LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

FEBRUARY 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

DRAFT GUIDELINES RELEASED FOR CURTAILING MISLEADING ADVERTISEMENTS BY COACHINGS

NEWS

The draft 'Guidelines for Prevention of Misleading Advertising in Coaching, 2024' ("Draft Guidelines") have been opened for public comments by the Central Consumer Protection Authority ("CCPA"). These guidelines are released after widespread complaints against certain coaching centres for 'misusing' the names and photos of successful candidates in various competitive examinations, including the civil services exam.

LEGAL TALK

Misleading advertisements are defined under Section 2 (28) of the Consumer Protection Act, 2019 ("CPA"). In the context of coaching institutions, it includes concealing important information related to name of the course (whether free or paid) & duration of course opted by successful candidate, making false claims regarding success rates, selections or rankings without providing verifiable evidence, and falsely representing students' success is solely attributable to the coaching. These guidelines are a positive development in light of the education industry, however, they fail to specify any repercussions specifically directed at coaching institutions if they fail to comply with the guidelines. It's unclear whether the consequences for such non-compliance would be under Section 89, CPA for misleading advertising in general, or there would be added consequences for coaching institutions. Additionally, it does not demarcate the liability of the faculties of coaching institutes from the directors or owners of such institutions.

THE WAY FORWARD

The Guidelines are a good step forward to curtail misleading advertisements in the education industry, despite the mentioned ambiguities. It ensures that a skewed picture is not presented to the public and also warrants privacy of the successful candidates being advertised. These guidelines have broadened the definition of "misleading advertisement" in the context of academics and education, ensuring the right information is advertised and protecting the consumers from being misled.

BOMBAY HIGH COURT SPLIT VERDICT OVER GOVERNMENT'S ONLINE FACT-CHECKING PROPOSAL

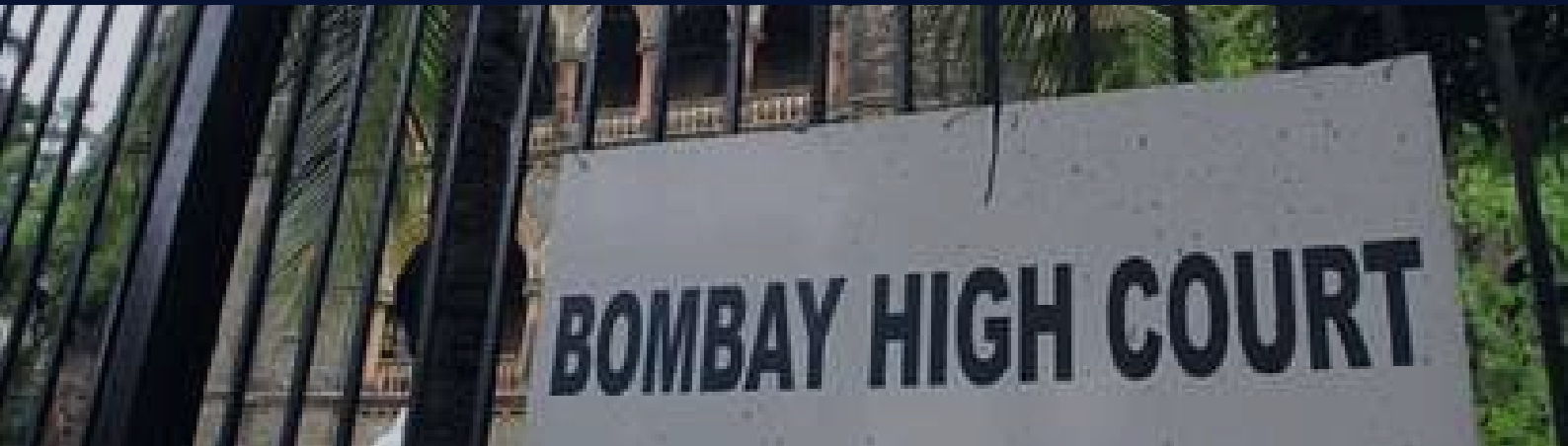
NEWS

The Bombay High Court issued a split verdict on petitions challenging Rules 3(i)(II)(A) & (C) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2023 (“Amendment Rules”), which empower the central government to establish a fact-checking unit (FCU) to tackle misinformation on social media. The rules target Section 79(1) of the Information Technology Act 2000 (“IT Act”), threatening platforms' legal immunity for non-compliance. The FCU, comprising government and media/law experts, will ensure content validation, aiming to curb the spread of false information on platforms like X and Facebook.

LEGAL TALK

In this particular case, the petitioner contended that the Amendment Rules violated Section 79 of the Information Technology Act, 2000 (hereinafter, "IT Act") and infringed upon fundamental rights guaranteed by Articles 14, 19(1)(a), and 19(1)(g) of the Indian Constitution, including the freedom of speech and the right to engage in any profession.

The Bombay High Court delivered a verdict on the challenge to the IT Rules 2023. One judge, Justice Patel, raised concerns about the amendment's impact on free speech and equal protection. He opined that the rules create an unfair system where online platforms have no say in content flagged by the government and cannot contest takedown notices for government-related information, even in court. Additionally, he found the terms used in the amendment, like "fake" and "misleading," to be unclear and potentially discriminatory. He ultimately concluded that the amendment was unconstitutional. While Justice Patel saw the IT Rules as detrimental to free speech, Justice Gokhale offered a contrasting view. She held that intermediaries have options for flagged content, and the FCU only identifies misinformation, not removing it directly. Additionally, immediate penalties are absent. Highlighting the rule's limited scope targeting demonstrably false information and clear terms like "business of the government," she emphasised existing safeguards against potential misuse. In essence, Justice Gokhale found the rule constitutional, presenting a viewpoint distinct from Justice Patel's critique.



