LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education initiative)

APRIL 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

सत्ये स्थितो धर्म

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

DIGITAL COMPETITION LAWS: CHECKING ABUSE OF DOMINANCE IN THE DIGITAL MARKETS

INTRODUCTION

India has experienced rapid digitization driven by increased internet accessibility. It has swiftly emerged as a hub for significant digital market segments spanning healthcare, financial services, and retail. This digital expansion has also fostered the growth of large digital enterprises, often functioning as multi-sided platforms offering services across various sectors. The emergence of these large digital enterprises and their distinctive business models has raised several antitrust concerns, which have been brought to the attention of the Competition Commission of India ("**CCI**"). These concerns encompass issues such as unilateral and opaque search ranking policies and the potentially anti-competitive use of aggregated data.

Recognising these challenges, the Committee on Digital Competition Law ("**CDCL**") was tasked with reviewing the Competition Act 2002 ("**the Act**") in the context of the context of the digital economy, analysing ex-ante regulatory models, studying international approaches to digital market regulation, examining government policies, scrutinising leading market players, and investigating other competition-related matters in digital markets. In pursuance of this, the Ministry of Corporate Affairs published a report consisting of the draft Digital Competition Bill along with CDCL's recommendations.

In this context, ten predominant anti-competitive practices of large digital enterprises were identified in the 53rd Report on "Anti-Competitive Practices by Big Tech Companies" ("**Standing Committee Report**"). The report emphasises the significant increase in growth of digital markets, driven by digitalisation and strong network effects favouring dominant digital players. To address this, the Committee suggests implementing a comprehensive ex-ante competition law model, proposing a new 'Digital Competition Act'. This legislation defines key terms and outlines lawful measures aiming to balance certainty and adaptability in regulating digital markets.

CDS and SSDEs

The Standing Committee recommended that the draft bill for proposed legislation should apply to specific Core Digital Services ("CDS") provided by firms having a significant market presence in the digital markets. Schedule I of the proposed legislation provides a non-exhaustive list of CDS, including online search engines, social networking services, video-sharing platforms, interpersonal communications services, operating systems, web browsers, cloud services, advertising services, and online intermediation services. The reason for the legislation being applicable to CDS is to regulate competition in the digital markets alongside the Act. It is based on the European Union's Digital Markets Act ("DMA") as it lists down core platform services to whom the Act shall be applicable.

Enterprises offering CDS may be designated as Systemically Significant Digital Enterprises ("SSDEs") if they meet certain prescribed conditions. The legislation aims to regulate only those enterprises with a significant market presence. An enterprise qualifies as an SSDE if it meets both financial and user thresholds; namely -

FINANCIAL THRESHOLD: It must satisfy at least one of four conditions over the preceding three financial years, including

- Turnover in India exceeding INR 4000 crore (USD 482 million)
- Global turnover surpassing USD 30 billion
- Gross merchandise value in India exceeding INR 16000 crore
- Global market capitalization exceeding USD 75 billion

USER THRESHOLD: An enterprise must meet at least one of two thresholds consistently for three financial years, which includes

- Turnover in India exceeding INR 4000 crore (USD 482 million) or
- More than 10,000 business users in India for its core digital services

CCI AND ITS POWERS

The proposed legislation grants the CCI residual powers to designate enterprises as SSDEs based on qualitative criteria, such as economic power, market integration, user dependence, and barriers to entry even if it does not meet the aforementioned thresholds. Before exercise of such power by CCI, to comply with the principles of natural justice, the enterprise will be allowed an opportunity to explain why it should not be designated as an SSDE.

When an SSDE is part of a group, and other enterprises of the said group are providing these CDS in India, directly or indirectly, then these other enterprises are termed as Associate Digital Enterprises ("ADEs"). The CCI has powers to designate entities as ADEs and shall be equally obliged to comply as an SSDE. For example, under the DMA, Meta has been labelled as a gatekeeper, which includes WhatsApp as a messaging service and Instagram as a social media service. The entire Meta group, in the Indian context, would be an ADE, as WhatsApp and Instagram are SSDEs.

THE EX-ANTE MEASURES

The current legal frameworks governing competition in India has ex-post measures in place wherein remedies are put in place after an anti-competitive practice has taken place. These frameworks, however, are not well-equipped as they are time-consuming and takes years before a solution is reached after investigations of the anti-competitive conduct have taken place. This has led the Standing Committee to suggest an ex-ante framework, i.e., a precaution taken before any anti-competitive practice takes place. This has further been done to ensure that remedies match the pace of digitalisation.

The CDCL Report holds answers of stakeholders to implementation of an ex-ante framework. While big giants like Google, Amazon and Zomato are against the proposed ex-ante framework, it is interesting to note that Paytm has agreed to the implementation of an ex-ante framework. The big tech firms argue that a copy of DMA may not be essential for the existing digital market in India and will hinder digital innovation. They state that consumer welfare should be the end goal of the legislation, but the proposed legislation seems to emphasise more on regulation of competition than to pay heed to consumer welfare status.

For example, in the European Union, users preferred having a direct link to Google Maps when they made a search on google, as it was convenient, but due to the DMA, the direct link has been removed to avoid preference of one's own services and comply with the DMA. Further, it took Google an unprecedented amount of time to implement Google AI due to the obligations imposed under DMA, and that such hindrance on digital innovation may discourage other players to innovate because they want to avoid such rigorous compliance. A similar situation may arise in India if the CDCL were to move forward with a replica of the DMA in India, hampering digital innovation and adversely impacting consumer welfare.

PENALTY

If SSDEs or ADEs fail to meet their obligations or violate CCI orders, the CCI can impose substantial monetary penalties, up to ₹1 lakh per day of non-compliance, with a maximum of ₹10 crores. Additionally, the CCI may penalise other group enterprises deemed contributory. Penalties are proposed to be calculated based on global turnover, with SSDE penalties capped at 10% of their previous financial year's global turnover to ensure a ceiling on the penalties that could be imposed in a case of contravention of the Digital Competition Bill.

THE WAY FORWARD

The main reason for implementing an ex-ante framework in the current digital landscape of India is that it is also being taken up in international jurisdictions that are experiencing digital growth spurts in their markets. However, implementation cannot be blindly copied on the basis of other jurisdictions and the same should be customised considering the Indian economy and the digital players. Further, international players like Amazon and Google are against the said framework on the grounds that implementation without testing the Act may adversely impact product innovation and benefits to customers. Flipkart has also stated that the one-size fits all approach similar to the DMA will be unsuitable. They have repeatedly stated that product innovation may take a hit, and despite stemming from personal interests, it should be paid close attention to as they have also highlighted possible misuse of powers.

Additionally, CCIs powers in terms of ascertaining even those enterprises that do not meet the threshold as SSDEs should be further regulated. The vague powers granted to CCI may lead to arbitrariness and biases amongst the CCI which shall prove detrimental to the objective of the proposed Digital Competition Act. Wide and discretionary powers granted should have a rational basis and should keep in place a system of checks and balances. While the executive has been given the power to supersede the CCI in cases where it is unable to discharge its duties, the measures to protect the tech companies in such cases is absent from this regulatory framework.

FinTech

SECTION 2

RBI'S FURTHER REGULATION OF PAYMENT AGGREGATORS

NEWS

In a significant move to refine the regulatory landscape, the Reserve Bank of India ("RBI") has introduced comprehensive revisions to the guidelines governing Payment Aggregators ("PAs"). These revisions are pivotal in addressing the evolving needs of digital transactions and ensuring robust oversight at both online and physical points of sale.

LEGAL TALK

The RBI's revised guidelines clearly define PAs, emphasising their role in facilitating transactions through various payment channels. Under the new definition, PAs are categorised into two types: those facilitating e-commerce transactions ("PA – Online") and those managing face-to-face or proximity payments ("PA – Physical"). This distinction is crucial for applying tailored regulatory measures to different transaction environments.

A significant update involves the management of escrow accounts. The guidelines now mandate that escrow accounts used by PAs must cater to both online and physical sales activities. This includes ensuring that funds related to Delivery versus Payment ("DvP") transactions, which were not previously covered, are now routed through these accounts. This change aims to increase the security and integrity of these transactions.

Moreover, the RBI has enhanced the Know-Your-Customer ("KYC") and ongoing due diligence requirements for PAs. The new guidelines require PAs to conduct rigorous due diligence before onboarding merchants and to monitor their transactions continuously. This involves detailed verification processes, especially for small and medium-sized merchants, to ensure they comply with financial norms and regulations. The intention is to prevent financial fraud and enhance the operational security of digital payments.

THE WAY FORWARD

The updated guidelines signal a shift towards more stringent regulatory practices for payment aggregators. As the digital payments landscape continues to grow, these guidelines will play a crucial role in shaping a secure and reliable environment for both merchants and consumers. For PAs, the immediate focus should be on adapting their operational and compliance frameworks to align with these new requirements. This includes enhancing their technological capabilities to manage escrow accounts effectively and refining their KYC processes to ensure thorough merchant vetting. By prioritising these areas, PAs can meet the stringent requirements set forth by the RBI and enhance their market trust and reliability. This proactive approach will support their long-term success in India's rapidly evolving digital payments landscape.

RBI CIRCULAR REGULATING PHYSICAL POINT OF SALE PAYMENT AGGREGATORS

NEWS

The Reserve Bank of India ("RBI") has issued a draft circular outlining regulatory measures for Payment Aggregators ("PAs") operating within the physical Point of Sale ("PA-P") domain. These measures involve direct regulation and authorization of PAs facilitating face-to-face payment transactions, aligning with the broader objectives articulated in the Payments Vision 2025.

LEGAL TALK

Non-bank entities providing PA-P services must adhere to distinct regulatory procedures covering both authorization requirements and the net worth criterion. They are required to notify the RBI within 60 days to seek authorization for PA-P activities and submit Form A accordingly. Compliance with governance standards, security protocols, and risk management frameworks is crucial for obtaining authorization. Entities planning to start PA activities must obtain explicit approval from the Department of Payment and Settlement Systems (DPSS) at the RBI Central Office before initiating such operations.

The net worth criterion serves as a crucial aspect of this regulatory framework. Existing non-bank PA-P providers must maintain a minimum net worth of ₹15 crore, rising to ₹25 crore by March 31, 2028. Newly established entities should achieve ₹25 crore within the third financial year post-authorization. Failure to comply or submit an authorization application by the specified timeframe mandates the cessation of PA-P activities by July 31, 2025. Banks must close accounts linked to non-compliant non-bank PA-P entities by October 31, 2025, unless proof of authorization application submission to the RBI is provided.

THE WAY FORWARD

The regulatory framework surrounding non-bank entities in the PA-P services sector offers a structured approach aimed at enhancing security, transparency, and financial stability. By mandating stringent authorization processes and setting a significant net worth criterion, regulators seek to instil confidence and accountability within the industry. However, these regulatory measures may inadvertently create barriers to entry for smaller players and stifle innovation. Striking a balance between regulatory compliance and fostering a competitive environment will be critical in ensuring a vibrant and resilient PA-P ecosystem that continues to meet evolving consumer needs while maintaining systemic integrity.

RBI ISSUES DRAFT RULES ON DIGITAL LENDING

NEWS

Recently, the Reserve Bank of India ("**RBI**") issued its Draft Guidelines on 'Digital Lending- Transparency in Aggregation of Loan Products from Multiple Lenders'. The main aim behind issuing these rules is to allow borrowers to make free and better decisions.

LEGAL TALK

The RBI has observed that numerous Loan Service Providers ("LSP") aggregate loan offers from lenders. Under these arrangements, LSPs or Regulated Entities ("RE") acting as LSPs have outsourcing agreements with multiple lenders. Through their Digital Lending App/Platform ("DLA"), these entities match borrowers with suitable lenders. In instances where an LSP has agreements with multiple lenders, the specific identity of the potential lender may remain undisclosed to the borrower until later stages of the process.

The guidelines mandate that LSPs provide a digital overview of all available loan offers to the borrower, tailored to their requirements and sourced from willing lenders with whom LSPs have agreements. This digital overview must include details such as the name(s) of the RE(s) extending the loan offer, loan amount and tenor, Annual Percentage Rate ("APR"), and other key terms and conditions. Additionally, LSPs are required to provide a link to the key facts statement for each RE. Furthermore, LSPs must disclose on their website the mechanism employed to determine lenders' willingness to offer loans. It is imperative that the content displayed by LSPs remain unbiased and devoid of any promotional biases toward specific products or REs. LSPs are prohibited from employing 'dark patterns' in their content presentation, ensuring transparency and fairness in loan offer comparisons for borrowers.

THE WAY FORWARD

The RBI's guidelines target a crucial aspect of digital lending - borrower awareness. By mandating a comprehensive digital overview showcasing all relevant loan options from partnered lenders, borrowers can easily compare loan terms like APR, repayment tenor, and crucial conditions. This empowers informed decision-making. Additionally, requiring links to key fact statements and disclosing the mechanism used to identify suitable lenders fosters transparency. Furthermore, a ban on biassed presentation and "dark patterns" ensures borrowers aren't pressured towards specific lenders or products. The overall effect of the guidelines would be a fairer and more transparent online loan comparison landscape, potentially increasing competition and driving lenders to offer more competitive rates and terms, ultimately benefiting borrowers in India.

RBI RELEASES STATEMENT ON DEVELOPMENT AND REGULATORY POLICIES

NEWS

Recently, the Reserve Bank of India ("**RBI**") released its Statement on Development and Regulatory Policies. The Statement sets out various developmental and regulatory policy measures relating to: Financial Markets, Regulations, and Payment Systems and FinTech.

LEGAL TALK

The RBI through this Statement has proposed enabling Unified Payment Interface ("UPI") facility for depositing cash at ATMs. Currently, the availability of the facility of cash credit is only available through debit cards. With the proposed feature, customers don't need to carry debit cards to deposit cash. It will also reduce the cash-handling burden on banks. Furthermore, the RBI has introduced a proposal to facilitate the linkage of prepaid payment instruments ("PPIs"), such as wallets and prepaid cards, with third-party UPI applications. Presently, UPI payments can be executed through various accounts associated with a user's UPI ID via the UPI application of the bank or any third-party UPI application. However, this capability is not extended to PPIs. Currently, PPIs can only be utilised for UPI transactions through the application provided by the PPI issuer. For instance, funds in a Paytm wallet can solely be utilised via the PayTM application and are not accessible through other applications such as MobiKwik, GPay, or PhonePe. The proposed feature by the RBI aims to enable users to link their PPIs to their UPI accounts on any UPI application of their preference. Consequently, users will be able to utilise their Paytm wallet, for instance, to conduct UPI payments through applications like GPay and PhonePe UPI apps.

The RBI has also proposed enabling non-bank payment system operators like PhonePe and GPay to offer Central Bank Digital Currency ("CBDC") wallets. It is proposed with the objective to make CBDC-Retail accessible to a broader segment of users in a sustained manner. The wider reach can boost financial inclusion and make CBDC a mainstream payment option. Additionally, including these established operators will test the system's ability to handle a larger user base and diverse transactions.

THE WAY FORWARD

This initiative by the RBI is expected to accrue several benefits for customers. Firstly, it will augment the array of options available to users for conducting UPI payments using PPIs, thereby alleviating the reliance solely on the PPI issuer's application for wallet-based UPI payments. Additionally, this initiative presents a compelling value proposition for the proliferation of digital transactions, particularly for small-value payments. Cumulatively, these factors are poised to bolster the utilisation of PPIs and foster the growth of digital payments. Moreover, allowing non-bank operators to offer CBDC wallets could broaden access and make the digital rupee a mainstream payment option. Overall, the proposed changes are expected to significantly boost digital payments in India.

RBI ISSUES REVISED MASTER CIRCULAR – BANK FINANCE TO NON-BANKING FINANCIAL COMPANIES ('NBFC')

NEWS

Recently, the Reserve Bank of India ("**RBI**") issued the Master Circular on Bank Finance to NBFCs. The purpose of issuing this Master Circular as stated by the bank is to lay down RBI's regulatory policy regarding financing of NBFCs by banks.

LEGAL ANGLE

(i) Bank Finance to NBFCs registered with RBI and those not requiring registration

The RBI has removed the ceiling on bank credit linked to Net Owned Fund ("NOF") for all NBFCs registered with RBI, engaged in asset financing, loan, factoring, and investment activities. Additionally, banks can offer finance against second-hand assets financed by NBFCs. For NBFCs not requiring registrations with the RBI, banks may take their credit decisions on the basis of usual factors like purpose of credit, nature and quality of underlying assets etc.

The directions aim to benefit both Banks and NBFCs by scrapping the ceiling on bank funding linked to NOF for registered NBFCs, they get easier access to capital, while banks can now finance pre-owned assets sold by NBFCs.

(ii) Activities not eligible for Bank Credit

Bank credit is not extended to NBFCs for certain activities, including bills discounted or rediscounted by NBFCs, except for bills from commercial vehicles and two or three wheeler sales, subject to specific conditions. Subject to certain exceptions, NBFC investments in any company, including shares and debentures, are ineligible for bank credit. Unsecured loans by NBFCs to any company, loans to their subsidiaries or group companies, and financing to NBFCs for individuals' Initial Public Offerings ("IPOs") subscriptions or share purchases from the secondary market are also excluded from bank credit eligibility.

These restrictions on bank credit to NBFCs are designed to mitigate risks and promote responsible lending practices within the financial system. By limiting credit for certain activities like bill discounting and investments in other companies, regulators aim to prevent excessive exposure to potentially risky assets. These regulations encourage NBFCs to focus on core activities and avoid speculative or high-risk ventures, thus enhancing financial stability. However, while these measures promote prudence, they may also limit access to credit for legitimate business activities, potentially impacting economic growth.

(iii) Bank Finance to Factoring Companies

Banks have the authority to provide financial support to Factoring Companies holding certification under the Factoring Regulation Act, 2011. However, in order to qualify for bank financing, these Factoring Companies must meet specific criteria like the financial assistance they receive must be secured by hypothecation or assignment of receivables in their favour. Moreover, they must derive a minimum of 50 per cent of their income from factoring activities, and the receivables financed by them must constitute half of their assets.

By requiring half of income and assets to be tied to factoring activities, and mandating secured financing with receivables, the RBI ensures these companies operate as intended and mitigates risk for banks. This likely aims to prevent misuse of funds, protect banks, and promote specialisation in the factoring industry.

(iv) Other Prohibitions on Bank Finance to NBFCs

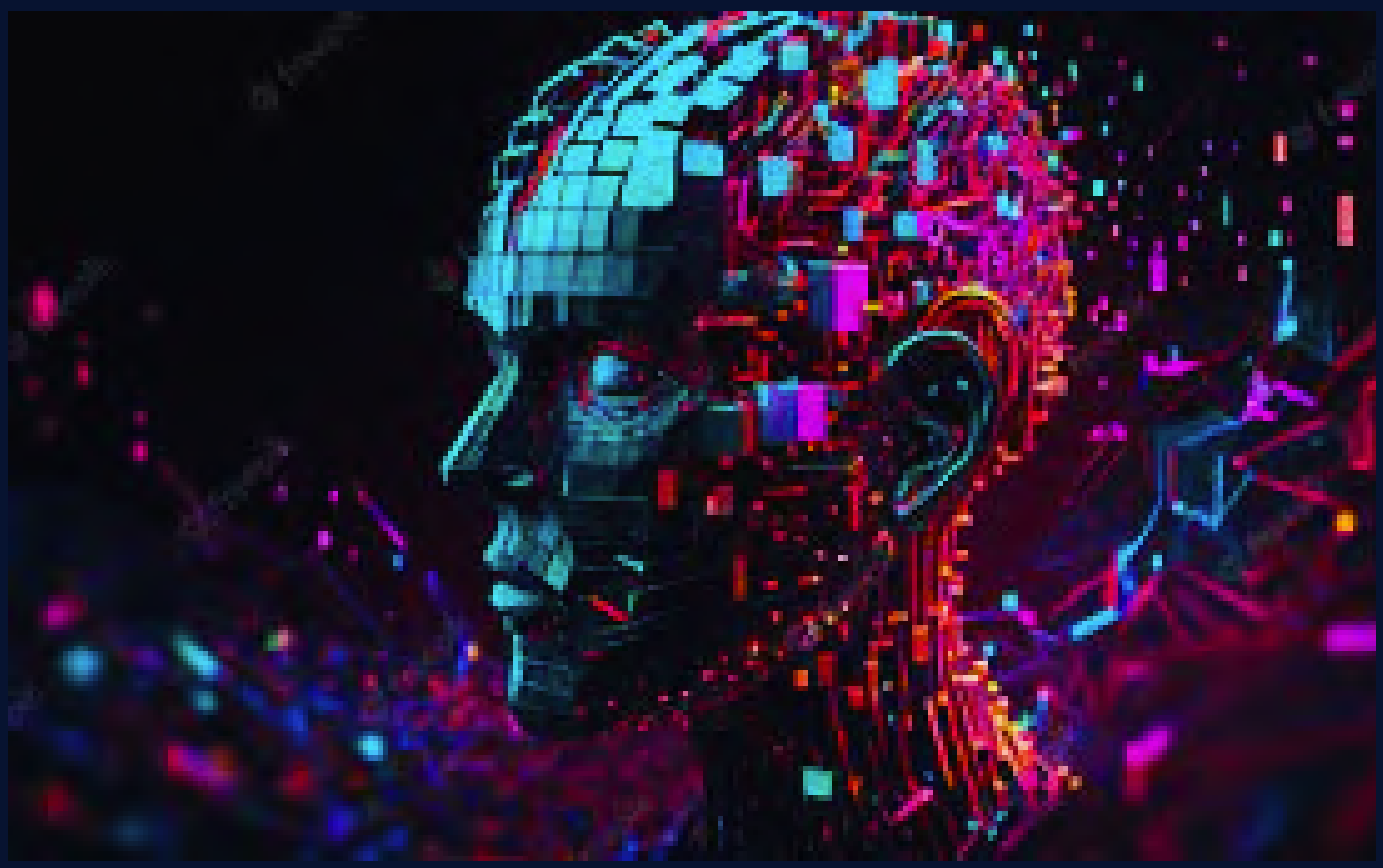
The directions provide that the RBI restricts banks from giving bridge loans or short-term financing to NBFCs intended to cover gaps before raising long-term funds. This applies to various forms of credit, including unsecured loans and bonds. NBFCs must use their own surplus to repay short-term loans, not funds raised externally. Moreover, according to the directions, shares and debentures cannot be accepted as collateral securities for secured loans granted to NBFCs for any purpose.

These provisions are aimed to discourage NBFCs from relying on unstable financial sources. This reduces the likelihood of defaults and enforces healthy borrowing practices.

THE WAY FORWARD

The direction will impact both Banks and NBFCs. Banks gain new lending opportunities and at the same gives NBFCs easier access to capital. However, for NBFCs, while these regulations promote responsible lending practices and mitigate risks within the financial system, they might face constraints in accessing credit for certain activities like bill discounting and investments in other companies. This could potentially impact their ability to engage in diverse business operations and spur economic growth. Therefore, moving forward, there is a need for continued collaboration between regulators and industry stakeholders to strike a balance between risk mitigation and fostering an environment conducive to sustainable financial innovation and growth.

ARTIFICIAL INTELLIGENCE & DATA PRIVACY



SECTION 3

SHURA COUNCIL OF BAHRAIN PROPOSES LAW TO REGULATE AI

NEWS

The Shura Council of Bahrain has unanimously approved a law aimed to regulate the use of artificial intelligence (“AI”) in the country. The law was proposed by Vice Chairman Ali Al Shehabi, along with a coalition of five members from the Human Rights Committee. The drafting of the legislation will be starting soon and it will be presented in the parliament within six months.

THE LEGAL TALK

The proposed legislation seeks to address various forms of AI-related misconduct, such as tampering with biometrics, invasion of privacy, and discrimination. It imposes substantial fines ranging from BD1,000 ($2,653) to BD10,000 ($26,526) for such offences. The purpose of imposing such fines is not only punitive but also preventive and corrective in nature. This legislation, by imposing financial penalties, aims to discourage AI-related misconduct and incentivize compliance with ethical standards and legal requirements. These fines will also serve as a mechanism for accountability, ensuring that those responsible for AI-related offences are held accountable for their actions. This will help in promoting trust and confidence in AI technologies and their responsible use. The legislation takes a firm stance against the use of AI in ways that could lead to societal unrest or political disturbances. It aims to criminalise such activities and imposes imprisonment of no less than three years. This reflects a commitment to safeguard democratic values, including freedom of expression, access to accurate information, and the integrity of electoral processes. AI technologies, if misused, can amplify disinformation, polarise communities, and erode trust in institutions. By targeting these risks through legal measures, the legislation aims to protect the democratic fabric of society.

The proposed law extends liability to establishments whose resources are employed in AI-related criminal activities. This measure recognizes the potential for organisations to be complicit in or facilitate AI-related offences. This measure aims to encourage organisations to proactively implement measures to prevent AI misuse and serves as a deterrent against negligence or complicity in AI-related offences. Penalties for such organisations can also include permanent closure, underscoring the severity of the consequences for non-compliance. This Penalty sends a strong message that organisations must take AI ethics and compliance seriously, as the stakes for non-compliance can be severe and potentially result in the cessation of business operations. Furthermore, a dedicated AI unit is also established to enforce compliance, which is a significant step towards ensuring effective implementation and oversight of the new regulations. The presence of a specialised unit demonstrates a commitment to addressing AI-related challenges comprehensively and with expertise. It will also enhance coordination among regulatory bodies, law enforcement agencies, and technical experts in addressing emerging AI risks

Bahrain's approach to regulating AI through criminal sanctions and penalties is a unique contrast to the approaches taken by other jurisdictions, such as the European Union and China, which largely focus on ex-ante risk management and quality management requirements. While criminal sanctions can serve as a deterrent and ensure accountability, it is essential to strike a balance between promoting innovation and mitigating potential risks associated with AI.

WAY FORWARD

The success of Bahrain's AI regulation will depend on its effective implementation, consistent enforcement, and continuous adaptation to the rapidly evolving AI landscape. It will be crucial to monitor the practical implications of this legislation and its impact on fostering responsible AI development and deployment within the country. The effective implementation of this AI regulation will pave the way for future AI regulations to follow.

BRITISH GOVERNMENT PROPOSES TO CRIMINALISE THE CREATION OF SEXUALLY EXPLICIT DEEP FAKE IMAGES

NEWS

The British government has proposed an amendment to the Criminal Justice Bill which seeks to address the creation of sexually explicit deepfake images. This law targets the creation of such images without consent in England and Wales. Under this law, individuals who create sexually explicit deepfake images of adults will face criminal charges.

THE LEGAL TALK

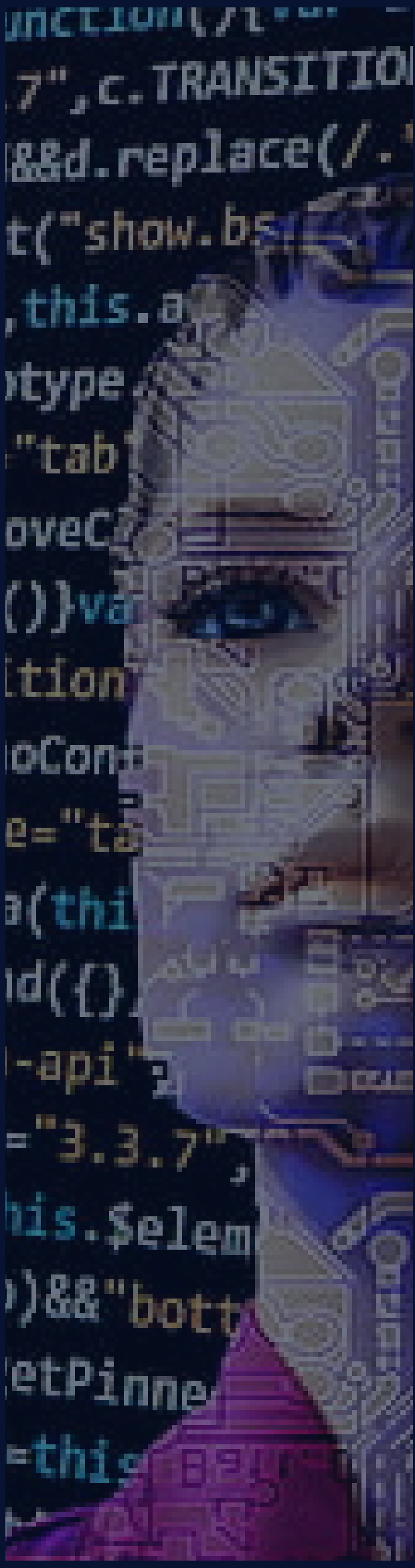
The proposed amendment to the Criminal Justice Bill in England and Wales represents a significant step in addressing the growing concerns surrounding non-consensual deep fake pornography. The amendment by criminalizing the creation of sexually explicit deep fake images of adults without their consent, even if the creator has no intention of sharing the content, the law recognizes the inherent harm and distress caused by such actions. This legislation acknowledges that the mere act of creating non-consensual deepfake pornography is a violation of an individual's privacy and autonomy, regardless of whether the content is ultimately disseminated. This stance shifts the focus from the creator's intent to the impact on the victim. It acknowledges that the harmful consequences of non-consensual deepfake pornography are not mitigated by the creator's motives or lack of intent to share the content publicly. This aligns with principles of victim-centred justice and places emphasis on the protection of individual rights. It also recognizes that stopping the creation of harmful content at the source is crucial in safeguarding individuals' rights and reducing the potential for harm escalation through dissemination.

However, this amendment alone may not suffice to address the complexities of deepfake technology and its potential harms. Education and awareness campaigns about deepfakes, digital literacy, and consent are essential in empowering individuals to protect themselves and recognize manipulated content. Collaborative efforts involving governments, tech companies, civil society organisations, and educators can enhance public understanding of deepfake risks and preventive measures.

The amendment also seeks to impose severe penalties, including criminal records, unlimited fines, and potential imprisonment for sharing the content which underscores the gravity of the offence and serves as a deterrent against such exploitative behaviours. Criminal records have a long-term impact on individuals' reputations and legal status, which can also lead to consequences like problems in finding employment opportunities, impact upon social standing and on personal well-being which will serve as a strong deterrent against engaging in such activities. Unlimited penalties are also intended to impose a significant financial burden on offenders and discourage such behaviour.

While the primary focus of the amendment is on protecting adults, it also can include similar offences involving children, highlighting the overarching commitment to safeguarding individuals from digital exploitation across all age groups. By emphasising the importance of malicious intent in creating deepfake images, the law aims to target those who seek to cause harm, humiliation, or distress to their victims, rather than unintentional or inadvertent actions.

Compared with other jurisdictions the European Commission has taken a proactive stance by introducing a directive aimed at criminalising the non-consensual sharing of intimate images online, including AI deepfake pornography, and addressing gender-based online harassment. This directive, if passed, would require all EU member states to enact domestic laws aligning with the outlined guidelines, fostering a unified approach to tackling digital exploitation and abuse across the region. In the United States, the proposed Disrupt Explicit Forged Images and Non-Consensual Edits Act (“**DEFIANCE**”) aims to establish a federal civil remedy for victims of digital forgeries, including deepfake pornography. This act seeks to provide legal recourse and support for those impacted by this form of exploitation, acknowledging the harm caused by such activities.



WAY FORWARD

This amendment represents a proactive step by the UK government to address the evolving challenges posed by deepfake technology and its potential misuse. By establishing clear legal boundaries and consequences, the law sends a strong message that the non-consensual creation and distribution of deepfake pornography will not be tolerated, and offenders will be held accountable for their actions. However, the effectiveness of these laws will depend on their consistent enforcement, public awareness campaigns, and the development of technological measures to detect and prevent the spread of deepfake content. Additionally, international cooperation and harmonisation of laws may be necessary to address the global nature of this issue and ensure comprehensive protection for individuals worldwide.

NEEL SAMIR SHUKLA V. UOI: THE RIGHT TO NOT TO SUBMIT TO AUTOMATED DECISION

NEWS

In the case of Neel Samir Shukla v. UOI, Shukla's Google account including Google Pay, Gmail, Google Docs etc. had been blocked due to possessing explicit content related to potential child sexual abuse or exploitation, purportedly stemming from the uploaded photo in which her grandmother was making him bath when he was 2 years old. This happened because of Google's AI-based Child Sexual Abuse Material ("CSAM") detector decided to block Shukla's account without human intervention.

THE LEGAL TALK

The primary purpose of Google's CSAM detector is to identify and remove illegal and harmful content from its platforms, such as Google Drive, Gmail, and Google Photos. By using AI algorithms, the system can detect CSAM materials more efficiently than manual human review alone. The detector has the ability to remove data directly without any human review. This removal of data solely by AI has become a contentious issue in the current scenario. Under the General Data Protection Regulation (**"GDPR"**) Article 22(1) clearly states that "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

This right serves as a vital safeguard against potential injustices, discrimination, and violations of individual autonomy. It underscores the need for human oversight, accountability, and transparency in decision-making processes that can have far-reaching consequences on people's lives, such as employment opportunities, financial assessments, access to services, or legal proceedings. By preserving this right, data protection regulations aim to uphold fairness, protect against algorithmic biases, and maintain trust between individuals and the entities that process their data, thereby promoting ethical use of technology and safeguarding fundamental rights in the digital age.

In the Indian Jurisprudence, under Digital Personal Data Protection Act, 2023 (“DPDPA”) there is no mention of the right to not to submit to automated decision making. The case of Neel Samir Shukla brings to the forefront the need for regulations that specifically address the challenges posed by AI-driven decision-making processes and the importance of accountability and transparency in data removal practices. This protects the rights of individuals to have human oversight and intervention in decisions that significantly affect them and also reduces the possibility of algorithmic bias and discrimination, ensuring that decisions are fair, unbiased, and based on relevant and accurate data. This further fosters trust and confidence in digital systems and technologies, enhancing public perception and acceptance of AI-driven processes.

WAY FORWARD

It is imperative at this for the legislature to address the absence of regulations regarding the right not to be subject to automated decision-making. The case of Neel Samir Shukla underscores the urgency of implementing specific provisions within the Digital Personal Data Protection Act, 2023 (DPDPA) that safeguard against potential injustices and algorithmic biases resulting from AI-driven decision-making processes. This can be achieved by drafting and incorporating guidelines or amendments that mandate human oversight and intervention in decisions with significant impacts on individuals. Additionally, establishing transparent accountability mechanisms, conducting regular audits, and promoting ethical AI frameworks will be essential in fostering public trust, ensuring fairness, and upholding fundamental rights in the digital age. Collaborating with international experts and adopting best practices from global data protection standards like GDPR can also guide India's efforts towards responsible and ethical use of AI technologies.

WHATSAPP MOVES TO DELHI HIGH COURT AGAINST IT RULES

NEWS

WhatsApp and its parent company Meta have moved to the Delhi High Court challenging the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021 [“IT Rules 2021”]. These rules require social media intermediaries to trace chats and make provisions to identify the first originator of information when required.

THE LEGAL TALK

WhatsApp argued that this requirement under the rules was against the user’s right to privacy. As the Meta-owned messaging service has end-to-end encryption [“E2EE”] and lifting the same for legal reasons is challenging for the company which could result in changing the user terms and privacy policies that customers depend on. Rule 4(2) of the IT Rules 2021 mandates significant social media intermediaries to facilitate the identification of the first originator of information upon judicial order. This is for legal purposes including prevention and instigation of offences against security, sexual abuse, etc. but it must be done using the least intrusive methods and without disclosing message contents or other users’ information. This places a significant burden on intermediaries and raises privacy concerns. Despite safeguards, security experts warn that implementing these rules could jeopardise E2EE norms, as platforms would need to identify all users, not just offenders. This breaks the privacy protection E2EE provides, which ensures only the sender and receiver can access messages. Additionally, in legal cases using platform messages as evidence, WhatsApp may lose intermediary protection defence. Courts may hold WhatsApp and its executives liable under Section 85 of the Information Technology Act 2000 [“IT Act”] for contributory negligence and vicarious liability. Due to excessive vagueness in the rules about when the liability can fall on these intermediaries, there is a possibility of over-compliance by social media companies to escape liability. The collateral damage here is citizens' free speech and privacy. The government claims authority under Section 87 of the IT Act to enact Rule 4(2) to combat fake news and content threatening national security or communal harmony. It argues that platforms monetizing users' data for business purposes are not legally entitled to claim they protect privacy. WhatsApp's contention in this case rests on the assumption that the only means to trace the originator of messages is by breaking E2EE. However, it's pivotal to emphasise that the government's rule doesn't explicitly mandate E2EE breach. Rather, it necessitates platforms to provide originator details through any available means or mechanism, taking into account their widespread prevalence and larger public duty. They have complete freedom to develop a mechanism that balances the user’s right to privacy while also meeting the compliance requirement.

THE WAY FORWARD

Legal authorities and law enforcement bodies worldwide have advocated for breaking E2EE to trace the origin of crimes such as violent deepfakes, child abuse media, and fake news. However, breaching E2EE means *everyone's* privacy is compromised; a direct contradiction to Rule 4(2). Previous proposals to implement traceability compatible with E2EE have shown vulnerability to spoofing, potentially leading to the framing of innocent individuals. The government must understand that maintaining law and order includes protecting citizens' fundamental rights. Forcefully breaking encryption is against democratic principles. Indeed, while the government could request social media intermediaries to devise a model that maintains E2EE integrity while meeting compliance requirements, such an endeavour would demand significant time, research, and resources. However, until such a solution is developed, it's imperative to explore alternative approaches to prevent harm. Simply tracing the message origin and imposing punishment isn't always effective and suggests the government is ready to take any action it deems necessary without exploring alternatives. Implementing safeguards to halt harmful message circulation and banning users who disseminate such content could be considered instead. Ultimately, finding a middle ground where both privacy and security are respected is essential for the well-being of society.

CONTRIBUTORS

DESIGNERS

SAMRIDHI BAJORIA

TRISHNA AGRAWALLA

WRITERS

LAVANYA CHETWANI

ANJALI PANDE

TRISHNA AGRAWALLA

SAGUN MODI

NAMAN OTSWAL

EDITORS

NIKHIL JAVALI

HARSH MITTAL

SAGUN MODI

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL