LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

MARCH 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

ACCESSIBILITY GUIDELINES IN CINEMA: CENTRE'S MOVE TO BE INCLUSIVE

NEWS

The Union Ministry of Information and Broadcasting ("**MIB**") issued the "*Guidelines for Accessibility Standards In The Public Exhibition Of Feature Films In Cinema Theatres For Persons With Hearing And Visual Impairment*" ("**Accessibility Guidelines**"). It is applicable to all feature films that have been approved by the Central Board for Film Certification ("**CBFC**").

LEGAL TALK

Section 29 and Section 42 of the Rights of Persons with Disabilities Act, 2016 ("**the Act**"), require the relevant government authorities to implement measures promoting universal service and access in the information and communication sector, including facilitating access to films for individuals with hearing and visual impairments. The Accessibility Guidelines align with the Act by aiming to increase accessibility for the hearing and visually impaired. The objective of MIB is to implement measures guaranteeing individuals with hearing and visual impairments equal access to the public screening of feature films in cinema halls or movie theatres intended for commercial purposes.

These Accessibility Guidelines require the producers to submit a *digital cinema package* after inclusion of the accessibility features like Audio Description, Closed Captioning/ Indian Sign Language Interpretation for the CBFC certification. It imposes obligations upon the producers as well as cinemas by stating that these cinemas must ensure the theatrical release feature films have the features as required by CBFC before the release.

Those feature films that have to be certified in more than one language shall incorporate one accessibility feature each for the hearing and visually impaired within 6 months of the date of implementation of the guidelines. Those submitted for awards will have to include the features 1st January, 2025 onwards and the remaining category of films need to comply within 2 years of the date of issue of these guidelines. Government of India.

THE WAY FORWARD

These guidelines emphasise not just the content of films, but also on the provision of information, assistive devices, and necessary infrastructure support to enable individuals with disabilities to enjoy movies in cinema theatres. Despite existing rules promoting inclusivity in education, employment, and healthcare, there has been limited focus on providing entertainment and creative outlets for individuals with disabilities. The reporting requirements on behalf of the cinemas ensures that the guidelines are being implemented throughout. Further, the setting up of a grievance redressal committee provides an avenue to the aggrieved persons in case of non-compliance with the said guidelines. With these new guidelines, theatres and film producers are provided with clear direction in creating an inclusive environment.

CINEMATOGRAPH (CERTIFICATION) RULES, 2024 NOTIFIED BY THE MINISTRY OF INFORMATION AND BROADCASTING

NEWS

The Cinematograph (Certification) Rules, 2024 replaces the old 1983 rules, and has been notified by the Ministry of Information and Broadcasting ("**MIB**") vide its powers under Section 8 of the Cinematograph Act, 1952. It has been done so in lieu of the recent Cinematograph (Amendment) Act, 2023 ("2023 Act").

LEGAL TALK

The New Certification Rules revolutionise the application process for film certification, shifting from written submissions to online applications via the dedicated 'E-CinePramaan Portal' of the Central Board of Film Certification ("**CBFC**"). All submissions, including synopses, scripts, and song lyrics, must adhere to the format outlined in the CBFC's common application form. Notably, these rules mandate one-third of CBFC members to be women, with a preference for fifty percent representation. Applicants can also opt for expedited certification by paying a higher fee.

Additionally, the UA category, i.e., unrestricted viewing but with a parental discretion advisory, now includes three age-based classifications - UA 7+, UA 13+ and UA 16+ for parental guidance, and complying with the 2023 Act. The New Certification Rules also streamline certification timelines and introduce perpetual validity for CBFC certificates, departing from the 10-year validity period stipulated by the previous 1983 rules.

THE WAY FORWARD

The updated rules are designed to simplify and bring the film certification process up to date for the digital era, aligning with the evolving technologies and progress in the film industry. It reduces the timelines for processing required in film certification by switching to a digital mode. It helps in avoiding the unnecessary paperwork required to renew the CBFC certificates as well. The objective of these rules is to ensure ease of doing business for the film industry. It is in line with the centre's motive of benefitting the Indian economy from the booming film industry.

EU PARLIAMENT PASSES THE MEDIA FREEDOM ACT

NEWS

The European Parliament has passed the European Media Freedom Act ("EMFA"), aiming to protect and strengthen media freedom across EU member states. The law enshrines the Journalism Trust Initiative ("**JTI**") as a benchmark for identifying news media and includes various safeguards to protect editorial independence and prevent political interference.

THE WAY FORWARD

The proposed amendments to the EMFA have drawn scrutiny due to concerns surrounding state advertising, regulatory bodies, and content moderation. Ambiguity in Article 17 raises apprehensions about its potential impact on media freedom, making it difficult to enforce the Digital Services Act against large platforms in a manner that respects human rights. This provision introduces a process for media service providers and 'Very Large Online Platforms' (VLOPs) to present themselves as independent and regulated media providers, subject to specific regulatory requirements. However, worries have been expressed about the potential consequences of this provision on content moderation.

Moreover, concerns have been expressed about the potential consequences of the provision on content moderation and its capability to protect media independence in line with European and international human rights standards. Clarity and safeguards are called for to ensure fair dispute resolution, transparent state advertising practices, and protection of freedom of expression, necessitating further amendments and clarifications to the EMFA.

LEGAL TALK

The EMFA addresses the decline of media freedom and pluralism in the EU and aims to improve the functioning of the internal market for media services. The Act introduces several key provisions to safeguard media freedom.

The EMFA requires media companies to disclose their ownership structures, promoting transparency and accountability in news reporting. This provision aims to prevent undue influence and hidden agendas, thereby fostering a transparent and accountable media landscape. The Act safeguards media companies from unjustified, disproportionate, and discriminatory national measures, allowing them to report freely without interference, thereby upholding the principles of media freedom and independence. The EMFA includes a provision that requires news outlets to disclose the amount they receive from state advertising, aiming to ensure transparency and prevent governments from unfairly favouring certain media organisations. The Act introduces a right of customization of media offered on devices and interfaces used to access media services, empowering users to tailor their media consumption, promoting a more personalised and user-centric media experience.