Supporting Justice Patel's perspective is crucial as it underscores the importance of upholding free speech and protecting individual liberties in the digital realm. His critique of the amendment's potential impact on free speech, lack of intermediary rights, and the need for clarity in the regulatory framework aligns with the fundamental principles of safeguarding constitutional rights. Whereas Justice Gokhale's viewpoint, while upholding the amendment rules, overlooks the potential for abuse and the need for clear procedural safeguards against the indiscriminate removal of content. Additionally, her assertion that the fact-checking unit's potential bias is premature disregards the need for proactive measures to prevent arbitrary content takedowns, potentially undermining free speech and expression

THE WAY FORWARD

With the certain divide of opinion between Judges Gokhale and Patel, now a third judge, Justice A.S. Chandurkar of the Bombay High Court, is set to preside over hearings concerning petitions challenging the IT Amendment Rules. The way forward could involve a review of the petitioners' claims regarding breaches of Section 79 of the IT Act and infringements upon fundamental rights, including freedom of speech and the right to engage in any profession.

WHATSAPP'S INTEROPERABILITY: GATEWAY TO MESSAGING EVOLUTION

NEWS

The forthcoming integration of messaging platform interoperability within WhatsApp has garnered significant attention, particularly in light of Meta's classification as a "Gatekeeper" pursuant to the EU's Digital Markets Act of 2022 ("DMA"). The move prompts discussions on technical viability, regulatory concerns over data privacy, and safeguarding users' sensitive information.

THE WAY FORWARD

The DMA clearly outlines that Gatekeepers must maintain high-security standards, which other applications seeking integration must adhere to. While Gatekeepers hold significant responsibility to oversee security, they shouldn't engage in anti-competitive practices to eliminate competitors solely based on security standards. Regulatory bodies must play a role in determining breaches fairly. One potential solution could be adopting a universal encryption standard across messaging platforms, simplifying DMA compliance. However, implementing this within the Act's strict timelines may be impractical for Gatekeepers. As a result, different encryption levels may persist for cross-platform messaging, potentially affecting user experience by segregating messages within the app interface. Balancing security requirements with competition and user experience remains a challenge under the DMA.

LEGAL TALK

The DMA aims to address anti-competitive practices of the major text messaging service providers dominated by a few major players like WhatsApp and iMessage. Article 7 of the DMA lays down requirements for major players in industries like Meta, Google, or Microsoft, known as gatekeepers, to introduce interoperability services. These services will enable users to communicate seamlessly across various messaging platforms, WhatsApp to Telegram or Signal to WhatsApp and vice versa etc, within set timeframes. This move aims to enhance communication between different messaging apps, promoting greater connectivity and convenience for users. While this move is intended to foster competition and innovation, concerns arise regarding its impact on security and encryption standards.

The DMA, sets strict timelines for achieving interoperability, like making sure different text messaging services can work together within just six months. However, this rush can pose serious challenges to security. Not all messaging apps use the same level of encryption, so trying to make them all conform to one standard in such a short time frame is quite the uphill battle.Cybersecurity experts argue that maintaining consistent standards across platforms with varying encryption levels is challenging without sacrificing security or privacy. Article 5 of the GDPR permits data processing to counterbalance reduced security, as might occur with the introduction of interoperability in text messaging apps. This suggests a need to balance security and interoperability. If security standards drop, increased data processing could mitigate risks, yet this raises concerns about user privacy and the extent of data processing.

In the realm of EU regulations, Articles 7 and 8 spotlight the significance of safeguarding personal data and privacy. When it comes to DMA, there's a delicate balance to maintain between fostering interoperability and respecting these fundamental rights. While ensuring interoperability within a tight timeframe might raise concerns about security standards, it's vital to distinguish between security, encryption, and data privacy. As long as stringent measures are in place to protect sensitive information and uphold end-to-end encryption, striving for interoperability shouldn't be seen as running afoul of the EU Charter.

Online Gaming and Betting Laws

SECTION 2

ONLINE REAL MONEY GAMES: GAMING OR GAMBLING?

INTRODUCTION

The Indian online gaming industry has witnessed exponential growth in recent years, particularly among young adults, solidifying its position as a mainstay. This increasing popularity is further evidenced by the Indian Olympic Association's inclusion of online gaming as a medal event in the 2022 Asian Games, signifying its evolution beyond leisure activity and potential to foster professional athletes. However, a crucial question remains: do online games involving real-money transactions constitute gambling? This blog delves into this complex issue, exploring the intersection of gaming and gambling in the digital age.

SKILL v CHANCE

The legal classification of online games involving real money transactions as "games of skill" or "games of chance" is crucial in determining whether they constitute gambling or not. Consequently, an understanding of the legal distinction between "skill" and "chance" is imperative in analysing the nature of such online games. This distinction arises from a nuanced legal landscape shaped by various judicial pronouncements over the years. These judgments have redefined the perception of certain activities, previously considered solely based on chance, as legitimate expressions of skill. Notably, such "games of skill" fall under the protection of Article 19(1)(g) of the Constitution, guaranteeing the right to pursue professions and engage in business activities.

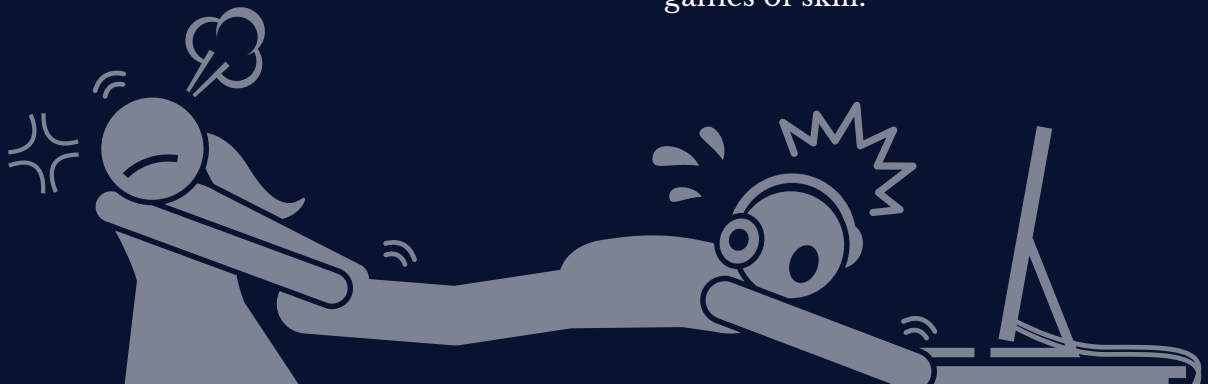
In RMD Chamarbaugwala v. Union of India, the Supreme Court (“**SC**”) established a crucial distinction: competitions involving "substantial skill" form a separate category, distinct from gambling, and qualify as protected business activities. Building upon this foundation, the court, in K. R. Lakshmanan v. State of Tamil Nadu, clarified that a "game of mere skill" requires a "predominant and preponderant" reliance on skill. The court further differentiated "gaming" from "games of skill," defining the former as wagering or betting on chance-based outcomes. This distinction led the court to conclude that skill-intensive competitions cannot be equated with gambling.

The application of this framework to card games was explored in State of Andhra Pradesh v K. Satyanarayana & Ors. and the State of Bombay v R.M.D. Chamarbaugwala. Here, the court specifically examined rummy through the "skill vs. chance" lens. While acknowledging the element of chance introduced by shuffling and dealing cards, the court ultimately categorised rummy as a "game of skill" as it highlighted the crucial role of skill in rummy, particularly memorising card sequences and strategically managing one's hand for an advantage. This emphasis on skill distinguishes rummy from games like "Teen Patti Flush," which lack such skill-based elements and are consequently classified as "games of chance." These SC judgments establish a legal framework in India where games demonstrably requiring a significant degree of "skill, knowledge, experience, and judgement" by the player are categorised as "games of skill" and are not subject to gambling regulations.

ONLINE v OFFLINE: IS THE STORY THE SAME?

While the judgments in the previous section addressed rummy and poker in a physical setting, the legal status of their online counterparts remained unclear. This was addressed in All India Gaming Federation And Ors. Vs State Of Tamil Nadu. Here, the state argued that online games lack genuine card shuffling, relying instead on software and random number generators. They contended that this introduced an element of chance not present in physical games, shifting them into the realm of gambling. However, the Court rejected this argument. It reasoned that the mere transition from physical to online format could not alter the fundamental nature of the game, nor could it negate the established classification of rummy and poker as games of skill.

The Court emphasised that the core element of skill in these games, as recognized in previous judgments, remains unchanged regardless of the platform. Additionally, the Court dismissed concerns regarding the use of artificial intelligence bots, holding that their presence does not introduce an undue element of chance. This stance aligns with the findings of a study by Prof. Tapan K. Gandhi of IIT Delhi, which concluded that the distinction between online and offline versions of these games is negligible in terms of required skill. Furthermore, the Karnataka High Court (“**HC**”) has also adopted a similar approach, recognizing both online and physical rummy as games of skill.



RMGs: GAMBLING OR GAMING?

In India, gambling falls under the legislative purview of individual States. This empowers each State to enact its own laws governing gambling activities within its jurisdiction. However, a central law, the Public Gambling Act, 1867, exists and serves as a foundational framework. Many States have adopted this Act with their own amendments, creating a patchwork of legal regulations across the country. These laws primarily target games predominantly reliant on chance and involving the wagering of money. Nevertheless, Section 12 of the Public Gambling Act exempts "games of skill" from its application, effectively excluding them from the legal definition of gambling. This distinction is critical for Real Money Games ("**RMGs**"), online platforms facilitating games with real-money transactions. Judicial precedents as discussed in the previous section have established that games like Rummy and Poker, both online and offline, qualify as games of skill. This inherent skill-based element differentiates them from gambling activities as defined by the Act. Consequently, RMGs featuring games like Rummy and Poker are legally distinct from gambling activities despite involving wagers and monetary transactions.

STANCE OF SUPREME COURT

IThe SC of India has not yet definitively established whether online games of rummy and poker constitute games of skill or chance. In the Mahalakshmi Case , the Court had the opportunity to address this issue, specifically regarding the classification of rummy under the Gambling Act. However, the Tamil Nadu government informed the Court that it had not yet determined whether the state's specific Gambling Act applied to online games. Consequently, the SC declined to rule on the matter at that time.
Furthermore, judgments from the Madras and Karnataka HC as discussed above, classifying these games as skill-based, are currently pending consideration by the SC. Here, the Tamil Nadu government has challenged the Madras HC's ruling, as gambling falls under the purview of state subjects in India. If the SC ultimately classifies these online games as "games of chance," they would fall within the purview of gambling regulations, granting states the authority to regulate or even ban them entirely. Conversely, a "game of skill" designation would likely exempt them from such restrictions.

CONCLUSION

The legal landscape surrounding online RMGs involving skill-based games like Rummy and Poker remains unsettled in India. While established legal precedent categorises physical Rummy and Poker as "games of skill" distinct from gambling, the status of online versions requires further clarity. The SC had the opportunity to address this issue in the Mahalakshmi Case but deferred its decision due to the Tamil Nadu government's concerns regarding the applicability of its specific Gambling Act to online games. Additionally, judgments from the Madras and Karnataka HC, classifying online Rummy and Poker as skill-based, await final determination by the SC, further complicated by the Tamil Nadu government's challenge.

Therefore, the definitive legal classification of online RMGs like Rummy and Poker, as either "games of skill" or "games of chance," hinges on a future SC judgement. This judgement will significantly impact the regulatory framework surrounding these online games, determining whether they fall under the ambit of gambling regulations or remain exempt as protected activities requiring significant skill and strategy from participants.

---

[1] Special Leave to Appeal (C) No(s).15371/2012 (Arising out of impugned final judgement and order dated 22/03/2012 in WA No. 2287/2011 passed by the High Court of Madras).

FinTech

SECTION 3

RBI HALTS BUSINESS PAYMENT SERVICE PROVIDERS OPERATIONS

NEWS

On February 15, 2024, the Reserve Bank of India ("**RBI**") took a significant step by directing an unspecified card network to immediately cease all business payments made through payment intermediaries to entities that don't accept card payments. Fintech intermediaries facilitating these transactions have also been asked to stop all transactions with immediate effect. As per industry sources, this was a special arrangement brought in by card networks, Visa and Mastercard.

LEGAL TALK

Several years ago, fintech intermediaries joined forces with banks to introduce co-branded credit cards tailored for businesses. These corporate credit cards became a convenient solution for businesses to make payments to vendors who typically accepted only bank transfers or checks. Acting as intermediaries, fintech companies would authorise the card payment and then transfer the necessary funds to the supplier through electronic channels like NEFT or RTGS. This particular method had notable advantages. Businesses, given the nature of credit cards, were granted a period of up to 45 days to settle their dues with the bank. Simultaneously, suppliers received prompt payments, and the fintech intermediaries earned a modest fee for facilitating the transaction. These entities were termed Business Payment Service Providers ("BPSP"). The phrase BPSP has not been properly defined anywhere and the industry lacks strict regulation, which has created a legal gap.

Following its notification, RBI has stopped the functioning of BPSPs. They noted that fintech intermediaries were pooling funds into an account that lacked designation as a recognized payment system under the Payment and Settlement Systems Act, 2007 (“**PSSA**”). According to Section 2(1) of the PSSA, a 'payment system' involves the payment, settlement, and clearing of funds, encompassing systems enabling credit card operations. The operation of a payment system requires explicit authorization from the RBI.

This discovery led to worries about the inability to trace the transaction trail from the BPSP's account to the vendor's bank account, and potential risks of money laundering or round-tripping of funds. Additionally, the established setup failed to fully comply with Know Your Customer (“**KYC**”) norms, raising the possibility of illicit financial activities, such as manipulating invoices. There were also concerns about businesses misusing these credit cards for personal transactions, like paying rent, which deviates from the intended use of merchant-to-merchant transactions. In formalising these concerns, the RBI acted to ensure regulatory compliance, safeguard financial systems, and address potential loopholes in the prevailing financial practices.

THE WAY FORWARD

The new rule aims to enhance transparency and regulatory compliance by temporarily halting BPSP operations. The RBI intends to scrutinise and potentially revamp existing processes involving these financial intermediaries, focusing on ensuring adherence to regulations and mitigating risks like opaque transaction trails, money laundering, and KYC non-compliance. For fintech intermediaries in this arena, the regulatory shift poses challenges, disrupting a model integral for businesses in managing vendor payments. The sudden halt in operations might lead to a disruption in services, causing inconvenience for businesses that have come to rely on these platforms for their day-to-day financial operations. Moreover, the regulatory scrutiny could necessitate adjustments to business models and practices to align with the RBI's guidelines. However, there's hope in the ecosystem, that the RBI might offer guidelines instead of a complete shutdown of BPSP operations.

RBI ALLOWS BANKS AND NBFCS TO ISSUE PPIS FOR PUBLIC TRANSPORT SYSTEMS

NEWS

To provide convenience, speed, affordability, and safety of digital modes of payment to commuters for transit services, the Reserve Bank of India ("RBI") has decided to permit authorised bank and non-bank Pre-Paid Instruments ("PPI") issuers to issue PPIs for making payments across various public transport systems.

LEGAL TALK

The RBI's Master Directions, unveiled in February 2021, define PPIs as instruments that facilitate purchase of goods and services, financial services, remittance facilities, etc., against the value stored therein. The two categories of PPIs requiring RBI approval are Small PPIs and Full-KYC PPIs. Small PPIs, issued with minimal holder details, are authorised solely for purchasing goods and services, without allowing fund transfers or cash withdrawals. On the other hand, Full-KYC PPIs permit users to purchase goods, transfer funds, or withdraw cash. These are issued after completing the KYC process which is a mandatory process used to verify a client's identity.

Previously, only Mass Transit System ("**MTS**") operators, like the Delhi Metro Rail Corporation, could issue PPI-MTS for transit services. However, following the RBI's amendment, banks and non-banks can now issue them too. These instruments will feature the Automated Fare Collection ("**AFC**") application, specifically designed for transit services, toll collection, and parking. The AFC system automates the ticketing system of a public transportation service, ensuring a hassle-free experience. The maximum outstanding amount on these instruments is limited to Rs 3,000. While they allow for reloading, cash withdrawal, refunds, or fund transfers are strictly prohibited. Issuance of these instruments does not mandate KYC verification of the holder.

The decision to allow PPI-MTS issuance without KYC verification aims to broaden participation, particularly for various public transport users. However, the lack of KYC verification might create opportunities for individuals with malicious intent to exploit the system. Importantly, PPI-MTSs come with perpetual validity. This means that the usual provisions of validity and redemption outlined in Section 13 of the guidelines do not apply to them.

THE WAY FORWARD

RBI's approval of PPI issuance without KYC has opened up the avenue for digital payments in various sectors like metro, bus, train, waterways, tolls, and parking services. This significant step is poised to propel the advancement of India's homegrown digital payments infrastructure, contributing to the overall growth of the nation's financial landscape. The fintech sector, in particular, stands to benefit directly from these amendments, empowering allied startups to offer commuters digital wallets and other services for transit. Moreover, the introduction of perpetual validity for these instruments adds another layer of convenience. Commuters will experience the sustained ease of digital payments for metro, bus, train, waterways, tolls, and parking services without the concerns of validity periods. The perpetual validity enhances user experience and promotes long-term adoption of digital payment solutions.

THE RESERVE BANK OF INDIA'S IMPOSITION OF RESTRICTIONS ON PAYTM PAYMENTS BANK LTD

NEWS

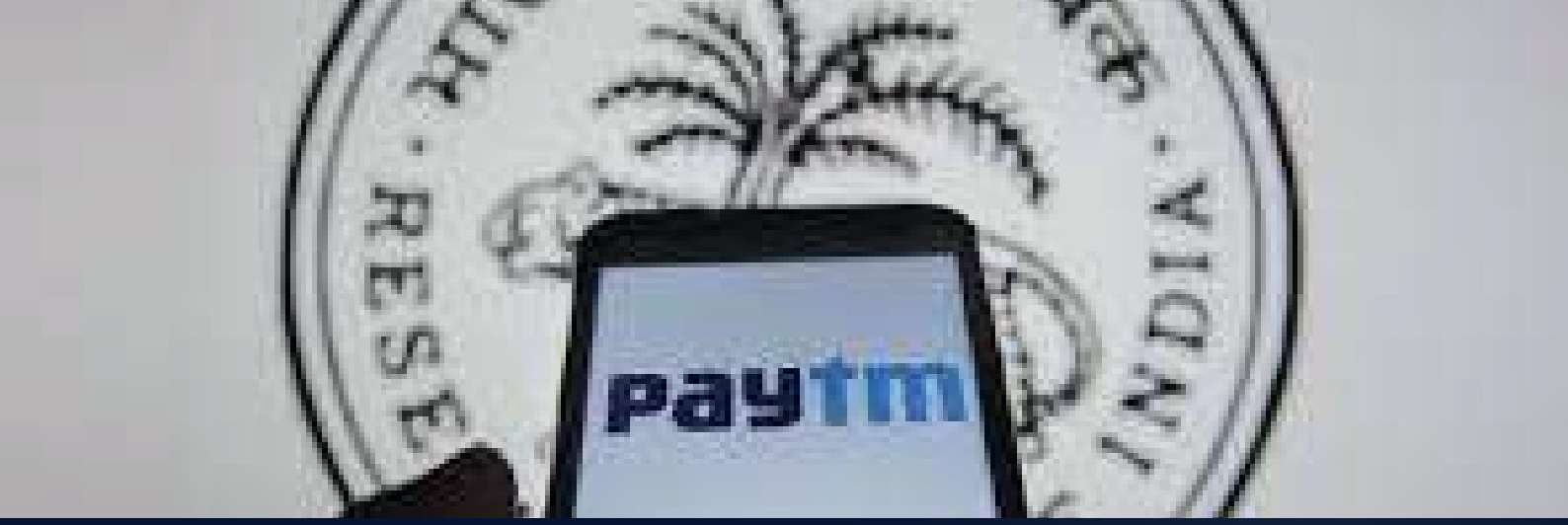
The Reserve Bank of India ("**RBI**") on January 31, 2024, and through a subsequent press release of February 16, 2024, directed Paytm Payments Bank Limited ("**PPBL**") to restrict certain banking activities. The RBI's actions stem from its identification of persistent non-compliances and ongoing material supervisory concerns with respect to PPBL.

LEGAL TALK

The RBI identified persistent non-compliances and ongoing material supervisory concerns at PPBL through external audits, including irregular Know Your Customer ("KYC") compliance and alleged related party transactions. Consequently, the RBI, under Section 35A of the Banking Regulation Act, 1949, directed PPBL to stop onboarding new customers with immediate effect, among other restrictions including:

1. No additional deposits or credit transactions will be permitted in customer accounts, prepaid instruments, wallets, FASTags, or National Common Mobility Cards until March 15, 2024.
2. The bank will cease providing banking services, including fund transfers (such as AEPS, IMPS, etc.), BBPOU, and UPI facilities after March 15, 2024.
3. The Nodal Accounts held by One97 Communications Ltd and Paytm Payments Services Ltd at PPBL must be terminated no later than February 29, 2024.
4. All pending transactions in nodal accounts must be settled by March 15, 2024, and no transactions will be allowed thereafter.

This action by the RBI stemmed from multiple instances of non-compliance with regulatory norms, particularly those related to anti-money laundering



("**AML**") and related-party transactions. The RBI's system audit revealed deficiencies in PPBL's adherence to AML regulations, including inadequate KYC checks on client funds' origins, insufficient KYC measures during onboarding conducted by partner firms, and permitting transactions through merchant accounts with dubious fund sources. Additionally, the RBI observed recurring related-party transactions between PPBL and other Paytm group companies, raising concerns about potential conflicts of interest. These transgressions culminated in an order issued in March 2022 barring the bank from onboarding new clients due to concerns over founder Vijay Shekhar Sharma's indirect control over decision-making and operations.

Furthermore, acknowledging PPBL's inability to accept further credit into customer accounts, the RBI has advised the National Payments Corporation of India ("**NPCI**") to evaluate the request of One97 Communication Ltd ("**OCL**") to operate as a third-party application provider ("**TPAP**") for the UPI channel. This move aims to ensure the continued operation of the Paytm application through UPI. Additionally, if NPCI grants TPAP status to OCL, the RBI recommends a seamless migration of '@paytm' handles from Paytm Payments Bank to designated banks to prevent disruptions. To facilitate this transition, NPCI may certify 4-5 banks as payment service providers ("**PSP**") with proven capabilities to handle high-volume UPI transactions. Finally, for merchants using Paytm QR codes, the RBI has authorised OCL to open settlement accounts with alternative PSP banks, excluding PPBL, to enable uninterrupted digital payments via UPI using the '@paytm' user handle.

THE WAY FORWARD

The RBI's directive underscores the paramount importance of rigorous adherence to compliance and regulatory standards within the banking and financial industry. Banks should take the PPBL ban imposition as an example and should conduct comprehensive compliance reviews and enhance due diligence processes to meet regulatory requirements. This could include strengthening risk management frameworks, fortifying governance structures, and enhancing board oversight to ensure transparency and accountability. Moreover, embracing technological advancements and staying abreast of regulatory updates are essential for ensuring trustworthiness and mitigating risks in the long term.

ARTIFICIAL INTELLIGENCE

SECTION 4

COMPLIANCE OBLIGATIONS FOR INTERMEDIARIES/PLATFORMS UTILISING AI MODELS: ADVISORY FROM MEITY

NEWS

The Ministry of Electronics and Information Technology ("**MeiTY**") has on 1st March, 2024 issued an advisory to all intermediaries/platforms to undertake due-diligence obligations outlined under Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules").

LEGAL TALK

The advisory issued emphasised on intermediaries' legal obligations under the Information Technology Act, 2000 ("IT Act") and the IT Rules in relation to their use of Artificial Intelligence model(s) /LLM/Generative AI, software(s) or algorithm(s)on ("AI Models"). The advisory mandated that Intermediaries/Platforms are to ensure that the utilisation of AI Models does not facilitate the dissemination of unlawful content. This includes preventing the hosting, display, upload, modification, publication, transmission, storage, updating, or sharing of content that contravenes the stipulations outlined in Rule 3(1)(b) of IT Rules. Intermediaries/Platforms must also deploy measures to prevent bias or discrimination, particularly concerning content that may influence electoral processes. Furthermore, the advisory highlights the requirement for explicit permission from the Government of India for the deployment of AI models that are still under testing or deemed unreliable. Such models must be clearly labelled to notify users of their potential fallibility.

In parallel, Intermediaries/Platforms must inform users about the repercussions of engaging with unlawful content on their platforms.

This includes the potential consequences such as the disabling of access to or removal of non-compliant information, suspension or termination of access or usage rights, and legal action under applicable laws. Lastly, the advisory emphasises that intermediaries must label content created through their platforms, particularly if it may be utilised as misinformation or deepfake material. This labelling should include a unique identifier or metadata to identify the origin of such content, thereby enhancing accountability and enabling effective content moderation.

The Intermediaries/Platforms are required to ensure compliance with the advisory on immediate effect along with a Action Taken-cum-Status Report to the MeiTY within 15 days of the advisory. Non-compliance with these regulations may result in penal consequences, including prosecution under the IT Act and IT Rules.

THE WAY FORWARD

The advisory ensures intermediaries uphold legal and ethical standards, fostering trust and credibility among users and stakeholders. By implementing robust mechanisms to prevent unlawful content dissemination and promoting transparency in content labelling, intermediaries contribute to a safer digital environment. Additionally, enhanced user awareness and clear content moderation procedures help in mitigating the spread of misinformation and maintaining platform integrity. However, challenges such as ensuring AI model accuracy and addressing resource constraints may arise. Collaborative efforts, continuous monitoring, and investment in AI technologies are necessary to overcome these challenges and ensure effective compliance. Overall, while MeitY's directives provide a framework for responsible digital governance, addressing associated challenges is crucial for intermediaries to fully realise the benefits of compliance.

STOPPING THE SPREAD OF AI-GENERATED MISINFORMATION IN INDIA WITH MCA'S WHATSAPP HELPLINE

NEWS

The Misinformation Combat Alliance ("MCA") and Meta have announced that a dedicated fact-checking helpline on WhatsApp, aimed at combating deepfakes and deceptive AI-generated content, will be available for the public in March 2024.

LEGAL TALK

In collaboration with the MCA, Meta is launching a dedicated fact-checking helpline on WhatsApp. The purpose of this project is to proactively combat the spread of AI - generated false information, or deep fakes, which have the potential to mislead people on important public issues. The WhatsApp chatbot, which will provide multilingual support in English and three regional languages (Hindi, Tamil, and Telugu), will allow users to report deep fakes.

This initiative aligns with the rule outlined in 3(1)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, under these rules, Intermediaries, such as social media platforms like Meta, must implement mechanisms to detect and eliminate illegal content, including deep fakes, content that deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature within set time limits.

Meta and the MCA have built the system with a commitment to four outcomes: detection, prevention, reporting and awareness. This strategy is designed to not only combat the spread of deep fakes but also to educate the public about the dangers of AI-generated misinformation. Non-compliance with these standards may lead to substantial fines, such as being held liable for damages and even criminal prosecution in some instances.

THE WAY FORWARD

Establishing a third-party fact-checking programme demonstrates WhatsApp's dedication to eradicating false information by using impartial specialists to evaluate the veracity of material. Fact-checkers assess material, particularly media that has been edited or synthesised, to find instances of false information that can mislead viewers. By improving accountability and transparency in content moderation activities, this programme complies with regulatory requirements for platform governance.

DATA PRIVACY

SECTION 5

META'S PAID AD FREE SERVICES: HOW IS IT POSING A THREAT TO PRIVACY?

NEWS

European Consumer Organisation along with the consumer protection authorities have challenged Meta, the company behind popular social media platforms like Instagram and Facebook on its recent initiative to introduce 'subscription for no ads'. Meta recently introduced an option for users in the European Union, Switzerland, and the European Economic Area to subscribe to a monthly service that enables them to use the platform without receiving targeted personal advertisements.

LEGAL TALK

Paid ad-free services by Meta are in clear violation of the privacy of an individual. This new initiative of giving the choice to the people to retain or opt out of tailored advertisements comes as a response to providing an alternative way to use and to the evolving nature of the regulatory landscape of Europe which permitted legal bases for personalised advertising under the GDPR and also the introduction of the Digital Market Act.

The crux of the matter lies in the implications of this offer itself. Opting for the subscription means users' personal information will not be utilised for personalised advertising. This model, dubbed 'Subscription for no ads' is positioned as a consent solution amidst varying compliance deadlines faced by social media platforms. This subscription service acts as a model to obtain valid consent from the users, and the same has been acknowledged by France, Denmark, and Germany

Yet, the implication is that users who do not subscribe to the ad-free option will have their data processed for behavioural advertising by these platforms. While the privacy regulations within these platforms are upheld, the extent to which third- party websites and apps utilise this data remains uncertain. This approach aligns with the direction set by the court of Justice of the European Union (CJEU), which endorsed subscription models as a means for users to consent to data processing for personalised advertising.

But, the European Data Protection Board in its 2022 decision had clarified that the contract is not a suitable legal basis for processing of personal data carried out by Meta for behavioural advertising. This model of 'pay or consent' which might be economically viable to the Meta, seriously undermines the GDPR and poses a continuous threat acting as a precedent for other social media platforms to offer the same, leading to a grave situation where the users will be expected to pay to protect their privacy.

THE WAY FORWARD

The Meta model comes as a serious concern to the existing laws of GDPR in Europe and poses a grave precedent to the other social media platforms. A stricter and a more comprehensive rule is called for to curb such instances by these data collectors, which also address the legitimate business needs of these platforms.

CONCERNS OVER JOURNALISM UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

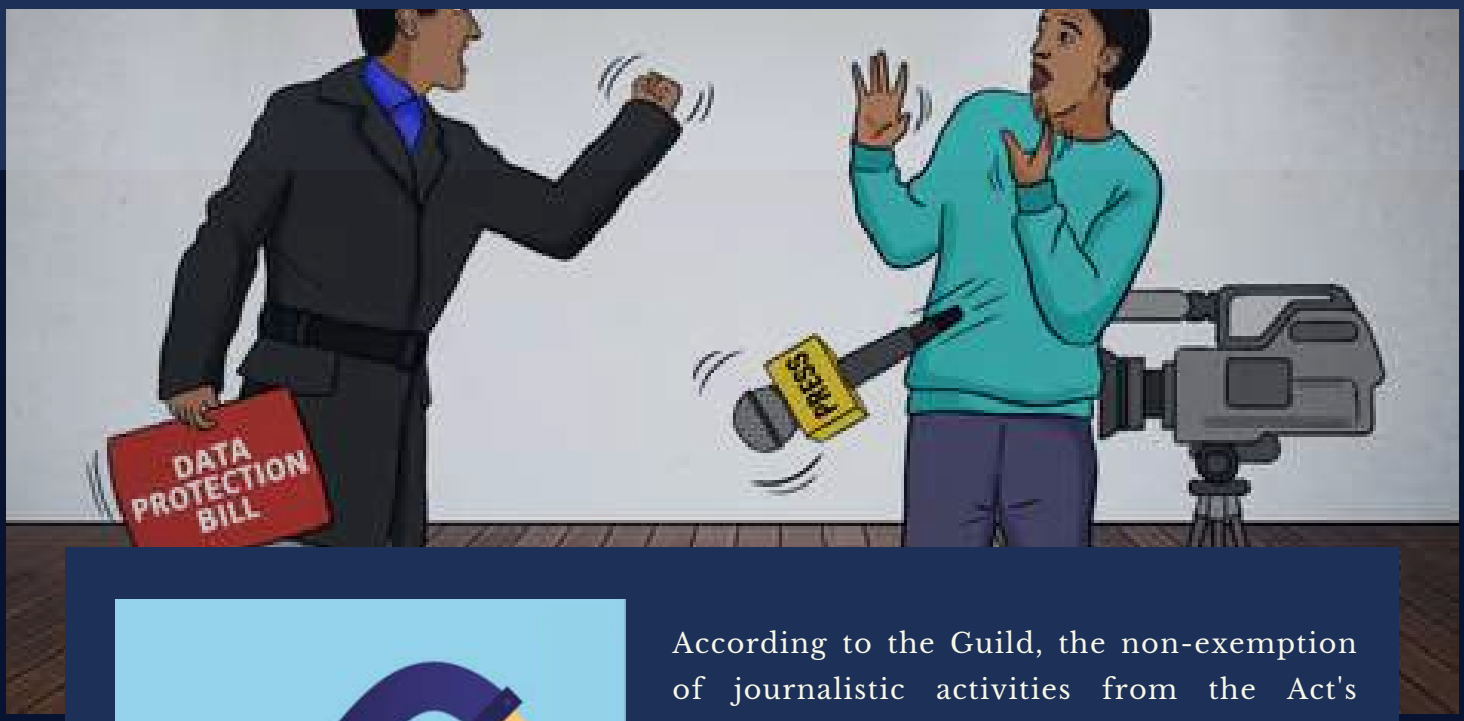
NEWS

Recently, the Editors Guild of India (‘**the Guild**’) expressed ‘grave concerns’ to the Union Ministry of Electronics and Information Technology regarding the impact of the Digital Personal Data Protection Act (‘**the Act**’) on journalist activities.

LEGAL TALK

Section 2(i) of the Act defines a "data fiduciary" as an entity responsible for determining the purpose and means of processing personal data. The absence of exemptions for journalists in the Act raises a significant concern, potentially impacting their activities in various ways.

One critical issue pertains to the mandatory requirement for obtaining consent, as outlined in Section 7 of the Act. This section permits data fiduciaries to process personal data based on consent or specific legitimate uses such as medical urgency or compliance with judgments. However, the narrow scope of these legitimate uses does not encompass data processing for journalistic purposes. Furthermore, the Act stipulates that data processing must be limited to "specified purposes." This presents a challenge for journalism, an inherently explorative field that often uncovers new leads or directions through particular pieces of information. Under the current provisions, journalists would be required to obtain consent from all data principals, leading to unreasonable delays that compromise the essential purpose of journalism. The Act also introduces the ability for data principals to withdraw their consent, posing a potential obstacle to the validation of news by journalists. Section 36 of the Act grants the Central Government powers to compel any data fiduciary or intermediary to furnish data it may seek. This provision raises concerns about its potential detrimental effect on journalism, as the confidentiality of information is crucial to investigative reporting. Journalists frequently rely on informants for sensitive information.



According to the Guild, the non-exemption of journalistic activities from the Act's provisions is perceived as a violation of fundamental rights, specifically the freedom of speech and expression (Article 19(1)(a)) and the right to practise any profession, occupation, trade, or business (Article 19(1)(g)) as guaranteed under the Constitution. However, sub-section (2) of the same Article empowers the State to impose reasonable restrictions on these rights. This authority is granted with the aim of safeguarding the interests of the State. One such permissible restriction, which aligns with this overarching objective, is the imposition of measures to uphold the right to privacy. In this context, preserving the right to privacy can be considered a reasonable restriction that the State may impose on journalists.

THE WAY FORWARD

The current provisions of the Act pose a significant threat to investigative journalism. Obtaining consent from all involved individuals could be impractical, hindering timely reporting and potentially silencing whistleblowers. Furthermore, journalists' reliance on confidential sources could be jeopardised by government data access powers, ultimately eroding public trust in the media's ability to hold power accountable. Finding a solution that balances privacy rights with press freedom through exemptions for journalistic activities, clear definitions for data processing purposes, and transparent data request mechanisms is crucial to prevent these detrimental consequences. Aligning the Act with international statutes, such as the EU's General Data Protection Regulation and Singapore's Personal Data Protection Act, which recognize exemptions for journalistic activities, is imperative. Notably, similar exemptions were considered in the 2019 and 2021 drafts of the Act. Implementing these adjustments will safeguard the essential role of journalism in society, ensuring its ability to operate freely.

CONTRIBUTORS

WRITERS

LAVANYA CHETWANI

ANJALI PANDE

TRISHNA AGRAWALLA

SAGUN MODI

ARYAN DASH

NAYANA KB

SHLOKA MATHUR

HARSH MITTAL

GARGI AGNIHOTRI

EDITORS

NIKHIL JAVALI

HARSH MITTAL

SAGUN MODI

DESIGNERS

SAMRIDHI BAJORIA

TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL