



LEXTECH



**INSTITUTION'S
INNOVATION
COUNCIL**
(Ministry of Education Initiative)

**DECEMBER 2023;
NEW YEAR'S EDITION**

MONTHLY NEWSLETTER

**LEXTECH: CENTRE FOR
LAW, ENTREPRENEURSHIP
AND INNOVATION**



सत्ये स्थितो धर्म



CONTENTS

1. Technology, Media and Telecommunications

2. Online Gaming and Betting laws

3. FinTech

4. Artificial Intelligence

5. Data Privacy

6. Panorama View





TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS



SECTION 1



GUIDELINES NOTIFIED FOR PREVENTION AND REGULATION OF DARK PATTERNS

NEWS

Recently, the Central Consumer Protection Authority ('CCPA') notified guidelines for the prevention and regulation of dark patterns ('Guidelines') fortifying consumers' interest. This step has been taken after seeing growing reliance on e-commerce platforms to protect consumer interests.

LEGAL TALK

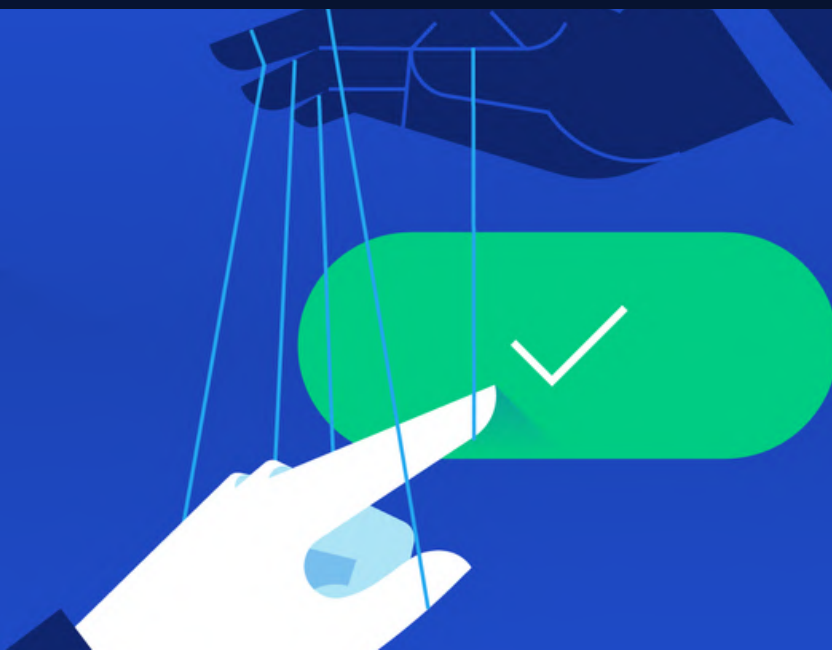
Section 2(e) of the guidelines defines "dark pattern" broadly as encompassing manipulative techniques that deceive consumers into making unintended choices. While this definition represents a commendable step towards consumer privacy protection, inconsistencies within the guidelines themselves raise concerns. One inconsistency lies in the scope of application. While the guidelines seek to encompass advertisers and sellers, the operative restrictions seemingly apply to "all persons," including platforms. This ambiguity creates uncertainty regarding the intended reach of the regulations.

Further, it has defined different types of dark patterns which include a term called 'nagging'. It is a type of dark pattern in which users are "disrupted and annoyed" by practices that can range from requirements to download applications or provide phone numbers. However, the definition forgot to meet the core requirement of alleged pattern, i.e. disruption of the transaction being carried out by a consumer.

Additionally, it has defined a dark pattern called 'subscription trap' which has classified some common business practices, such as requiring payment details for free trials or authorizing auto-debits for a free subscription as a dark pattern. However practically, several free trials require small amount of money to be deposit for the confirmations of users' payment mechanisms, to ensure that potential subscribers have the valid means to pay.

THE WAY FORWARD

The guidelines have various drafting concerns with the lack of specificity. These can hamper effective enforcement and compliance and overburden the routine appeal mechanism to high courts from the decisions of the CCPA. Furthermore, there is a need to adopt a balanced, specific, and business-friendly approach to prevent unintended consequences. This approach is essential to avoid hindering legitimate content, market practices, and technological innovation, particularly in the context of a rapidly evolving digital ecosystem.



THE REVISED TELECOM BILL EXCLUDES OTT REFERENCE

NEWS

The revised telecom bill introduced in the Lok Sabha has removed over-the-top ('OTT') players or applications under the purview of the telecommunication ('telecom') service definition. The earlier drafts of the telecom bill contained provision to regulate the OTT platform which had received opposition from various internet companies.

LEGAL TALK

Section 2(t) of the telecommunications bill defines "telecommunication service" as any service related to telecommunication. This definition is broad and can be interpreted to encompass OTT services, potentially triggering a requirement for internet companies to obtain authorization. However, the revised bill has provided significant relief to social media and OTT companies.

The rationale behind that can be that the bill stipulates that the telecom services that offer communication services, such as messaging and online calling, have to obtain authorization from the government. Additionally, users of these services will be required to undergo biometric-based Know Your Customer ('KYC') processes, which involve identifying and verifying the user's identity through fingerprints, irises, or facial recognition. If these regulations were applied to OTT services, it could have imposed a substantial burden on such companies, potentially leading to a decline in users due to the increased compliance requirements.

Moreover, the legislation grants the government authority for interception and examination, enabling the interception, surveillance, or obstruction of messages for reasons related to public safety, emergencies, or specified circumstances like state security. This provision poses a potential risk to the integrity of end-to-end encryption on online messaging platforms as it necessitates the divulgence of messages in an understandable format. Such a requirement may also result in a breach of of the Section 8 Data Privacy and Protection Act ('DPDP Act'), which imposes an obligation on entities to safeguard the personal data they possess.

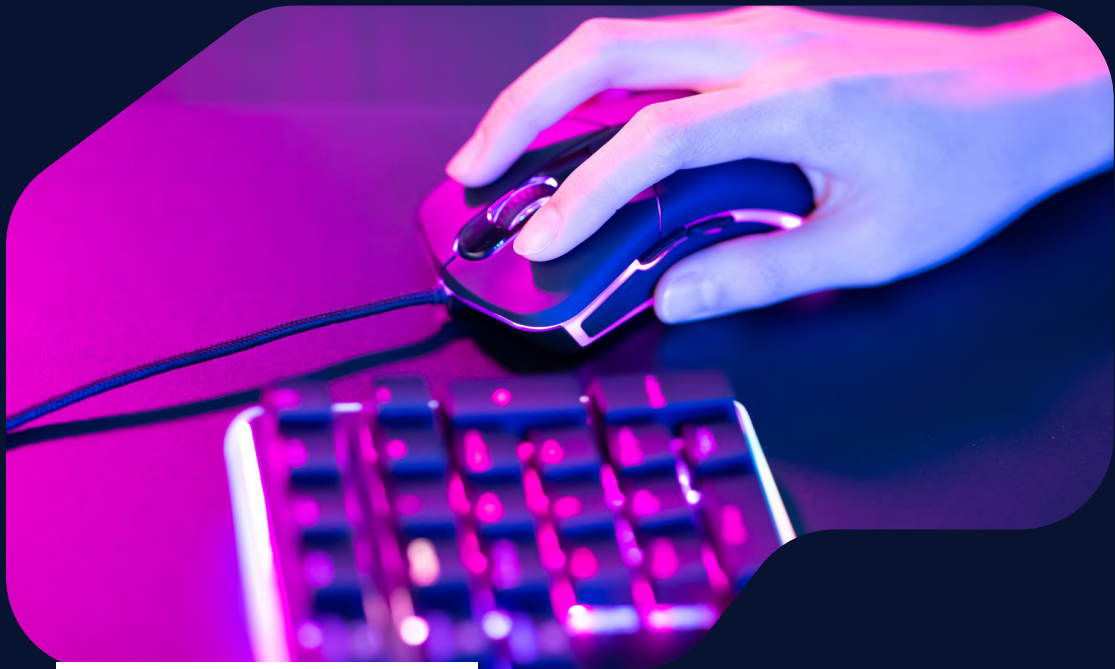


THE WAY FORWARD

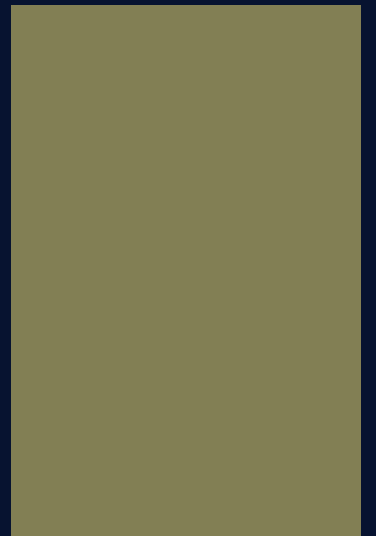
The revised bill represents a significant alleviation for OTT platforms and social media companies. It resolves the discord arising from conflicting provisions in recently proposed bills, including the Digital India Bill, Broadcasting Regulation Bill, and Telecommunication Bill, all of which sought to regulate these entities. Additionally, internet companies now have clear guidance to adhere to the IT Act for lawful operation within India.



Online Gaming and Betting Laws



SECTION 2



FOUR GAMING INDUSTRY BODIES SIGNED A VOLUNTARY CODE OF ETHICS

NEWS

The Internet and Mobile Association of India (IAMAI), All India Gaming Federation (AIGF), E-Gaming Federation (EGF), and Federation of Indian Fantasy Sports (FIFS) signed the “[Voluntary Code of Ethics for Online Gaming Intermediaries](#)” with main aim being to protect consumer’s interest and enable them to make informed choices regarding the online games available to them.

LEGAL TALK

The newly codified regulations for online gaming in India establish a comprehensive framework for legal operations while differentiating them from gambling activities. Companies must adhere to the 2005 RBI Know Your Customer (“KYC”) [Guidelines](#), ensuring KYC, displaying verification marks, providing a functional grievance redressal system, utilizing verifiable RNG, and obtaining no-bot certificates. To uphold transparency and responsible practices, they must further: specify winner selection methods and platform fees on their websites, restrict deposits to in-game usage, enable user spending limits and age verification to prohibit gameplay for those under 18, and ensure advertising complies with the [Customer Protection Act, 1986](#). Non-compliance carries the risk of penalties. Additionally, companies must adhere to the latest data protection and storage guidelines prescribed by the [Digital Personal Data Protection Act, 2023](#). This multi-pronged approach aims to safeguard consumer interests, promote fair play, and ensure responsible conduct within the burgeoning online gaming industry.



THE WAY FORWARD

All these steps are taken into account after the Ministry of Electronics and Information Technology (MeitY) had notified rules for online gaming which allowed for the setting up of self-regulatory bodies to vet the legitimacy of online games with oversight of the government. This regulation after the full implementation of the rules, will help in testing waters and pave way for a more formal regulatory framework in near future. The code of ethics will ensure that the people are free to choose and play video games on their own but there will be less chances of mishaps like game addiction, financial frauds etc with the code of ethics overlooking the industry with its safeguards.



FinTech



SECTION 4



RESERVE BANK OF INDIA ('RBI') BAN ON 2 BAJAJ FINANCE E-LENDING PRODUCTS

NEWS

Recently, the RBI has ordered Bajaj Finance to halt loan issuance through its 'Ecom' AND 'Insta EMI Card' due to non-compliance with the Digital Lending Guidelines ('DLG') issued by the RBI in September 2022.

LEGAL TALK

The order is a result of non-compliance with paragraph 5.2 of the guidelines which make it mandatory for the Regulated Entities to provide a Key Fact Statement ('KFS') to the borrower in a standardized format before the execution of the contract. Bajaj Finance did not issue the KFSs to the borrowers under these two lending products and there were also deficiencies in the KFSs issued in respect of other digital loans sanctioned by the company.

The KFS serves as a concise document outlining crucial loan terms and conditions across 15 parameters, including interest rates, fees, total cost, duration, and repayment terms. Annexure II of the DLG prescribes the standardized format, enabling borrowers to streamline comparisons between similar financial products or loans. This structured presentation of key information in a clear and consistent format empowers borrowers to effectively assess and compare competing options. Furthermore, the upfront disclosure of all essential details mitigates the risk of borrowers encountering hidden fees or undisclosed terms, thereby promoting informed decision-making. This transparency fosters trust and protects borrowers from potential exploitation, upholding the core principles of fair and responsible lending practices.

THE WAY FORWARD

The RBI's initiative is directed towards safeguarding consumer interests and ensuring fair lending practices in the digital lending space. The move may also see a decline in loan growth since the step has been taken to reduce excesses in the NBFC space.



RBI ISSUES STATEMENT ON DEVELOPMENTAL AND REGULATORY POLICIES

NEWS

Recently, the RBI issued a Statement setting out various developmental and regulatory policy measures relating to Financial Markets, Regulations and Payment Systems and FinTech.

LEGAL TALK

According to the regulations, the UPI caps on payments to hospitals and educational institutions will be increased from Rs. 1 lakh to Rs. 5 lakh per transaction. This move is aimed to encourage the use of UPI system for medical and educational services. Additionally, the RBI has proposed to exempt the requirement of Additional Factor of Authentication ('AFA') (it refers to additional factors to achieve authentication for payments like password, PIN, biometric etc.) for recurring online payments with transactions up to Rs. 1 lakh for the categories- subscription to mutual funds, payment of insurance premium and payments of credit card bills. Currently, the limits for execution of e-mandates without AFA stands at Rs. 15,000. The RBI is also set to establish a cloud facility for the financial sector which will be used as a scalable data storage and data processing facility. The facility will be set up and operated by the Indian Financial Technology and Allied Services. This move by RBI appears to be a deliberate shift away from an overreliance on the various public and private cloud facilitates in use today. The facility is a welcome move as it would ensure security of consumer data.

THE WAY FORWARD

The RBI expects the cloud facility to enhance security, integrity and privacy of financial sector data. FinTech companies may expect smoother operations with the establishment of the cloud facility and will act as a source of transparent information about the FinTech companies which in turn will benefit the consumers. The strategy of promoting voluntary contributions from FinTech companies will enable informed, quick, and risk-mitigating decision-making for regulators by providing them with real-time insights.



RBI TIGHTENS NORMS FOR REGULATED ENTITIES INVESTING IN ALTERNATE INVESTMENT FUNDS ('AIF')

NEWS

Recently, the RBI issued guidelines for all Regulated Entities ('REs') including all banks and NBFCs for investing in AIF which has downstream investments in a debtor company of the RE. The guidelines aim to tighten control over REs' investments in these funds.

LEGAL TALK

Downstream investments, though not defined in these guidelines, have been defined under Rule 23 Explanation (g) of the Foreign Exchange Management (Non-Debt Instrument) Rules, 2019 as investment made by an Indian entity which has total foreign investment in it, or an Investment Vehicle in the capital instruments or the capital, as the case may be, of another Indian entity. As per the directions REs are prohibited from investing in any scheme of AIFs which has downstream investments either directly or indirectly in a debtor company of the RE. Additionally, if a RE has already invested in an AIF scheme and that scheme makes a downstream investment in a debtor company of the RE, the RE has to liquidate its investment within 30 days. For the REs who have investments in such AIF schemes as on date, their 30-day period will begin from the date of issuance of the circular (19 December).

The guidelines provide for REs to make a 100% provision on their investments if they are unable to liquidate them within this time frame. The directions further stipulate that investments by REs in the subordinated units of any AIF scheme employing a "priority distribution model" will be fully deducted from their capital funds. This provision, as per SEBI's circular issued in 2023, targets AIF schemes with waterfall distribution models where subordinated unit holders suffer a disproportionately greater share loss relative to other investor classes in case of losses.

The action of the RBI is aimed to deal with the problem of REs evergreening loans through the AIF route. Evergreen loans are the loans that never end. This tactic, where REs mask non-performing loans by offering new loans through AIFs as investment vehicles, artificially inflates credit profiles and skews non-performing asset (NPA) ratios. The new guidelines aim to curtail this practice and promote transparency in loan portfolios.

THE WAY FORWARD

The regulatory intervention will impact both the REs and AIFs. REs accustomed to the practice of evergreening may face challenges as they will no longer be able to conceal these loans from being listed as NPAs. AIFs which are reliant on investments from these entities may experience a setback on their ability to raise funds





ARTIFICIAL INTELLIGENCE



SECTION 4



AI DRIVEN SURVEILLANCE BANNED BY THE EUROPEAN UNION

NEWS

The European Union ('EU') has banned the use of real-time AI-driven biometric data by police and security bodies without judicial authorization, except for specified serious crimes or terrorist threats. Compliance with the new AI prohibitions is required by June across the EU, as per the historic Artificial Intelligence Act ('AI Act')

LEGAL TALK

The ban provides for three exceptions, it means police would be able to use the invasive technologies only in the event of an unexpected threat of a terrorist attack, the need to search for victims and in the prosecution of serious crime. This ban responds to concerns about data privacy and potential misuse, particularly in the absence of specific regulations governing biometric data processing under frameworks like General Data Protection Regulation ('GDPR') and the AI Act. The ban addresses this legal gap by establishing clear limitations on the technology's application, seeking a balance between security needs and individual privacy rights.

THE WAY FORWARD

The ban in the EU represents a first amidst privacy concerns due to AI across the globe. Despite the new GDPR addressing many concerns, the use of biometric data remained a problem. The new ban helps in filling up that gap. However, a blanket interpretation of the same cannot be implemented across the EU. Deviations and further exceptions have to be made according to the needs of all EU member states. Similar protests have been noticed in the state of Kerala, India when use of AI surveillance cameras in traffic were violative of privacy laws. To catch up with the fast-paced development of AI, laws to regulate and address privacy concerns are the need of the hour.



OPENAI'S DEAL TO USE LICENSED MEDIA FOR TRAINING ITS PRODUCTS

NEWS

Last week, [OpenAI](#) and the German media conglomerate Axel Springer [signed](#) a multi-year licensing agreement. It allows OpenAI to incorporate articles from Axel Springer-owned outlets like Business Insider and Politico into its products, including ChatGPT.

LEGAL TALK

Prominent AI firms obtain their training data by scraping the internet without initially obtaining licenses for the copyrighted materials they utilize. This has triggered a series of legal actions, spearheaded by Matthew Butterick, targeting companies such as OpenAI and Meta. In lieu of engaging in permissionless scraping to acquire Axel Springer's articles, OpenAI has adopted a practice of paying to incorporate news stories into its products.

OpenAI, aiming to avoid legal complications, has transitioned from scraping Axel Springer's articles to a paid model for incorporating news content into its products. This addresses copyright concerns, but privacy issues persist. Services like ChatGPT, trained on vast data sets, may generate biased texts reflecting the opinions of the sources used. This raises questions about liability: could Axel Springer be held responsible for the dissemination of potentially biased or harmful information through its articles utilized in AI training? The question of liability, particularly in the context of Axel Springer's role as an information provider, necessitates further exploration and nuanced legal frameworks to navigate the complexities of AI training and its potential impact on society.

THE WAY FORWARD

Although this approach may regulate the news articles used to train AI products, it doesn't guarantee accountability from AI giants in delivering responsible outcomes. The method, while addressing one aspect, falls short in ensuring responsible behaviour and transparency in the overall AI development process. Stricter measures are needed to hold these AI giants accountable for the impact of their products on society and to foster a more responsible and ethical AI ecosystem.

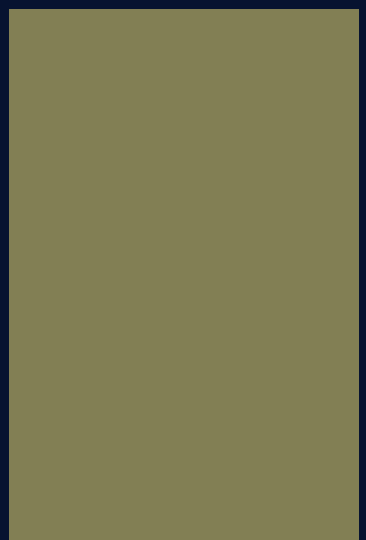




DATA PRIVACY



SECTION 5



META INTRODUCES NEW “PAY OR CONSENT” MODEL AMIDST EUROPE-WIDE RESTRICTIONS

NEWS

Meta has introduced a contentious "Pay or Consent" model in Europe to comply with the General Data Protection Regulation (“GDPR”). This unique model offers users two options for data and platform access (Facebook and Instagram): the first option allows users to pay for an ad-free subscription, eliminating targeted ads and potentially limiting data collection; the second option provides a free ad-supported version with familiar features, but users ‘technically’ consent to data collection by using this version.

LEGAL ANGLE

Section 4 of India's Digital Personal Data Protection Act 2023 ("DPDPA") mandates that personal data processing by an individual must align with DPDPA and serve a lawful purpose, contingent upon the Data Principal's consent. The Data Principal's consent must be a free, unconditional, and specific affirmative action. The Data Fiduciary must provide a notice before or along with every request for consent. This notice should outline the required personal data and the intended processing purpose. When one agrees to give consent, they permit the processing of personal data only for the purpose specified in the notice. The paid ad-free version of the Meta model lacks clarity on data collection limitations, raising concerns about undisclosed tracking practices. This lack of transparency goes against the principles of the DPDPA, which mandates data principals to be clear and upfront about their data processing purposes. The DPDPA's consent requirement aligns with the GDPR. Although the DPDPA's definition of personal data is similar to the GDPR's, it does not cover personal data made public by the data principal or by any other person under a legal obligation to make that data publicly available.





THE WAY FORWARD

The current model arguably also fails to provide consumers with a genuine opportunity for 'free and unconditional' consent. Users are compelled to participate in social networks without the option to opt out, placing Meta in control of their social connections. Leaving the services results in the loss of contacts and interactions, while staying entails being tracked or incurring a cost. The model forces users into a difficult predicament, forcing a trade-off between the desire to safeguard their privacy and the additional financial burden imposed by the subscription fee. Meta's 'free' option might feel more like a mirage of freedom, considering users end up paying with their data. Users must have the freedom to individually refuse consent to certain data processing operations without being forced to completely waive the use of the service. In Justice K.S. Puttaswamy v Union of India, the Court affirmed that the right to privacy is intrinsic to fundamental rights, emphasizing its importance in upholding dignity, autonomy, and liberty. Engaging in open and critical discussions about this model is crucial to safeguard user rights and prevent the emergence of a digital landscape where privacy becomes a luxury rather than a fundamental right.



PANORAMA VIEW



SECTION 6





THE COMPLETE PICTURE: DECODING THE MAHADEV APP SCAM FROM A LEGAL ANGLE

BACKGROUND

The Ministry of Electronics and Information Technology (“MeitY”) last month took action against illegal betting activities by banning 22 apps, including the Mahadev app.

WHAT IS THE MAHADEV APP?

Sourabh Chandrakar and Ravi Uppal, originally from Chattisgarh and currently based in Dubai, initiated the Mahadev app. This platform facilitates illegal betting activities which involve poker, card games, badminton, tennis, football, and cricket. Additionally, the app offers virtual games such as Teen Patti.

HOW THE APP FUNCTIONS?

The application is promoted across various websites to entice individuals into participating for monetary gains. A designated contact number is supplied, typically on platforms like WhatsApp. Upon reaching out to this number, interested players are furnished with two distinct numbers. The initial one is utilized for depositing funds and converting them into points within the app for betting purposes. Meanwhile, the second number facilitates the withdrawal of the earnings accrued by the player. The Mahadev app was purportedly utilizing the online betting platform to register new users, generate IDs, and engage in money laundering through a complex network of undisclosed (benami) bank accounts. The gaming structure is strategically designed to initially attract players with wins, encouraging continued participation. Subsequently, the game is orchestrated to ensure that promoters do not incur losses, placing players at substantial financial risks. Operating on a franchise model, the app follows a 70:30 profit distribution ratio. Franchise owners are entrusted with promoting the app within their designated regions. This franchise approach serves to shield the actual promoters, Sourabh and Ravi, as it establishes a vast and intricate network, complicating efforts to apprehend them. Notably, the app has been reported to generate a daily profit of Rs. 200 crores, with funds transferred through hawala channels to Dubai.

ASSOCIATED LEGAL ISSUES

IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023

According to the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 only online real-money games that do not involve wagering or any specific outcome are permissible. The rules, however, do not provide a clear definition for the terms "wagering" or "outcome." The MeitY holds the authority to issue blocking orders against such games. The Law Commission of India, in Report No. 276, defines wagering as a broad term encompassing diverse forms of gambling and betting, without the necessity of an opposing party. It also includes predicting both the occurrence and non-occurrence of events. This expansive definition of wagering makes the Mahadev App potentially violating the established guidelines.

Information Technology Act, 2000

The blocking orders can be executed under Section 69A of the Information Technology Act, 2000. This section empowers the central government to restrict the use of any website or application that is found to violate public order, defence, security, friendly relations with other states, or the sovereignty and integrity of the nation. The 22 apps including the Mahadev app were banned under the same section.

Prevention of Money Laundering (PMLA)

On December 13th, Ravi Uppal, one of the proprietors, was apprehended under Section 19 of the Prevention of Money Laundering Act (PMLA). The app owners face charges under Section 3 of PMLA, which pertains to the offense of money laundering. Any individual involved, directly or indirectly, in the concealment, possession, acquisition, use, or projection of proceeds of crime as untainted property is considered to have committed money laundering. The penalty for money laundering is stipulated under Section 4 of PMLA.

Consumer Protection

The Consumer Protection (E-Commerce) Rules, offer a broad definition of e-commerce entities, encompassing any person who owns, operates, and manages a digital or electronic platform for electronic commerce. This expansive definition can make real money online gaming platforms fall within the scope of e-commerce entities. Consequently, the application of Consumer Protection Rules may extend to regulate and govern the activities of real-money online gaming platforms, ensuring consumer protection within this digital domain.

Foreign Exchange Management Act, 1999

The gaming entities are generally registered in small island nations. Bank accounts are opened in India in the name of Proxy persons who don't have any relation with gaming. Money collected through these applications are transferred to multiple bank accounts and ultimately in form of remittances of import of services and goods taken out of the country. As per ED, the amount nears to Rs. 4,000 crores.

The Reserve Bank of India ("RBI") has issued Master Directions on 'Other Remittance Facilities' which restricts on remittances that are related to participation in lottery-like schemes, which may exist under various names such as money circulation schemes, or remittances intended for securing prize money or awards. Individuals who engage in online real-money games are obliged to make payments in foreign currency making it a prohibited transaction.

Central Goods and Services Tax, 2017

The Integrated Goods and Services Tax (Amendment) Act, 2023 requires offshore online money gaming operators to obtain mandatory Goods and Services Tax ("GST") registration. If the entity Fails to register it could result in the GST department blocking any information generated, transmitted, received, or hosted in any computer resource used for the supply of online money gaming by the offshore operator. A significant number of platforms are evading tax as they operate offshores and are not registered under GST, but these platforms are easily accessible on internet.

THE WAY FORWARD

As the ED delves into the intricacies of the matter, the government should institute robust regulations aimed at curbing tax evasion and money laundering facilitated through online gambling. The MeitY should identify the other gambling activities operating in the same manner and try to strike down all the apps. The government should take decisive action against all illegal betting sites, closing the legal loopholes that these entities exploit for their operations. Implementing stringent measures will be crucial in addressing the issues of tax evasion, money laundering, and the illicit operation of betting sites.



CONTRIBUTORS

DESIGNERS

SAMRIDHI BAJORIA

NAMAN OSTWAL

WRITERS

LAVANYA CHETWANI

ANJALI PANDE

TRISHNA AGRAWALLA

KUSHAL AGRAWAL

UTSAV BISWAS

NAMAN OSTWAL

EDITORS

NIKHIL JAVALI

HARSH MITTAL

**LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP
AND INNOVATION**

CONTACT US:



[INSTAGRAM](#)



[LINKEDIN](#)



[EMAIL](#)