The EMFA ensures that Member States provide in national law for an assessment of media market concentrations that could significantly impact media pluralism and editorial independence, promoting a well-functioning internal media market.The establishment of the European Board for Media Services reinforces the enforcement of media freedom protections and ensures the right application of the EMFA, thereby promoting accountability and trust in the European media landscape. The EMFA complements the Digital Services Act and the Digital Markets Act, providing a clear, legally binding framework for national regulatory authorities to address providers engaged in disinformation and abuse of internal market freedoms.

Online Gaming and Betting Laws

SECTION 2

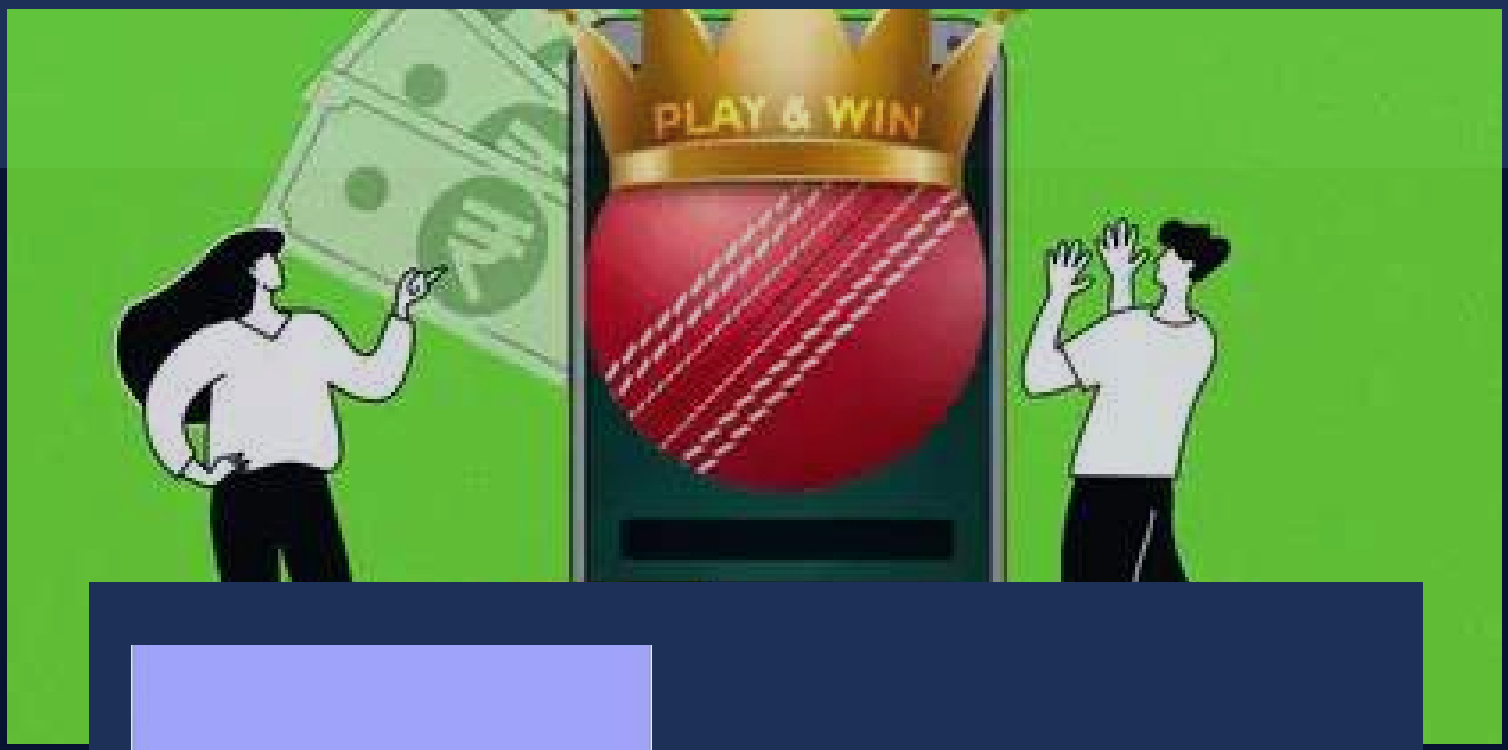
CCPA ISSUED ADVISORY AGAINST ILLEGAL BETTING AND GAMBLING ADVERTISEMENTS

NEWS

The Central Consumer Protection Authority ("**CCPA**") on 6 March 2024 issued '*Advisory in terms of Consumer Protection Act, 2019 on Prohibition of Advertising, Promotion, and Endorsement of unlawful activities prohibited under various laws*' ("**Advisory**"). The advisory has been issued in accordance with the Consumer Protection Act, 2019, emphasises the prohibition of advertising, promotion, and endorsement of activities deemed illegal under various laws.

LEGAL TALK

The advisory aims to prohibit the promotion of illegal activities like online betting and gambling by celebrities and influencers. This action stems from the inherent illegality of such activities under the Public Gambling Act, 1867. The advisory emphasises the significant financial and socio-economic risks associated with online gambling, particularly for young audiences. The advisory strengthens its position by referencing Clause 9 of the Guidelines for Prevention of Misleading Advertisements, 2022 ("**Guidelines**"). This clause explicitly prohibits advertisements for products or services banned by existing legal frameworks. The advisory emphasises the universality of these guidelines, encompassing all forms of media used for advertising. Notably, the CCPA clarifies through this advisory that activities deemed illegal under other laws are automatically prohibited under the aforementioned guidelines. Therefore, any form of advertisement promoting prohibited activities, directly or indirectly, including betting and gambling, will face rigorous scrutiny. Furthermore, the advisory emphasises that participating in the promotion or advertisement of such activities is akin to participating in the illegal activity itself. In the event of violations, stringent measures will be implemented against all involved parties under the Consumer Protection Act, 2019. This includes manufacturers, advertisers, publishers, intermediaries, social media platforms, celebrities, influencers, and other stakeholders.



Moreover, it is important to note that the Ministry of Information and Broadcasting (MIB) also issued a complementary advisory on 21 March, 2024, titled "*Advisory on Celebrity/Influencer Endorsements and Advertisements, including Surrogate Advertisements, of Offshore Online Betting/Gambling Platforms.*" This action reinforces the focus on online advertisements, a domain over which the MIB holds regulatory authority and the power to issue notifications to intermediaries.

THE WAY FORWARD

With the emphasis on the illegality of gambling and betting under the Public Gambling Act and its potential financial and social harms, particularly towards young people, the advisory strengthens the legal basis for holding all participants in its promotion accountable. Clause 9 of the Guidelines prohibits advertising banned products, and the CCPA clarifies its application to online endorsements by celebrities and influencers. This broadens the scope of potential violations under the Consumer Protection Act, subjecting not only gambling platforms but also manufacturers, advertisers, social media platforms, and the endorsing individuals themselves to stringent legal repercussions.

FinTech

SECTION 3

THE RBI NOTIFIES THE BBPS MASTER DIRECTIONS, 2024

NEWS

The Reserve Bank of India ("RBI") notified the RBI (Bharat Bill Payment System) Master Direction, 2024 ("BBPS Directions") on 29th February 2024. The amended and updated direction was issued in light of recent advancements and significant developments in the payments sector, revising the bill payment process, encouraging more involvement, and improving customer safety, among other things.

LEGAL TALK

The core of the BBPS Directions centres around the NPCI Bharat Bill Pay Limited ("**NBBL**"), functioning as the Bharat Bill Pay Central Unit ("**BBPCU**") and authorised as the Payment System Provider for BBPS. The BBPCU is responsible for setting operational, technical, and business standards within the BBPS platform and manages critical functions like clearing and settlement to ensure smooth transaction processing.

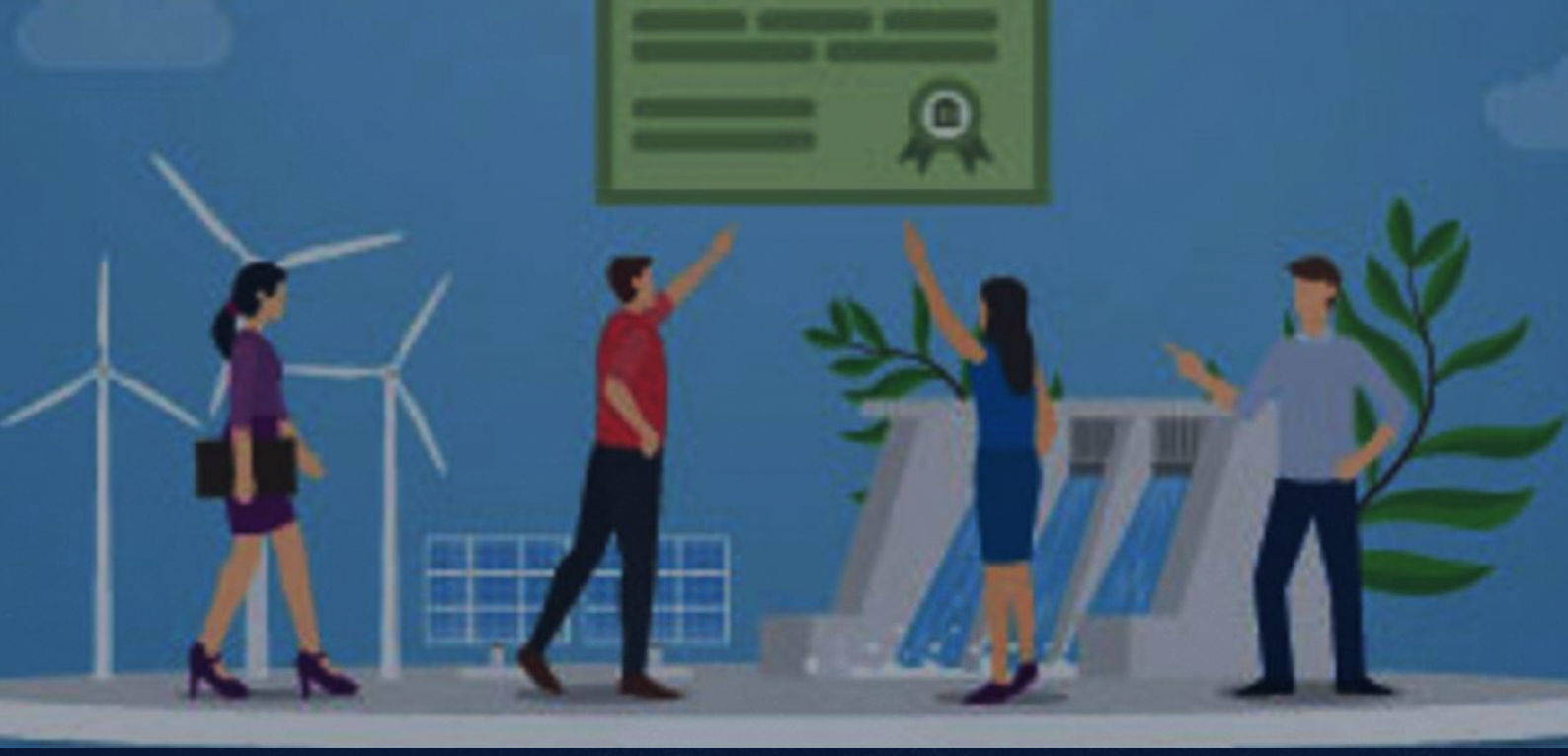
Further, the Bharat Bill Payment Operating Units ("**BBPOUs**") encompass banks, non-bank Payment Aggregators (PAs), and other authorised participants. BBPOUs operate as essential Operating Units within the BBPS framework, with Biller Operating Units ("**BOUs**") handling biller onboarding, due diligence compliance, and managing intricate relationships with billers and biller aggregators. On the other hand, Customer Operating Units ("**COUs**") provide digital and physical interfaces for processing bill payments, managing customer access to billers, and handling consumer-related disputes.

In terms of financial operations, non-bank BBPOUs are required to maintain dedicated escrow accounts exclusively for BBPS transactions. These escrow accounts play a critical role in ensuring proper fund management and adhering to specific guidelines established by the RBI for bill payments, settlements, charges, and recoveries.

Lastly, an essential framework introduced is the dispute resolution mechanism, which integrates all participating COUs and BOUs. This mechanism facilitates efficient and timely resolution of complaints and disputes, establishes timelines for handling failed transactions, and ensures proper customer compensation.

THE WAY FORWARD

The BBPS directions aim to enhance efficiency, transparency, and security within the system. It streamlines processes, enhances customer protection, encourages greater participation, and ensures clear responsibilities among participants. However there are potential downsides. Increased compliance burdens may strain smaller players and escalate costs. New entrants could face complexities meeting strict standards, limiting market competition. Mandating escrow accounts may add financial burdens, and existing systems may face disruptions. Although customer protection measures improve, initial challenges could affect user satisfaction. Balancing these aspects is crucial for achieving a more effective and consumer-friendly BBPS ecosystem.



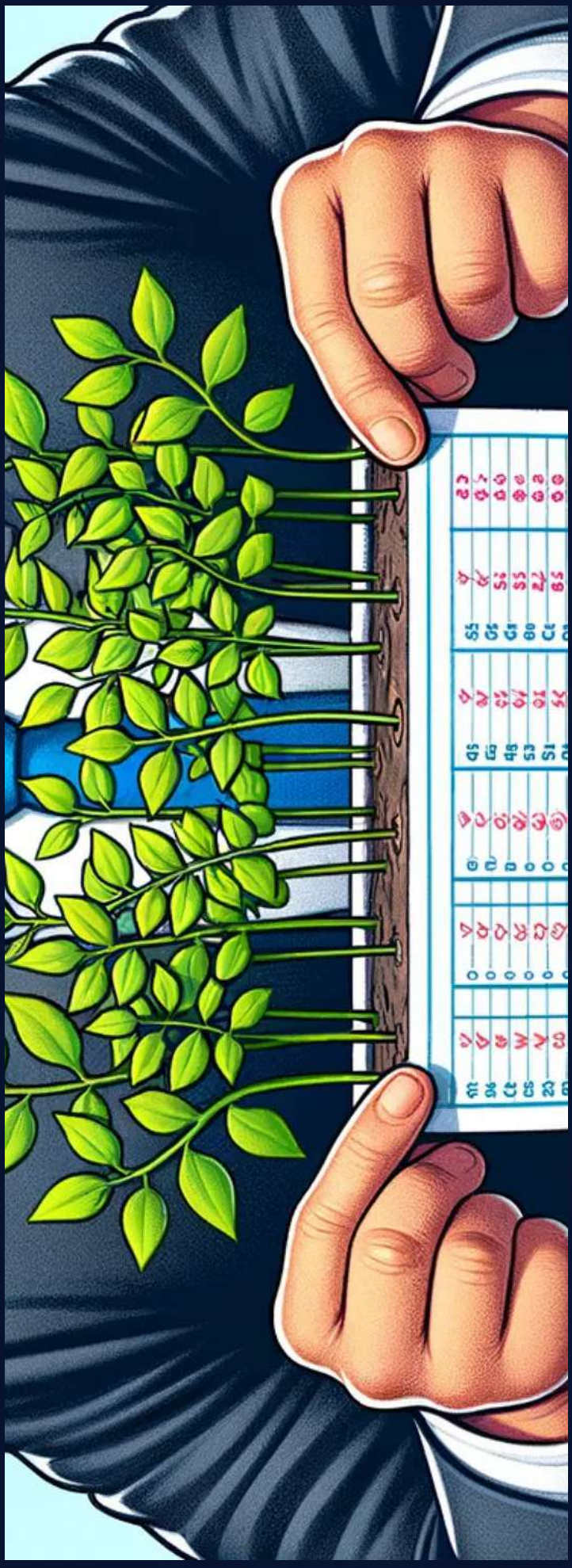
RBI ISSUES A DRAFT FRAMEWORK TO ADDRESS CLIMATE RELATED FINANCIAL RISKS

NEWS

The Reserve Bank of India ("**RBI**") notified the Draft Disclosure Framework on Climate-related Financial Risks, 2024 ("**Disclosure Framework**") on February 28, 2024. The Disclosure Framework provides a guideline to address the increasing threat of climate change, market changes towards sustainability, and the role of financial institutions in financing environmentally sustainable initiatives. It further emphasises implementing robust climate-related financial risk management policies and processes by Regulated Entities ("**REs**")

LEGAL TALK

The RBI exercised its powers under the Banking Regulation Act, of 1949 in the public interest and issued the Disclosure Framework. The applicability of the Disclosure Framework extends to a wide range of REs within the financial sector, including Scheduled Commercial Banks, Tier-IV Primary (Urban) Co-operative Banks, All-India Financial Institutions, and Top and Upper Layer Non-Banking Financial Companies. The framework introduces four thematic pillars of disclosure: Governance, Strategy, Risk Management, and Metrics/Targets. These pillars serve as foundational elements guiding REs in articulating their approach to identifying, assessing, managing, and reporting on climate-related financial risks and opportunities. The Governance pillar emphasises disclosing governance structures and responsibilities. The Strategy pillar focuses on strategies for identifying and responding to climate risks. Risk Management entails disclosing risk assessment methodologies and integration processes. Metrics/Targets require disclosing performance metrics, capital deployment, and integration into remuneration policies.



THE WAY FORWARD

The Disclosure Framework has a profound impact on stakeholders by fostering transparency and accountability within REs. For investors, the framework offers valuable insights into how REs manage climate-related risks and opportunities, enabling informed investment decisions aligned with sustainability goals. Regulators benefit from enhanced risk assessment capabilities and improved market discipline, contributing to financial stability. However, the framework's implementation may encounter challenges, including varying capacities among REs to gather and report relevant data accurately. This could lead to inconsistencies in disclosed information, potentially affecting the comparability and reliability of climate-related disclosures. Despite these challenges, the framework represents a crucial step forward in addressing climate-related financial risks, highlighting the need for ongoing monitoring and support to ensure its effectiveness and meaningful impact on stakeholders.

RBI'S NEW RULES REGARDING CARD NETWORK CHOICE

NEWS

Currently, the choice of network for a card issued to a customer is decided by the card issuer (bank/non-bank) and is linked to the arrangements that the card issuers have with card networks in terms of their bilateral agreements. Recently, RBI vide its circular has given customers the opportunity to opt for their choice of card network.

LEGAL TALK

Card issuers are financial institutions (like banks and non-banks) that issue you the credit, debit, or prepaid cards. Card networks are the bridge between card issuers and acquirers. They route, process, and facilitate the transaction. Some examples of card networks authorised by RBI are RuPay, Visa, and Mastercard, etc. As per the circular, card issuers shall not enter into any arrangement or agreement with card networks that restrain them from availing the services of other card networks. Additionally, multiple choices of card networks must be provided to the customers by the card issuers at the time of issuance. This option may be given to the existing cardholders at the time of renewal. This direction implies that card issuers can no longer have an exclusive tie up with a particular card network and they have to provide at least two options to the customers. However, the directions do not apply to card issuers with their own card network and smaller issuers (with less than 10 lakh active cards). The circular portrays RBI's customer centric approach and it will benefit customers as it will provide them a wider range of options to choose from. They can make this decision based on the unique benefits, customer service and acceptance rate of these networks. Additionally, encouraging credit card issuers to diversify networks can ensure customer independence from single-network dependencies. This will ultimately help in preventing network failures.

THE WAY FORWARD

Diversifying card networks among issuers may induce competition, reducing the Merchant Discount Rate ("MDR"). MDR is the charge recovered by the acquirer (entities which enable the acceptance of payment instruments) from the final recipient of money (the merchant). Networks may leverage discounts and cashback incentives to lure customers to choose their card network. Overall, customer-centricity lies at the heart of the circular and will ultimately benefit the customers.

RBI ISSUES MASTER DIRECTIONS FOR FILING OF SUPERVISORY RETURNS

NEWS

Recently, RBI issued master directions for filing of supervisory returns. The bank issued directions to bring clarity, brevity and harmonisation to the instructions issued to various supervised entities for submission of returns. The move aims at reducing the burden of compliance on the regulated entities.

LEGAL TALK

The directions will be applicable to all commercial banks, Urban Co-operative Banks, All India Financial Institutions, all non-banking financial companies ("**NBFC**"), and Asset Reconstruction Companies. These entities, for these directions, are called Supervisory Entities ("**SE**"). The RBI excluded regional rural banks and housing finance companies from the ambit of the directions. The major provisions of the directions are:

1. **Responsibilities of the board and senior management**

The central bank has asked bank boards and senior management to exercise caution on risk data aggregation and reporting practices, besides ensuring adequate resources for execution. Also, the management must include the identification, assessment, and management of data quality risks as part of its overall risk management framework.

The directive seeks to enhance the accuracy and reliability of reported data, mitigating the potential for erroneous decision-making and regulatory non-compliance. Compliance with these directives is likely to result in improved data governance, enhanced risk management

practices, and ultimately, greater financial resilience within the banking sector.

2. IT infrastructure

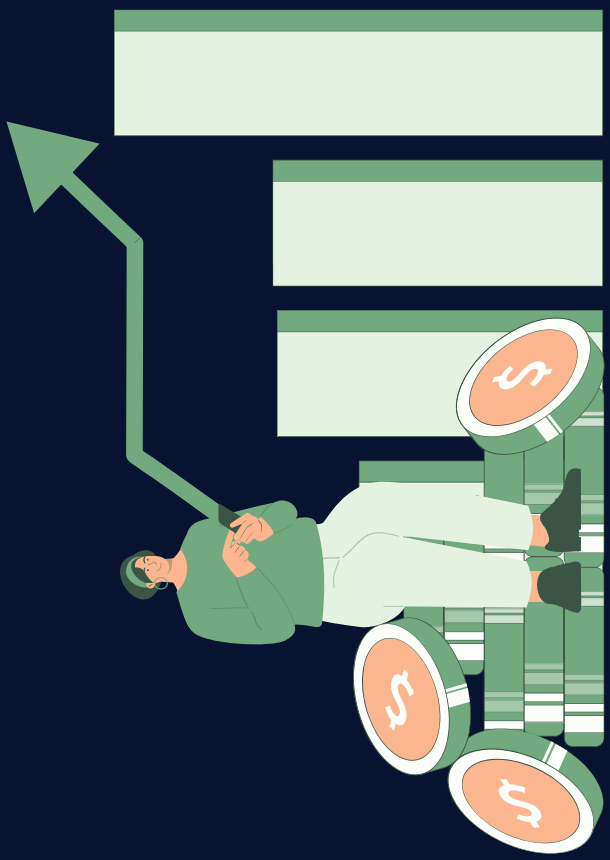
The directions provide that a SE shall design, build, and maintain the data architecture and supporting IT infrastructure for accurate, complete and timely data aggregation and reporting not only in normal times but also during times of stress or crisis. Additionally, SEs should ensure that resources and IT infrastructure is adequate to meet a broad range of on-demand, ad hoc reporting requests.

These directions reflect a proactive approach to risk management. By ensuring these provisions, SEs can bolster their resilience to adverse market conditions and operational disruptions.

3. Accuracy and integrity

The directions provide that all return reports are to be reconciled with SE's sources to ensure the accuracy and completeness of the same. SEs should also measure and monitor the accuracy of data and develop appropriate escalation channels and action plans to rectify any deterioration in data quality. The directions aim at enhancing trust and confidence in the financial system. By seeking automation in data generation, SEs can streamline reporting processes, reducing the risk of human error and enhancing efficiency.

Apart from these, the direction also provides for harmonised timelines for filing all the returns for the SEs. According to the directions, commercial banks have to file 36 returns, including "asset quality", "liquidity return" etc. Select all Indian financial institutions that have to file 10 returns; urban cooperative banks (20 returns) and NBFCs (12). RBI has provided that all SEs have to file returns relating to Financial Soundness Indicators; Fraud Monitoring and Vigilance Monitoring



THE WAY FORWARD

The Master Direction is a welcome move as it consolidates all major aspects of compliance and makes it more transparent and in one place. Additionally, aspects related to facilitating ease-of-doing business, reducing compliance burden, rationalising regulations, and simplifying requirements aim to make these more transparent and consolidated in one place through a comprehensive Master Direction.

ARTIFICIAL INTELLIGENCE

SECTION 4

UNDERSTANDING THE EU AI ACT 2024 AND ITS IMPACT

INTRODUCTION

The European Parliament has recently passed the Artificial Intelligence Act, 2024 ("**the Act**"). The Act has become the first law that specifically addresses Artificial Intelligence ("**AI**"). The primary objective of the Act is to enhance the internal market's functionality by establishing a legal framework for the development, market entry, deployment, and usage of AI systems within the EU. The implementation of this law will occur gradually over varying periods, ranging from 6 to 36 months.

THE LEGAL TALK

The Act defines an AI system under Article 3 (1) as a software designed to achieve human-defined objectives and generate outputs like content, predictions, or recommendations that affect the environments they interact with. This broad definition encompasses various systems falling under this category. Article 2 of the act outlines its scope, which includes AI service providers offering services within the EU, regardless of their location within the EU or in a third country. It also covers users of AI systems within the EU, as well as providers and users in third countries whose outputs are utilised within the EU. However, the act does not apply to AI systems used exclusively for military purposes, nor does it apply to public authorities of third countries and certain specified international organisations. The Act categorises AI on the level of Risk it poses, on four levels of risk – unacceptable risk, high risk, limited risk and minimal risk. These risks lay down the regulatory compliances for varying levels of risk which ensures the protection of consumer interests and promotes structured and regulated growth of AI.

UNACCEPTABLE RISK

Article 5 of the AI act talks about prohibited AI practices. It forbids employing subliminal methods or exploiting vulnerabilities of specific groups using AI for causing physical or psychological harm. Additionally, using AI in social scoring for unjust treatment and utilising real-time biometric identification systems in public areas for law enforcement unless strictly required for specific purposes like preventing crimes, finding victims etc.

These regulations aim to prevent harmful or discriminatory AI practices, ensuring responsible and ethical deployment of AI technologies in various contexts. Such techniques can exploit psychological vulnerabilities and infringe on individuals' autonomy and decision-making processes. Overall, these prohibitions align with ethical principles and human rights considerations, reflecting the need for responsible AI development and deployment.

HIGH RISK

The "high-risk" category is mentioned in Article 6 of the Act. It encompasses a wide range of AI applications, including educational or vocational training tools, employment evaluation platforms, and financial or insurance-related systems. However, the exact scope of high-risk technologies is still under development, with the European Commission and AI Office tasked with providing practical guidance within 18 months. To avoid certain restrictions, companies must conduct thorough assessments before market entry and provide these assessments to national authorities upon request. High-risk technology developers and implementers must adhere to several requirements, including registering with the centralised EU database, implementing a compliant quality management system, maintaining detailed documentation and logs, undergoing conformity assessments, following usage restrictions, and ensuring ongoing regulatory compliance.

LIMITED RISK

The third risk under the Act deals with limited-risk AI systems, which include chatbots and which impose lighter transparency obligations. Developers and deployers of these systems are required to make sure that end-users are aware that they are interacting with AI. This provision aims to promote transparency and awareness without burdening limited-risk AI systems with extensive regulatory requirements.

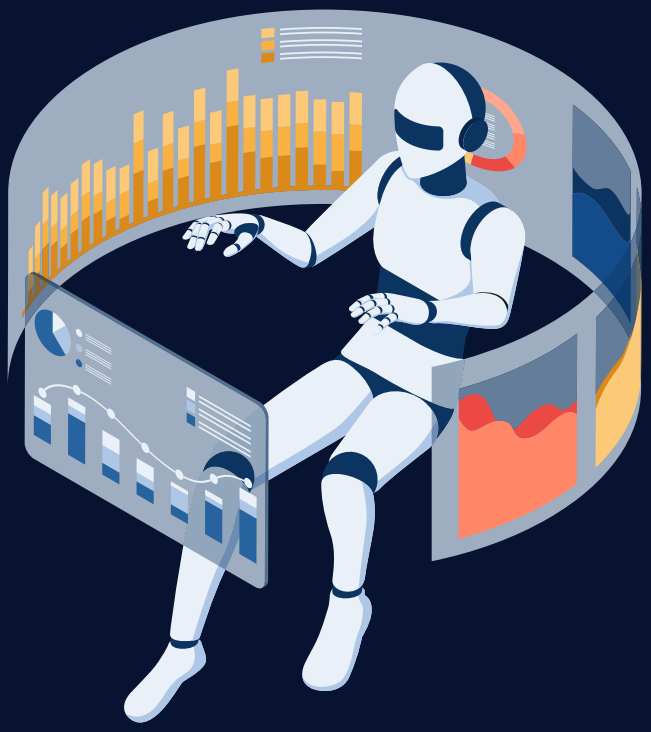
MINIMAL RISK

AI applications categorised as minimal risk are not subject to regulations, including many AI applications already available in the EU single market, such as AI-powered video games and spam filters. It is important to note that this category is evolving in nature and with the emergence of generative AI technologies it may lead to changes in regulation regarding minimal-risk AI applications.

GPAI PROVIDERS

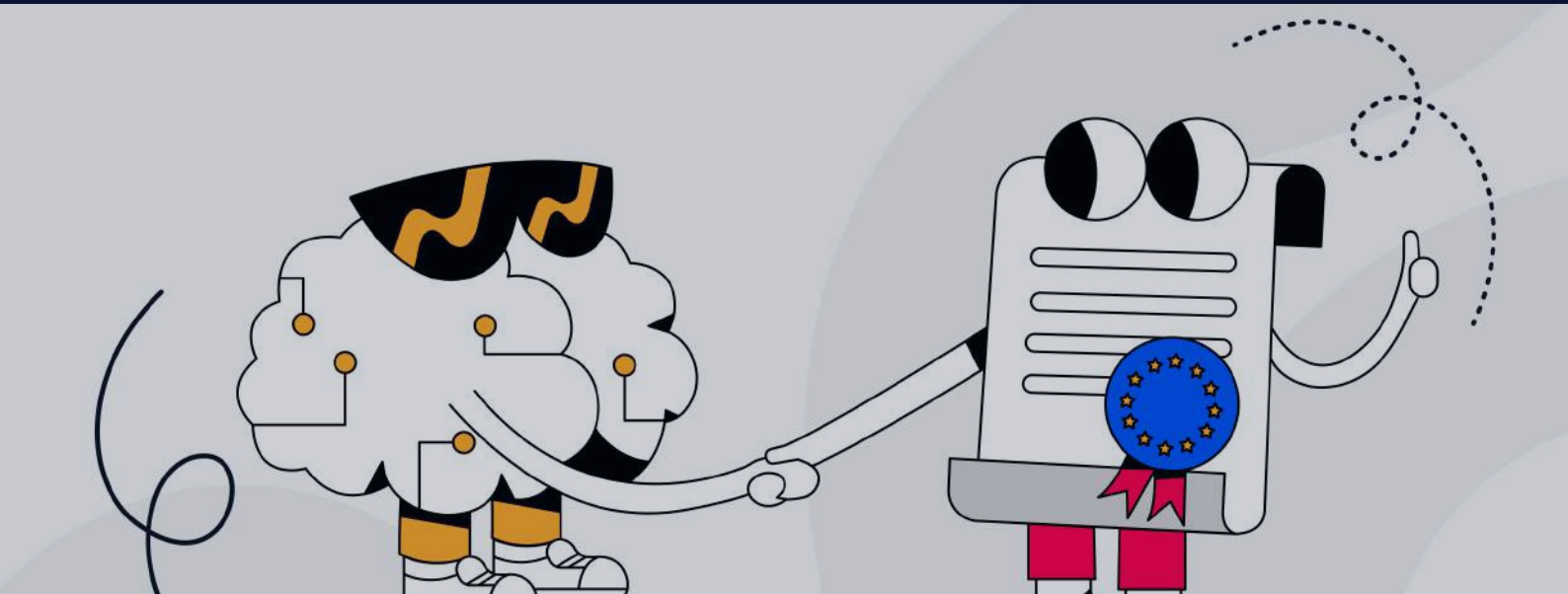
A General-Purpose Artificial Intelligence (“**GPAI**”) is defined under Article 3 (44e) of the Act and it refers to an AI system that is built upon a general AI model and is capable of serving diverse purposes which includes direct use as well as integration into other AI systems. Providers of models are subject to varying requirements based on their licensing and potential risk factors. Firstly, all providers of GPAI models, regardless of their licensing status, must furnish technical documentation, user instructions, abide by the Copyright Directive, and disclose a summary detailing the content used during the model's training. However, there are distinctions for free and open-licence GPAI model providers. These providers are only obligated to comply with copyright regulations and publish a summary of their training data, unless their models are deemed to pose a systemic risk.

On the other hand, providers of GPAI models categorised as presenting a systemic risk , regardless of whether they are open or closed-licence models, must adhere to additional requirements. The determination on systemic risk will rely on the capacity of the AI system, which can be assessed either by a quantitative threshold on the basis of total cumulative resources used during its training which is measured in floating-point operations (“**FLOPs**”) or by an individual decision made by the Commission.This includes conducting thorough model evaluations, performing adversarial testing, tracking and reporting serious incidents, and implementing robust cybersecurity measures. These regulations are designed to promote transparency, accountability, and responsible usage of GPAI models, with stricter measures in place for models identified as potentially carrying higher risks to individuals or society as a whole.



THE WAY FORWARD

The adoption of the AI act marks a significant milestone in the regulation of AI technologies within the European Union. By categorising AI systems based on risk levels and implementing specific regulatory measures, the Act aims to promote responsible and ethical deployment of AI while safeguarding fundamental rights and societal well-being. Moving forward, stakeholders, including AI developers, providers, and users, must closely monitor the evolving landscape of AI regulations and ensure compliance with the provisions outlned in the Act. Additionally, continuous collaboration and dialogue among regulatory bodies, industry experts, policymakers, and civil society will be crucial in refining and adapting AI regulations to address emerging challenges and technological advancements effectively. By fostering a culture of responsible AI governance, stakeholders can contribute to building trust in AI technologies and harnessing their full potential for positive societal impact while minimising risks.



DECODING THE UNGA'S PROPOSED RESOLUTION ON ARTIFICIAL INTELLIGENCE

NEWS

On 21st March 2024, the United Nations General Assembly ("**UNGA**") adopted the resolution on Artificial Intelligence ("**AI**"). The resolution aims to promote "safe, secure and trustworthy" AI systems and also plans to accelerate the process of achieving the Sustainable Development Goals.

LEGAL TALK

The AI systems referred to in the resolution are only applicable to non-military domains. The resolution does not address the governance of AI systems used in military applications. This raises concerns about the unequal power dynamics and the risk of technological warfare, between developed and developing countries as in most cases developed countries lead the AI systems. The resolution also emphasises on promoting and safeguarding human rights and fundamental freedoms along with protecting individuals from unlawful privacy infringements.

States and other stakeholders are called upon to either refrain or cease the use of AI systems that cannot operate in compliance with international human rights, this is essential to ensure that basic human rights don't get violated in developing AI. It also safeguards intellectual property rights, including copyright-protected content, while fostering innovation. This highlights the need for a balanced approach to encourage creativity and protects creators rights in the AI ecosystem. The resolution has stressed upon the importance of safeguarding privacy and personal data during AI system testing and evaluation. It calls for transparency and compliance with legal frameworks at international, national, and subnational levels, particularly concerning personal data usage throughout AI systems. This covers an important aspect of AI systems as it ensures transparency and control over the use of data. Member States are also urged to take specific measures to reduce the digital divide in gender and ensure equitable access to AI technologies. This reflects a broader commitment to inclusivity and addressing digital disparities among different demographic groups. The private sector is encouraged to adhere to relevant international and domestic laws and align their actions with the United Nations Guiding Principles on Business and Human Rights.

THE WAY FORWARD

The resolution highlights the need for more equitable distribution of the benefits derived from safe, secure, and trustworthy AI technologies. However, the absence of guidelines for military AI systems remains a notable gap that may require further international attention and regulatory frameworks. Moving forward, the UNGA draft resolution on AI necessitates collaborative efforts among Member States, stakeholders, and international bodies. This involves developing comprehensive regulatory frameworks that uphold human rights, promote ethical AI practices, and ensure transparency and accountability. Implementation strategies should include capacity-building initiatives, knowledge-sharing platforms, and regular monitoring mechanisms to assess progress and address emerging challenges. Emphasising inclusive access, responsible data governance, and continuous dialogue will foster innovation while safeguarding individual rights. In conclusion, a concerted global approach is crucial for harnessing the benefits of AI while mitigating risks and advancing sustainable, equitable AI development.

DATA PRIVACY

SECTION 5

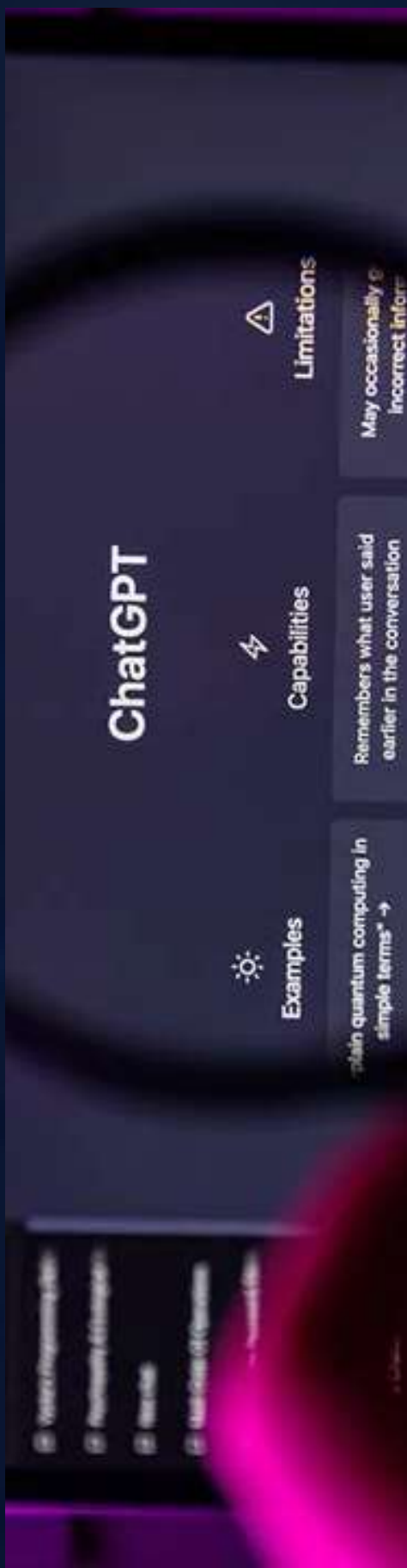
HOW CHATGPT IS VIOLATING GENERAL DATA PROTECTION REGULATION ("GDPR")

NEWS

Italy's privacy watchdog, the Data protection Authority (Garante), which had temporarily banned ChatGPT last year, owing to a partial exposure of personal data of its users, have concluded their investigation. It has asserted that ChatGPT is breaching the EU's GDPR.

LEGAL TALK

Garante, owing to the data breaches and the lack of legal basis for using personal data to train the popular chatbot ChatGPT, had imposed a ban on it temporarily to safeguard the personal data of the Italian users. It is an undeniable fact that ChatGPT has been a sensation since its inception given its ability to produce vast amounts of content including essays and documents on prompt by the users. But, this whole system of artificial intelligence has its strong basis on the amount of data and information that is fed to it, which is culled from the internet. The concern lies in the lack of any notice to the users about their data being gathered by OpenAI. Which has no legal backing that supports the massive collection and processing of personal data to train the algorithms. ChatGPT's tendency to produce inaccurate information at times has raised a doubt on the veracity of the processing of the data, leading to inaccurate personal data being processed. The absence of any age verification has exposed children to inappropriate content. The Italian data protection authority allowed for the reactivation of ChatGPT only upon addressing the concerns regarding the right to decline consent to use personal data to train algorithms. Its fusions of supervised and reinforcement learning to develop the responses have raised alarming concerns. Article 17 of the GDPR provides for 'right to erasure', but given the fact that these generative AIuses natural language processing to create responses from the data collected, makes it impossible to remove the traces of an individual's personal information. The privacy guidelines of OpenAI have reiterated that all the data collected would be confidential and limited. But it is far from complying with the requirements of the European Union GDPR.



THE WAY FORWARD

The concerns raised calls for an extensive investigation into the identity and the enforcement of the legislation regarding the utilisation of AI models in order to ensure that an individual's personal data is protected. The AI Act by the European Union would definitely bring in more comprehensive rules, but its implementation and compliance needs to be given the most importance to safeguard unauthorised utilisation of the personal data by these big giants.

CONTRIBUTORS

WRITERS

LAVANYA CHETWANI

ANJALI PANDE

SAGUN MODI

SHLOKA MATHUR

HARSH MITTAL

NAMAN OSTWAL

EDITORS

NIKHIL JAVALI

HARSH MITTAL

SAGUN MODI

DESIGNERS

SAMRIDHI BAJORIA

TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL