LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

MAY 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

EXCLUSION OF OTT FROM THE NATIONAL BROADCASTING POLICY 2024

NEWS

The Telecom Regulatory Authority of India (“**TRAI**”) has released a consultation paper for the National Broadcasting Policy (“**NBP**”). The paper calls for inputs on the formulation of the policy and one such suggestion it requires is the growth of regional content through Over-The-Top (“**OTT**”) platforms.

LEGAL TALK

One of the policy’s aims is to promote Indian content by utilising OTT platforms, while also supporting Indian OTT platforms. The ministry aims to increase the growth of regional content viewers in India and abroad, similar to the European Union’s requirement of featuring at least 30% of European works on OTT platforms in Europe. The primary concern is that including OTT platforms within the NBP could lead to confusion, as these platforms are already regulated under Part III of the Information Technology Rules (Intermediary Guidelines and Digital Ethics Code) (“**IT Rules**”). While inclusion shall ensure the security and growth of Indian platforms and regional content, it shall create overlapping difficulties between the Ministry of Electronics and Information Technology and TRAI. By including OTT platforms, TRAI has failed to differentiate between *streaming* and *broadcasting* services. While broadcasting “pushes” certain fixed content onto its viewers, streaming services allow individual viewers to “pull” a piece of content of their choice by deciding what they view. Further, in the case of *All India Digital Cable Federation vs. Star India Pvt Ltd*, the Tribunal held that an OTT platform is not a TV channel and is not under the TRAI’s jurisdiction. The contention revolved around Star India streaming ICC Cricket World Cup matches for free on mobile devices through its OTT platform Disney Hotstar, while the same matches were only accessible on the Star Sports TV channel via paid subscriptions.

THE WAY FORWARD

Excluding OTT platforms from TRAI's policy prevents overlap with IT Rules, which already regulate these platforms. Alternatively, including OTT platforms ensures content parity, as technological advancements have allowed the same content to be delivered via OTT and DTH providers This creates a level playing field for the DTH providers who are seeing a decline in viewership due to preference of OTT platforms. Two mediums that are delivering the same content are being regulated differently. However, it is preferable to keep OTT platforms outside TRAI's jurisdiction and instead, make amends to the IT Rules to ensure content parity. If TRAI regulates regional content on OTT platforms instead of the designated ministry, it would indirectly cause confusion and chaos.

DIGITAL MARKETS, COMPETITION & CONSUMERS BILL: UK'S EX-ANTE FRAMEWORK

NEWS

The UK Parliament has passed the Digital Markets, Competition and Consumer ("**DMCC**") Bill which is expected to come into force later this year. This regime is an addition to the ex-ante regulation of digital markets globally. It covers important changes to digital markets, consumer law, merger control, and antitrust rules.

LEGAL TALK

It will give the Competition & Markets Authority ("**CMA**") the power to impose tailored conduct requirements on firms and label them as having a Strategic Market Status ("**SMS**"). The CMA's Digital Markets Unit ("**DMU**") will be handed power to designate firms as having SMS if they have *substantial and entrenched market power* and *a position of strategic significance* in relation to digital activities linked to the UK. The DMU will create tailored codes of conduct for each SMS firm, focusing on designated activities and based on principles of fair trading, open choices, and transparency. The Indian Digital Competition Bill ("**the Bill**") follows the UK's DMCC in contemplating company-specific prohibitions, as opposed to industry-wide generally applicable rules. This gives regulators more discretion to craft individualised conduct codes for each company but raises issues yet again it intended to avoid. The Bill anticipates extensive noncompliance inquiries, leading to high administrative costs from discovery, fact-finding, and adversarial proceedings. Moreover, this approach raises concerns about unequal treatment and favouritism towards established players over new entrants. Instead of addressing market failures, the Indian Bill risks increasing administrative costs and creating digital winners and losers. The UK's DMCC applies only to tech firms with substantial *market power*, ensuring the law targets major players rather than all digital firms. In contrast, the Indian Bill relies on quantitative criteria, such as user numbers and financial thresholds, to determine applicability. By focusing on market power, the UK approach avoids overregulation of smaller firms, thereby fostering innovation among small and medium-sized firms. This distinction ensures that regulatory efforts are concentrated on entities with significant influence, encouraging a more dynamic and competitive digital marketplace.

THE WAY FORWARD

Looking ahead, the key challenge for India will be to strike a balance between regulation and innovation. While the Indian Bill's focus on user and financial thresholds aims to capture significant market players, it must ensure that it does not hamper the growth of smaller firms. Adopting a similar system to the UK's DMCC, which considers the market power of tech firms could help mitigate the risks of regulatory capture and ensure fair competition. By refining its approach, India can ensure a competitive digital market that encourages innovation while safeguarding consumer interests.

FinTech

SECTION 2

RBI ISSUES REVISED GUIDANCE NOTE ON OPERATIONAL RISK MANAGEMENT AND OPERATIONAL RESILIENCE

NEWS

The Reserve Bank of India ("**RBI**") released an updated Guidance Note on Operational Risk Management and Operational Resilience on April 30, 2024 ("**Guidance Note 2024**"), superseding the previous guidance issued in 2005 ("**Guidance Note 2005**"). This revision addresses the significant advancements and emerging risks in the financial sector, particularly for FinTech companies.

LEGAL TALK

The Guidance Note 2024 expands the scope and complexity of operational risk management to include contemporary threats such as cyber-attacks, technological changes, geopolitical conflicts, and natural disasters. It emphasises the need for robust governance, a strong risk culture, and comprehensive risk management policies. The Guidance Note 2024 includes several key updates.

The definition of operational risk has been expanded to cover modern threats like cyber risks, technological disruptions, and third-party dependencies. The RBI highlights the necessity for regulated entities ("**REs**") to manage a broad range of risks, including those arising from external and internal frauds, and operational disruptions due to natural causes. Additionally, the updated note places a stronger emphasis on the role of the Board of Directors and senior management in fostering a risk-aware culture, advocating for continuous training and clear accountability across all organisational levels.

A detailed operational resilience framework is introduced to ensure the continuity of critical operations during disruptions. This framework provides guidelines for incident management, business continuity planning, and the management of third-party dependencies. The three lines of the defence model are reinforced, outlining clear roles and responsibilities for business unit management, independent risk management functions, and internal audit.

Furthermore, the guidance adopts a principle-based and proportionate approach, offering flexibility for REs of various sizes and complexities to implement the guidelines effectively.

Comparison with the Guidance Note 2005

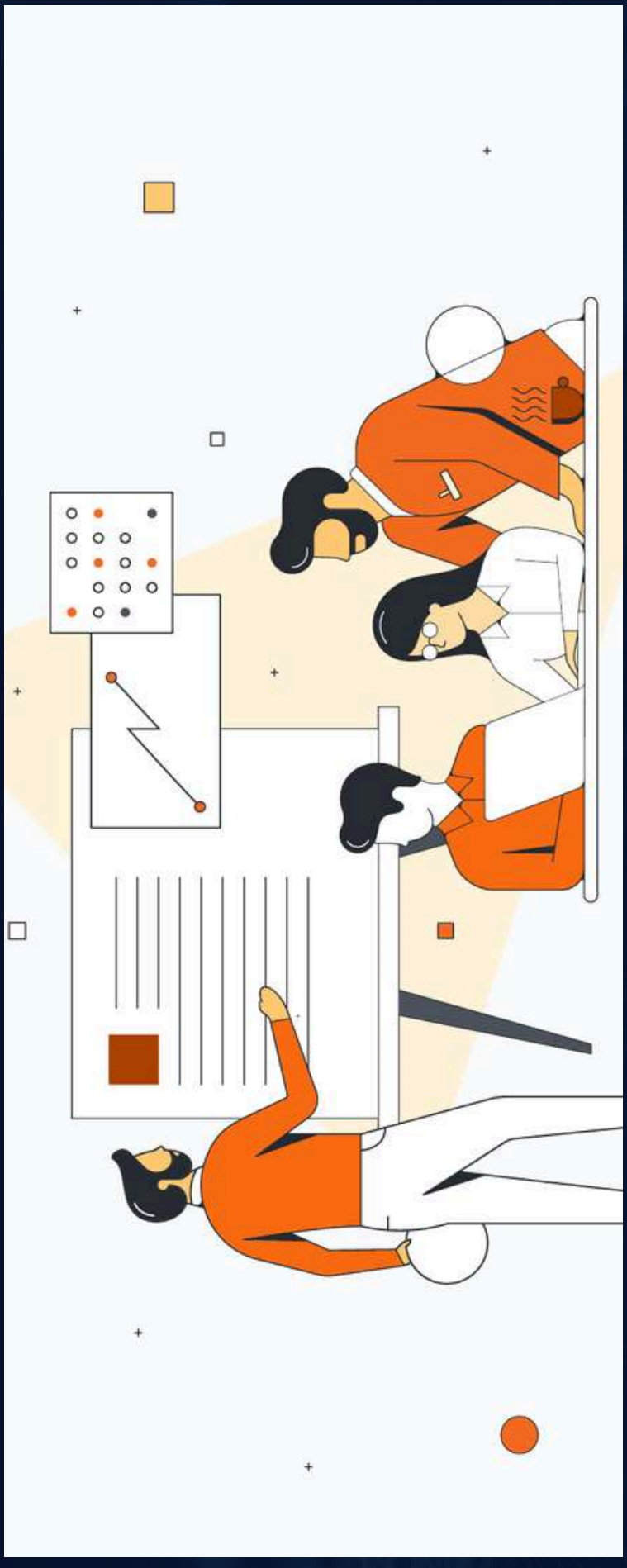
- **Scope and Complexity:**
  - *2024*: Addresses increased complexity including technological advancements and third-party services, recognizing modern financial operations' dynamic and interconnected nature.
  - *2005*: Focused on basic operational risk management without extensive consideration of technological advancements and third-party services.

- **Governance and Culture:**
  - *2024*: Requires active involvement from the Board and senior management in risk management processes, emphasising the creation of a strong risk culture and adherence to ethical business practices.
  - *2005*: Provided limited guidance on the involvement of the Board and senior management and placed less emphasis on cultivating a risk-aware culture.

- **Technology and Cyber Risk:**
  - *2024*: Introduces specific measures for managing IT risks and ensuring cyber resilience, acknowledging the critical role of technology in financial services.
  - *2005*: Contained limited provisions for addressing technology-related risks, reflecting the lesser reliance on digital systems at the time.

- **Third-Party Dependencies:**
  - *2024*: Provides comprehensive policies for managing third-party dependencies, crucial for maintaining operational continuity in an environment with significant outsourcing.
  - *2005*: Lacked detailed guidance on third-party risk management, as outsourcing and third-party dependencies were less prevalent.

The Guidance Note 2024 significantly expands upon the scope and complexity addressed in the 2005 version. The Guidance Note 2024 considers the increased complexity of the financial sector, including technological advancements and third-party services, and provides more detailed and specific guidelines for managing various types of operational risks and ensuring resilience. In terms of governance and culture, the updated note requires active involvement from the Board and senior management. In response to technological advancements and rising cyber threats, it includes specific measures for IT risk management and cyber resilience, areas with limited coverage in the 2005 note. Additionally, it includes comprehensive policies for managing third-party dependencies, which have become more critical with the growing reliance on outsourced services, an aspect not extensively covered in the Guidance Note 2005.



THE WAY FORWARD

The updated Guidance Note is particularly relevant for FinTech companies due to their heavy reliance on technology and third-party services. FinTech companies need to strengthen their IT and cybersecurity measures by implementing robust IT governance frameworks and continuously monitoring and managing cyber risks. Additionally, managing third-party dependencies is crucial; this involves conducting detailed due diligence, continuous monitoring, and contingency planning for third-party service providers to ensure operational resilience. Furthermore, enhancing governance and risk culture is vital. Boards and senior management should be actively engaged in risk management practices and foster a culture of risk awareness and ethical behaviour across the organisation. By adhering to these updated guidelines, FinTech companies can enhance their operational resilience and overall risk management capabilities, ensuring a secure and stable operational framework.

NPCI ISSUES GUIDELINES FOR MERCHANT ACQUISITION ON BHIM AADHAR PAY

NEWS

Recently, the National Payments Corporation of India ("**NPCI**") issued guidelines that put the responsibilities and accountabilities of verifying merchant details on acquiring banks for BHIM Aadhar Pay.

LEGAL TALK

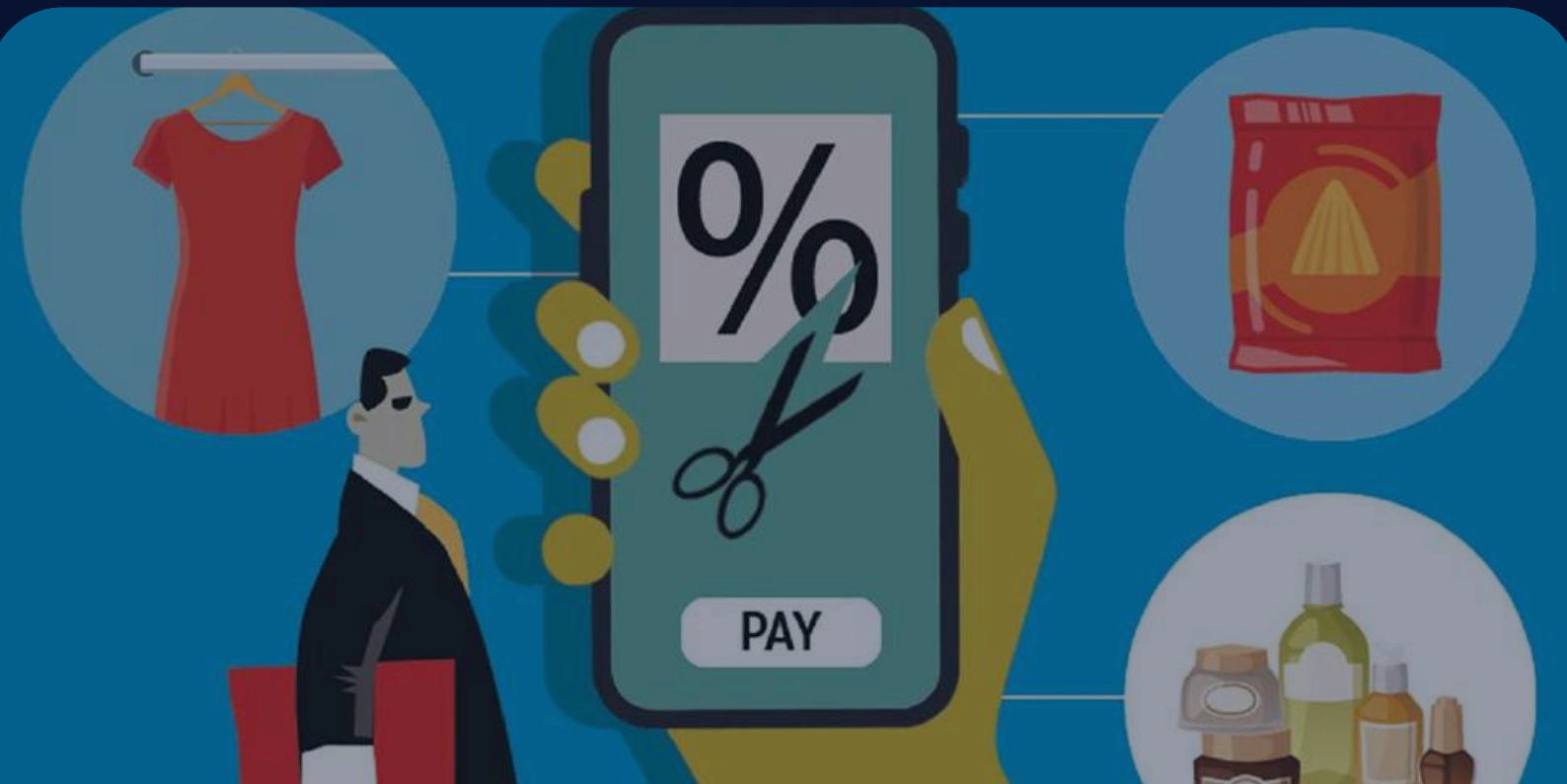
BHIM Aadhar Pay is a platform that enables Merchants to receive digital payments from customers through Aadhar Authentication. Acquiring Member Banks should address the following:

(i) Board-Approved Policy for Merchant Acquisition

According to the guidelines, the Merchant Acquisition policy of an Acquiring Member Bank should be approved by the Board of Directors and should also include standards in order to mitigate financial or reputational risks. By requiring a board-approved policy for merchant acquisition, NPCI ensures that banks establish formalised standards and procedures endorsed at the highest level, fostering consistency and transparency in merchant management practices.

(ii) Agreements with Various Stakeholders

The guidelines provide that merchant agreements should be entered with each merchant/aggregator before any service is provided by them. Agreements should also be placed with third-party service providers in case any of the activities pertaining to the merchant portfolio is outsourced. These agreements must also be reviewed periodically. Such clear agreements have the potential to help mitigate disputes, clarify liabilities, and ensure compliance with regulatory requirements.



(iii) Merchant Underwriting

Acquiring banks are advised to assign Merchant Category Codes based on business type, evaluate new merchants' financial risk exposure (e.g., sales volume, dispute history, delivery method), and ensure compliance with relevant data security standards. Merchants should be categorised into Critical, High, Medium, or Low-risk tiers for periodic due diligence. Certain merchant categories must be prohibited, including those banned under Central or State laws, those posing high brand risk, and those dealing in unregulated financial products/services. The guideline on merchant underwriting underscores the necessity of robust risk assessment methodologies to categorise merchants based on their risk profiles, enabling tailored due diligence measures and risk mitigation strategies.

(iv) Merchant Portfolio and Risk Management

The NPCI suggests the use of predetermined merchant sales volume and transaction amount parameters for risk monitoring processes. Acquiring banks must monitor fluctuations in merchant volumes, and incidences of fraud in relation to sales, chargebacks, reversals, and refunds. Utilising web crawler scan services is advised to identify any discrepancies between the offered products/services and the merchant's transaction history. Furthermore, Acquiring Member Banks are obligated to investigate any suspicious transactions and take appropriate action upon uncovering fraudulent activities. This highlights the proactive approach required to detect and mitigate emerging risks in real time.

(v) Merchant Training

The guidelines recommend Acquiring Member Banks to create ongoing training modules with Merchants on the acceptance methods and guidelines and the training should be conducted physically or virtually with adequate information in line with the policy of the Acquiring Member Bank. This recommendation underscores the significance of continuous training and rigorous oversight in maintaining the security and integrity of the payment ecosystem.

(vi) Third-Party Agent Oversight and Governance

According to the guidelines, a periodic review/audit of the third parties engaged by the Merchant shall be conducted and an Acquiring Member Bank will be responsible for all security system-related activities by the Merchant to any third party.

THE WAY FORWARD

The primary objective of these measures is to foster a secure and efficient BHIM Aadhaar Pay ecosystem, safeguarding against potential risks and ensuring compliance with regulatory requirements. Adequate merchant training and diligent oversight over third-party agents are imperative to ensure adherence to guidelines and mitigate operational risks. By adhering to these guidelines conscientiously, banks can not only mitigate operational risks but also contribute to the smooth functioning of the digital payment system, ultimately benefiting merchants and customers alike.

RBI FRAMEWORK FOR SROS IN THE FINTECH SECTOR

NEWS

To enhance the regulatory framework for the FinTech sector, the Reserve Bank of India ("**RBI**") has introduced a comprehensive framework for Self-Regulatory Organisations ("**SROs**"). This move aims to provide a judicious balance between maximising the creative potential of FinTechs while minimising the risk they pose to the financial system such as customer protection, data privacy, cyber security, grievance handling, etc.

LEGAL TALK

The RBI's framework delineates the roles and responsibilities of SROs in the FinTech sector, emphasizing their function in ensuring adherence to regulatory norms and best practices. SROs are expected to establish a robust governance structure, comprising a well-defined constitution, a code of conduct, and a set of standards to which their members must adhere. The finalised framework has been released following the stakeholder comments received on the draft framework released on 15 January 2024. Key changes in the framework include:

- The RBI has provided some clarity over the general requirements required by an applicant to be registered as a member. In addition to the requirement that the applicant should be a Section 8 company, the framework has also mandated that the shareholding of the SRO should be sufficiently diversified and no entity should hold 10% or more of its paid-up share capital, either singly or acting in concert. Further RBO has also specified the minimum net worth of Rupees two crore within a period of one year after recognition as an SRO-FT by the RBI. Moreover, RBI in the new framework has also defined 'user ham' instances as those which may include fraud, mis-selling, unfair practices, unauthorised transactions, or any other form of misconduct that harm consumers of financial services.
- The mandate for diversified shareholding aims to prevent any single entity from exerting undue influence over the SRO's operations, thereby promoting impartiality and accountability. Additionally, the stipulation of a minimum net worth ensures that SROs possess the financial stability necessary to effectively fulfil their regulatory responsibilities. These changes are ultimately aimed to uphold market integrity and customer interests.

- Under the standard-setting part, RBI has added that apart from framing standard documents for FinTech sector-specific requirements, they should also encourage members to use these documents as a baseline and adapt them to their specific needs, recording reasons and deviation thereof. Additionally, RBI has mandated that the data collected and the standard practices developed must comply with applicable rules and regulations. These changes reflect RBI's efforts to ensure transparency, accountability, standardization, and compliance within the sector.
- For oversight and enforcement, RBI has included a few additional requirements such as the mandate for SRO-FTs to ensure stringent confidentiality of surveillance data and restrict data collection to essential information disclosed to the FinTechs for the specified purposes. Furthermore, the SRO-FT should implement data collection procedures from member FinTechs that safeguard proprietary information while effectively fulfilling broader functions outlined in this framework. By stipulating procedures that safeguard data while enabling the fulfilment of broader regulatory functions, the RBI aims to instill trust among FinTech firms and consumers alike, fostering a conducive environment for innovation and market growth. These changes also portray RBI's efforts to ensure data protection and ethical use of consumer data.
- Moreover, under the guidelines for governance and management, RBI has added that the SRO-FT must uphold impeccable governance standards, ensuring impartiality in decision-making. Its Articles of Association or Bylaws should explicitly emphasize the need for functional autonomy and impartiality to prevent external influence. Besides the requirement of one-third of members of the Board, including the chairperson to be independent, RBI has clarified that the majority of non-independent directors are to be representative of FinTechs that are currently not directly regulated.
- By emphasizing strict governance standards and the need for functional autonomy and impartiality, the RBI aims to mitigate the risks of external influence, and ensure fair decision-making processes and it also reflects RBI's commitment to inclusive representation and diversity of perspectives.

THE WAY FORWARD

The RBI's SRO framework is a critical move towards a self-regulating FinTech ecosystem in India. By following these guidelines, FinTech companies can enhance regulatory compliance, operational integrity, and market trust, supporting long-term growth and sustainability in India's dynamic FinTech environment.

ARTIFICIAL INTELLIGENCE

SECTION 3

ECI RELEASES GUIDELINES FOR THE RESPONSIBLE USE OF AI DURING ELECTIONS

NEWS

From AI-generated video of Narendra Modi dancing to Aamir Khan's public criticism of the Prime Minister, the use of AI and deepfakes has surged in the context of the 2024 Lok Sabha Election. In response, the Election Commission of India **("ECI")** has issued guidelines to ensure the responsible and ethical use of social media platforms, including AI and Deepfakes.

THE LEGAL TALK

The ECI's directive comes in response to the increasing concerns over the misuse of social media for spreading misinformation, manipulated content, and deepfakes, which have the potential to sway voter opinions and erode trust in the electoral process. The ECI guidelines bring to the notice of political parties, their representatives, and star campaigners, that the use of deep fakes and AI-generated distorted content that spreads false information, misinformation, disinformation and factual distortions can lead to their liability under different statutes. The ECI has also specifically stated to not allow their respective social media handles to publish and circulate deepfake audios/videos which violate the provisions of extant rules and regulations. In the case, such deep fake audios/videos, come to the notice of political parties, they shall immediately take down the post but a maximum within a period of 3 hours and also identify and warn the responsible person within the party.

ACTS UNDER WHICH LIABILITY CAN BE IMPOSED

(i) Information Technology Act, 2000:
Section 66C of the Act punishes individuals who fraudulently or dishonestly use electronic signatures, passwords, or unique identification features of others. Section 66D of the act punishes individuals who use communication devices or computer resources with malicious intent to cheat or impersonate. Further, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 provides a framework for addressing unlawful information and fake user accounts on social media platforms.

(ii) Representation of the People Act, 1951:
Section 123(4) of the Act states that the publication of a false statement or a statement he does not believe to be true about a candidate's character, conduct or candidature which can prejudice the prospects of their election, will be considered as a corrupt practice.

(iii) Indian Penal Code, 1860 (“IPC”):

Section 171G of IPC punishes any person who makes a statement that is false or a statement that he does not believe to be true about a candidate's character or conduct. Section 465 and Section 469 talks about forgery and forgery with intent to harm reputation. Section 505 gives liability to any person who makes, publishes or circulates any statement, rumour or report which promotes enmity or ill-will between classes.

(iv) Model Code of Conduct:

Paragraph I(2) of the Model Code of Conduct provides that parties and candidates should refrain from criticism of private lives that are unrelated to public activities and should also refrain from making unverified allegations or distortions against other parties or their members.

While the guidelines issued by the ECI were a much-needed step, they fall short of providing a comprehensive and stringent framework to effectively tackle the rampant misuse of these advanced technologies during elections. The guidelines do not impose an outright prohibition on the use of AI and deepfakes, nor do they prescribe specific penalties or strict actions that the ECI can take against offenders. This lenient approach raises concerns about the efficacy of the measures in curbing the potential dangers posed by the reckless use of such technologies.

Moreover, while the guidelines instruct political parties to remove any deepfake content created by their own members within three hours, this directive lacks deterrence. The imposition of more stringent punitive measures, such as fines or temporary bans on campaigning activities, could have served as a stronger deterrent against the misuse of these technologies. We can take the example of the Cambridge Analytica scandal which involved the misuse of personal data obtained from millions of Facebook users without their consent. This data was then used to create targeted political advertising campaigns and psychological profiling to influence voter behaviour during elections. In the context of deepfakes and AI manipulation, similar tactics could be employed to create highly convincing and entirely fabricated media content, such as fake videos, images, or audio recordings of political figures and candidates. These deepfakes could be used to spread misinformation, smear campaigns, or even influence public opinion on specific issues.

THE WAY FORWARD

The ability of AI and deepfake technologies to manipulate and distort information can mould the views and opinions of voters, potentially persuading them to make decisions that could have far-reaching consequences for the next five years. Furthermore, the absence of strict penal provisions specifically tailored to address the proliferation of deepfakes remains a significant concern. The existing legal framework, although encompassing various acts and provisions, may not be adequate to effectively combat the rapidly evolving nature and sophistication of deepfake technologies.

To safeguard the integrity of the electoral process and uphold the principles of a truly democratic society, it is imperative that the ECI revisits these guidelines and considers implementing a more robust and comprehensive regulatory framework. This framework should not only impose stricter penalties but also address the technical and legal challenges posed by the misuse of AI and deepfake technologies, ensuring that the democratic rights of citizens are protected and the sanctity of the electoral process is preserved.

DELHI HIGH COURT RESTRICTS AI CHATBOT FOR PERSONALITY RIGHTS VIOLATION

NEWS

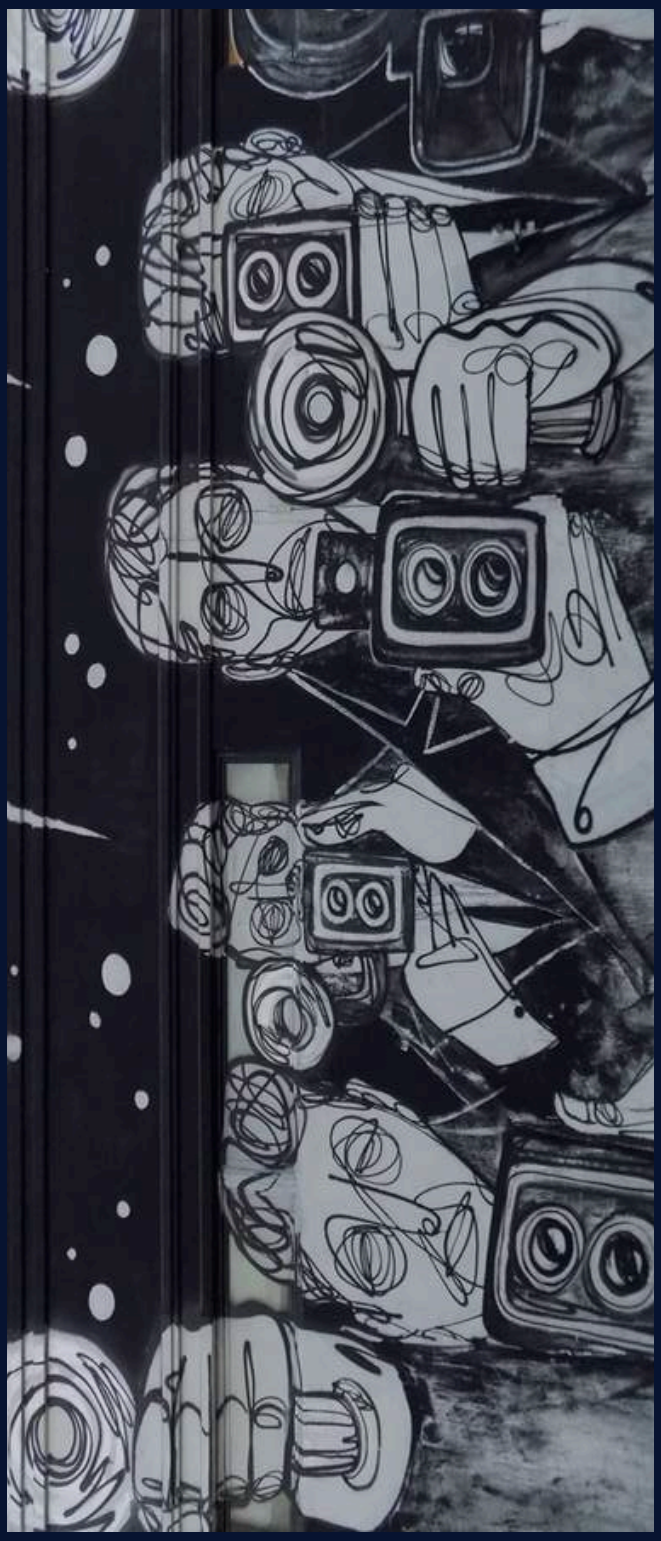
The Delhi High Court has ordered to restrain a chatbot developed using AI to mimic the renowned Bollywood actor Jackie Shroff. This order comes after the court had a prima facie view that the AI Chatbot violated Jackie Shroff's personality rights.

LEGAL TALK

As per the case of *Shivaji Rao Gaikwad v. Varsha Productions*, Personality rights are granted to individuals who are publicly recognized and have achieved celebrity status. These rights aim to prevent deception, confusion, and falsity by prohibiting the misrepresentation and impersonation of such individuals. The concept of personality rights in India originated in the case of *D.M. Entertainment v. Baby Gift House* in which Daler Mehendi, a renowned singer, who had a registered trademark "DM" and ran "D.M. Entertainment Pvt. Ltd.", filed a lawsuit against a defendant selling dolls, inspired by him which also sang his songs. The court ruled that Daler Mehendi's identity and reputation had economic value, making unauthorised use of his persona a case of false endorsement. The plaintiff was granted relief under the concept of passing off, which means no one possesses the power to represent someone else's goods as theirs under trademark law.

In the case of *Amitabh Bachchan v. Rajat Nagi and Others*, Amitabh Bachchan argued that his name and voice were being misused to spread fraudulent messages on WhatsApp for commercial gain in lottery scams. The court acknowledged Mr. Bachchan's celebrity rights and issued an ex-parte injunction to safeguard his public image. In essence, all of the aforementioned cases establish the recognition of personality rights in India, particularly for public figures and celebrities. These rights aim to protect individuals from the unauthorised commercial exploitation of their identities, which includes their names and voice. The recent development of an AI chatbot designed to mimic the voice of actor Jackie Shroff raises significant concerns regarding personality rights and the potential for misuse. This ground

breaking instance of an AI system replicating a celebrity's vocal characteristics represents a violation of Jackie Shroff's personality rights, as the chatbot could be employed for various unspecified purposes, leading to grave injustice and malicious exploitation of his voice for personal gain or defamation, as can be seen in the case of Amitabh Bachchan. This issue demands a broader examination of the consequences that may arise if chatbots or other applications are developed to mimic the voices of artists and public figures. Such technology could facilitate the wrongful persuasion of individuals through the influential voices of renowned personalities, potentially inciting civil unrest, exacerbating societal divisions, and even instigating riots. The unauthorised access and replication of their vocal identities could severely undermine their commercial interests and livelihood as the voices of these individuals are intrinsically associated with their professional endeavours, including performances, advertisements, and films. This situation represents a profound invasion of privacy, as it becomes increasingly difficult for the public to distinguish genuine vocal instances from artificially generated imitations. Furthermore, the proliferation of such technology raises ethical concerns regarding the exploitation of an individual's identity without their explicit consent. It could potentially enable the creation of deepfakes or synthetic media that misrepresents the views and opinions of public figures, contributing to the spread of misinformation and eroding public trust.



THE WAY FORWARD

Addressing this issue requires a multifaceted approach involving legal frameworks, guidelines, and technological safeguards. Policymakers must prioritise the development of robust regulations and intellectual property laws that protect individuals' personality rights and prevent the unauthorised commercial exploitation of their voices. Additionally, guidelines should be established to ensure the responsible development and deployment of AI systems that mimic human characteristics, with a focus on transparency, accountability, and respect for individual privacy. The advent of AI chatbots that are capable of mimicking celebrity's voices raises critical questions about privacy, intellectual property, and the potential for misuse. We must address these concerns proactively, fostering a collaborative effort among policymakers, legal experts, technologists, and stakeholders to strike a balance between innovation and the protection of individual rights.

COUNCIL OF EUROPE ADOPTS INTERNATIONAL TREATY ON AI

NEWS

On 17 May 2024, The Council of Europe (**"CoE"**) took a significant step towards addressing the challenges posed by AI systems with the adoption of the world's first internationally binding treaty on AI focusing on the intersection of AI, human rights, democracy, and the rule of law. The treaty was Coordinated by the Committee on Artificial Intelligence, which brought together 46 CoE member states, 11 non-member states, as well as representatives from the private sector, civil society, and academia in observer roles.

THE WAY FORWARD

Moving forward, robust international cooperation, ongoing dialogue, and knowledge-sharing among stakeholders are crucial. Developing standardised risk assessment methodologies, capacity-building initiatives, and mechanisms for continuous review and adaptation of regulatory frameworks can help address the challenges. Additionally, further work is needed to establish clear guidelines for allocating responsibility and determining liabilities in case of AI-related violations. Ultimately, a comprehensive and deliberative approach is necessary to understand the social, economic, and legal implications of AI systems, enabling the design and implementation of effective regulatory frameworks that balance innovation with the protection of fundamental rights and values.

LEGAL TALK

Article 3 of the treaty lays down the scope which encompasses the public sector and the private actor's use of AI, including companies acting on behalf of public authorities. However, an exemption is given to research and developmental activities and in matters of national security. The term national security is quite broad, and the treaty does not provide explicit boundaries on the scope of exemption. Given the evolving nature of warfare, which increasingly relies on technology, there remains a concern about the potential misuse of AI systems by using the name of national security.

Article 16 of the Convention adopts a risk-based approach to AI governance, Each Party shall adopt measures for the identification, assessment, prevention and mitigation of risks posed by AI systems by considering actual and potential impacts to human rights, democracy and the rule of law. Parties are free to impose moratoria, prohibition, or alternative measures for AI applications that pose risks incompatible with human rights norms. However, this approach is not without its challenges. Regulating AI systems is distinct from traditional areas of regulation, as it involves a continually evolving frontier of emerging digital capabilities, including machine learning, computer vision, and neural networks, among others. Managing the risk-based implications of AI necessitates navigating complex interdependent dynamics, such as autonomy, learning, and inscrutability, as the performance and scope of AI systems continue to evolve.

While the Convention represents a significant step in moving beyond high-level principles in AI governance, it falls short in addressing critical questions surrounding the allocation of responsibility and determination of liabilities in case of violations. The assessment of risks to human rights, democracy, and the rule of law inherently involves subjective interpretations. Different stakeholders may have divergent perspectives on what constitutes a risk or an acceptable level of risk, leading to potential conflicts and inconsistencies in risk evaluation and mitigation measures.

DATA PRIVACY

SECTION 4

CHATGPT FACES YET ANOTHER PRIVACY COMPLAINT

NEWS

Privacy rights non-profit noyb has filed a complaint in Austria against OpenAI's chatbot ChatGPT. The complaint focuses on the bot's inability to correct misinformation, claiming it to be 'technically impossible'. OpenAI offered to restrict responses mentioning the public figure's name instead.

LEGAL TALK

Both the General Data Protection Regulation, 2016 ["**GDPR**"] and the Digital Personal Data Protection Act, 2023 ["**DPDPA**"] aim to protect personal data. Personal data includes any information related to an identified or identifiable person, such as your name, identification number, etc. The GDPR covers both publicly available data and data obtained with consent, while the DPDPA focuses only on consent-based data. Publicly available data isn't just information accessible to everyone without special permissions but also includes information from social media sites like Reddit and TikTok, as well as data exposed through breaches. Section 12 of the DPDPA and Articles 5 and 16 of the GDPR grant individuals the right to correct, complete, and update their data to ensure accuracy. This is known as the right to rectification. Generative AI tools like ChatGPT struggle with data handling. They claim they cannot correct misinformation because they can't access or modify their training data, which serves as the foundation for their outputs. Once trained, the model's information becomes static and unchangeable, making it impossible to correct inaccuracies.

These issues highlight the difficult balance nations face with AI tools. While AI is seen as economically essential and the "next big thing," there is fear of falling behind if development is restricted. Current regulations did not anticipate the challenges specific to generative AI, making compliance difficult. Two possible solutions are to ban these AI models due to non-compliance or amend existing laws to accommodate them. The key question is which option offers more benefits. ChatGPT and similar tools provide significant technological advancement and aid, making a complete ban harsh.

However, technology must comply with legal requirements, not the other way around. It's irresponsible for companies to create products expecting laws to accommodate them. This could lead to unchecked technological development. Nations must understand these technologies to balance AI's revolutionary potential with robust legal standards, and companies must put in more effort to meet regulatory standards.

THE WAY FORWARD

The consequences of these actions are highly problematic, especially when false information is about individuals. OpenAI's privacy policy allows users to request corrections for inaccuracies but mentions potential "technical complexities," making it unclear when corrections can be made. If corrections are not possible, users are advised to request removal of their personal information via a web form. This approach conflicts with GDPR and DPDPA, which do not allow for *selective* compliance. As noyb points out, OpenAI cannot *choose* which rights to grant. Blocking incorrect responses is not feasible due to the *vastness* of the training data. Also, this approach fails to address the AI's inability to accurately track and correct personal data. Fixing mistakes requires retraining the model, which takes months and is impractical for every correction. Researchers are exploring "machine unlearning" techniques, but this technology is still in its early stages and likely won't effectively remove the incorrect data. Creating AI tools like ChatGPT without training datasets is impractical, and avoiding personal data in training is also unrealistic. These issues emphasise the inefficacy of current methods and the need for more robust solutions.

CONTRIBUTORS

WRITERS

LAVANYA CHETWANI

ANJALI PANDE

SAGUN MODI

TRISHNA AGRAWALLA

NAMAN OSTWAL

NIKHIL JAVALI

EDITORS

NIKHIL JAVALI

HARSH MITTAL

SAGUN MODI

DESIGNERS

SAMRIDHI BAJORIA

TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL