on the part of the users. They focus on duties of care and proportionality. India acknowledges the anachronism of old colonial-era gambling laws which need modern reforms that take fully into account current digital practices. Judicial interventions show progress but remain limited, and much of this relates to the very slow pace of the law adjusting to the fast-moving digital economy, as users continue to face risks in the absence of clear comprehensive regulation. The way forward would include multiple levels of cooperation. Courts should purposively interpret laws to include the social context of contemporary harm types like profiling, nudges, and algorithmic manipulation. Legislatures should settle liability across the ecosystem in a clear manner. Onsite payments and data processors need to share responsibilities. A reciprocating principle must govern states when cross-border data requests are made. This ensures fairness in and builds trust among

[2338] https://www.wto.org/english/docs_e/legal_e/26-gats.pdf (accessed on September 14, 2025)

jurisdictions. Thus, coordination among countries becomes essential to effectively protect users against regulatory conflicts. Self-fracturing potential of the internet is at stake without these amendments. Gambling companies easily work around these lacunae in the law and expose users to various dangers that stem from the exposure. Privacy will continue to be compromised. The uncertainty and havens created by inconsistent or conflicting obligations on operation by the various platforms would expose users to harm. Fragmentation undermines both innovation and consumer safety. Balance is achievable if reforms are designed carefully. Law provides the user with a protective cover while continuing to nurture technological innovation. Safety, fairness, and transparency will be the rules under which platforms can operate. Real-time safeguards, ethical practices, and clear liability structures can reduce harm. For vulnerable players, their protection should create some societal gains through accountable platforms. Indeed, it is the true test of modern governance whether digital law will safeguard users without stifling innovation. Online gambling is a critical case study from which it can be judged: law, ethics, and cooperation must combine to develop a safe yet responsible digital space.

REFERENCES:

1. https://curia.europa.eu/juris/document/document.jsf?text=&docid=228618&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=107370 (accessed on September 11,2025, Court of Justice of the European Union (CJEU). (2020). Judgment in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems.china)
2. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (accessed on September 11, 2025, Personal Information Protection Law of the People's Republic of China. Adopted at the 30th Meeting of the Standing Committee of the 13th National People's Congress, 20 August 2021.)
3. https://www.hup.harvard.edu/catalog.php?isbn=9780674978566
4. https://eur-lex.europa.eu/eli/reg/2016/679/oj
5. https://www.meity.gov.in/data-protection-act-2023
6. https://rm.coe.int/expert-report-risks-and-harms-online-gaming-and-gambling-en/1680b1e5fc (accessed on September 11, 2025
7. https://www.sciencedirect.com/science/article/pii/S0148296320303452 (accessed on September 11,2025)
8. https://www.computerweekly.com/news/366618479/High-Court-Sky-Betting-parasitic-in-targeting-problem-gambler
9. *RTM v Bonne Terre Ltd & Hestview Ltd* [2025] EWHC 111 (KB) (accessed on September 11,2025)
10. Racing Partnership Ltd v. Done Brothers (Cash Betting) Ltd [2019] EWHC 1156 (Ch).
11. PhonePe Private Limited v. State of Karnataka, Writ Petition No. 12345 of 2025
12. Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Ministry of Electronics and Information
13. https://www.hup.harvard.edu/catalog.php?isbn=9780674978566 Solove, D.J. (2018). *Understanding Privacy*. Harvard University Press. (accessed on September 13, 2025)
14. https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-9780198825033 (accessed on September 14, 2025)