LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

FEBRUARY 2025 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

सत्यमेव जयते धर्म

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

MIB ISSUES ADVISORY TO OTT PLATFORMS ON CONTENT REGULATION

NEWS

The Ministry of Information & Broadcasting (MIB) has issued an advisory to OTT platforms, emphasizing the need for strict compliance with Indian laws and the Code of Ethics prescribed under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

This move comes in response to concerns raised by Members of Parliament, statutory bodies, and public grievances regarding the alleged spread of obscene, pornographic, and vulgar content on streaming platforms and social media. The advisory reiterates the obligations of OTT platforms under Part III of the IT Rules, which require content classification based on age-appropriateness, implementation of access control mechanisms for restricted content, and ensuring that no content prohibited by law is transmitted. It also calls on self-regulatory bodies to take proactive action against platforms that violate these guidelines.

LEGAL TALK

The advisory reinforces the three-tier grievance redressal mechanism under the IT Rules, where self-regulatory bodies play a key role in ensuring that OTT platforms adhere to the Code of Ethics. These bodies, formed by industry associations, act as an intermediary between platforms and the government, ensuring content classification, age restrictions, and compliance with the law. The structure and functioning of these self-regulatory bodies raises some concerns. While they are seemingly independent, oversight by the MIB blurs the lines between self-regulation and state intervention. The IT Rules mandate that these bodies escalate unresolved grievances to an interdepartmental government committee, meaning that final adjudication still rests with the state. This structure deviates from established global models of self-regulation, such as the UK's Ofcom framework, which allows for greater industry-led decision-making without direct governmental oversight. Moreover, the advisory's call for self-regulatory bodies to take "proactive action" may lead to excessive pre-censorship by platforms. The MIB has also drawn attention to multiple legal provisions that impose criminal liability for publishing obscene or pornographic content, including the Indecent Representation of Women Act, 1986, the Bharatiya Nyay Sanhita (BNS), 2023, the Protection of Children from Sexual Offences (POCSO) Act, and the Information Technology (IT) Act, 2000. The advisory makes it clear that violations of these laws could invite penalties and legal consequences, reinforcing the need for OTT platforms to be cautious about the content they host.

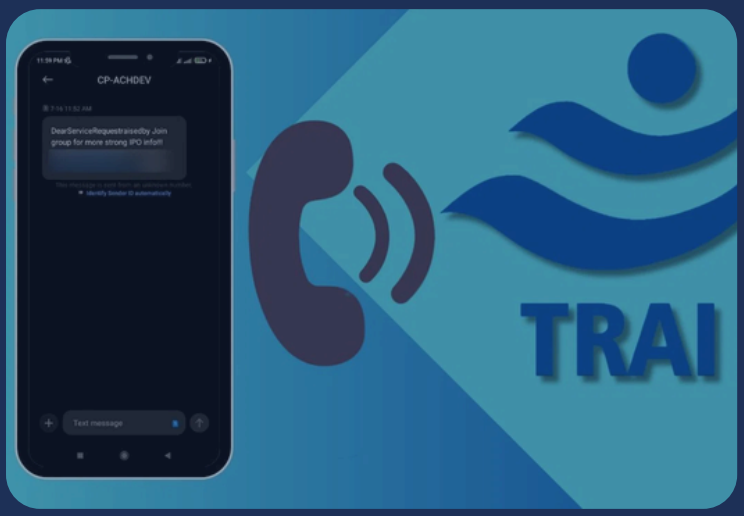
THE WAY FORWARD

While the advisory aims to regulate digital content and ensure compliance with Indian law, it raises concerns about potential implications for creative freedom, platform liability, and the role of self-regulation.Given that the IT Rules already provide for a structured grievance redressal mechanism, the directive's emphasis on proactive intervention by self-regulatory bodies could result in heightened scrutiny of content and possibly a more restrictive environment for streaming services. There is also ambiguity regarding the scope of what constitutes obscene or vulgar content, which could lead to inconsistent enforcement. Moving forward, clearer compliance guidelines and a transparent enforcement framework will be crucial to balancing regulatory objectives with artistic and commercial interests.

TRAI NOTIFIES MAJOR AMENDMENT TO TCCCPR STRENGTHENING TELECOM REGULATIONS

NEWS

The Telecom Regulatory Authority of India (TRAI) has issued a major amendment to the Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, marking a significant shift in the country's regulatory approach to Unsolicited Commercial Communication ('**UCC**'). The new rules introduce stricter measures to combat spam calls and messages, enhance consumer protection, and increase compliance obligations for businesses and telecom operators. The amendment builds upon the existing blockchain-based Distributed Ledger Technology (DLT) framework but introduces more stringent controls to tackle evolving spam tactics. It envisions revised complaint mechanisms, tighter restrictions on unregistered telemarketers, and harsher penalties for violators.



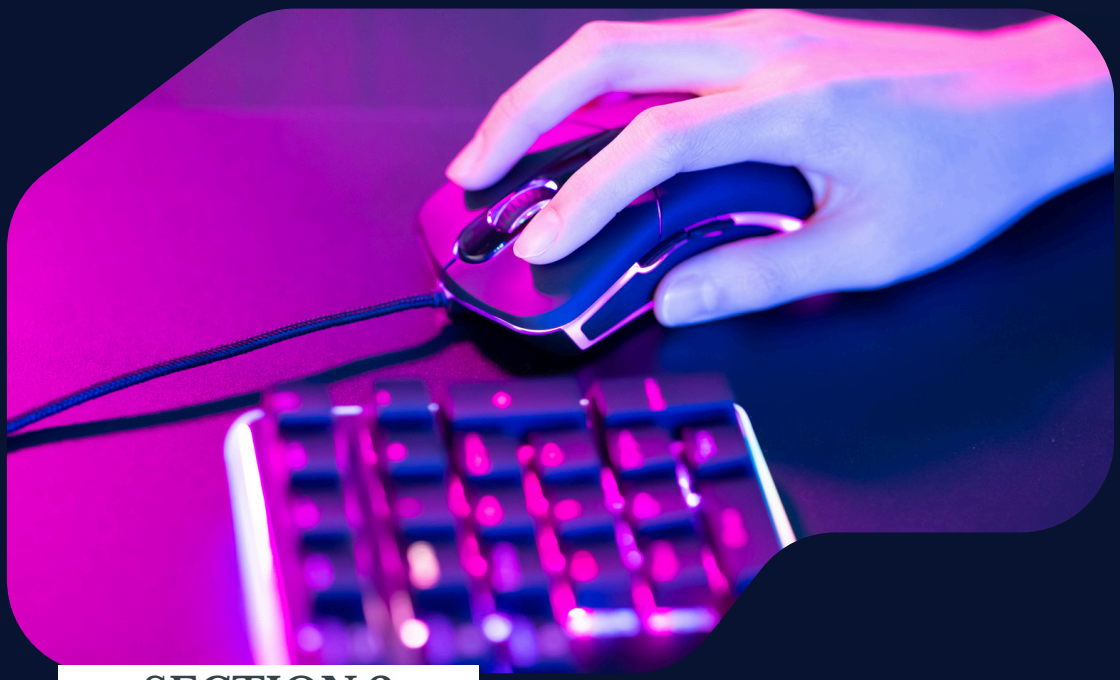
THE WAY FORWARD

These updated regulations aim to protect consumer interests and foster a secure digital communication environment. While TRAI seeks to ensure that critical communications are not filtered, this could interfere with consumers' ability to screen unwanted calls. With enforcement beginning in phases over the next two months, all stakeholders, including businesses and telecom operators, are urged to align their systems with the amended framework to ensure smooth implementation.

LEGAL TALK

The amendment reinforces TRAI's three-tier regulatory approach by requiring that all commercial communication occur through registered headers or designated number series. Telecom operators are now required to actively identify and block spammers using advanced AI-based analytics and honeypot numbers, which are dedicated lines designed to attract and track spam activity. The new framework also mandates biometric authentication and physical verification of telemarketers to improve traceability and accountability. The amendment also looks to make reporting spam easier for consumers, with extended complaint windows and app-based auto-capture of call and SMS details to streamline the process. The threshold for regulatory action against spammers has also been raised, now requiring just five complaints within ten days, as opposed to the previous ten complaints in seven days. Additionally, businesses will need to ensure that promotional messages provide a clear opt-out option and are tagged with standardized identifiers, such as "-P" for promotional, "-S" for service, "-T" for transactional, and "-G" for government messages. The amendment also targets the misuse of normal 10-digit numbers for telemarketing by mandating that promotional calls and messages only originate from designated number series. Repeated violators will face telecom resource suspensions of 15 days for the first violation, with full disconnection and one-year blacklisting for subsequent breaches. Telecom providers that fail to curb UCC will face financial penalties starting at ₹2 lakh for the first violation, scaling up to ₹10 lakh for repeated failures. The latest amendment strengthens consumer protection against spam while imposing significant compliance burdens on businesses and telecom operators. The revised complaint mechanisms and AI-based spam detection herald a more proactive regulatory stance. However, stricter biometric verification and compliance costs could disproportionately affect smaller businesses and independent telemarketers, leading to concerns about market access. Moreover, the ban on call management apps blocking government and commercial numbers raises questions about user control and privacy.

Online Gaming and Betting Laws



SECTION 2

GOOGLE INTRODUCES REVISED “GAMBLING AND GAMES” ADVERTISEMENT POLICY

NEWS

Starting April 14, Google will update its gambling and games advertising policy, allowing online "non-casino" games, including skill-based games, to advertise if they meet specific criteria. Currently, only gambling and fantasy sports platforms are permitted under this policy, but the revision expands opportunities for compliant skill-based gaming platforms.

LEGAL TALK

Google's upcoming revision to its "Gambling and Games" advertising policy represents a pivotal shift in India's online gaming landscape. While current regulations restrict advertising to rummy and fantasy sports, the new policy will permit skill-based games with real-money prizes—such as chess and pay-to-play multiplayer games—to advertise on the Play Store, subject to certification. The policy defines non-casino games as those where outcomes are not determined by chance. However, India's lack of a government-backed classification of "games of skill" versus "games of chance" introduces regulatory ambiguity. The Public Gambling Act, 1867, which influences Meta’s advertising policies, may serve as a benchmark for Google's certification framework. Given India's state-specific gambling laws, platforms must navigate legal complexities, especially in states like Andhra Pradesh, Assam, and Telangana, where even skill-based real-mney games face restrictions.Google’s policy shift presents a major opportunity for gaming platforms like WinZO, expanding market reach and fostering innovation. However, compliance with state laws and Google’s certification requirements remains critical. Legal challenges may arise if states dispute game classifications under gambling laws, given India’s fragmented regulatory framework. While Google’s decision aligns with global digital trends, its impact in India hinges on evolving legal interpretations and state-wise regulations. Gaming companies must navigate these complexities, ensuring adherence to state gambling laws and consumer protection norms. Proactive compliance strategies will be essential to mitigate legal risks while capitalizing on this growth opportunity.

THE WAY FORWARD

Gaming companies must ensure compliance with state-wise laws, secure Google certification, and implement responsible gaming measures. Geo-restrictions and legal assessments are essential for risk management. Industry collaboration and government engagement can drive regulatory clarity. Innovation in skill-based formats, coupled with ethical advertising, will be key to sustainable growth.

TAMIL NADU ONLINE GAMING AUTHORITY ROLLS OUT NEW REGULATIONS FOR ONLINE REAL MONEY GAMES

NEWS

The Tamil Nadu Online Gaming Authority ('**TNOGA**') has introduced a new set of regulations, Tamil Nadu Online Gaming Authority (Real Money Games) Regulations, 2025 ('**Regulations**'). The regulations seek to impose restrictions on children's use of online real money games and functioning hours of the platforms and introduce additional verification requirements.

LEGAL TALK

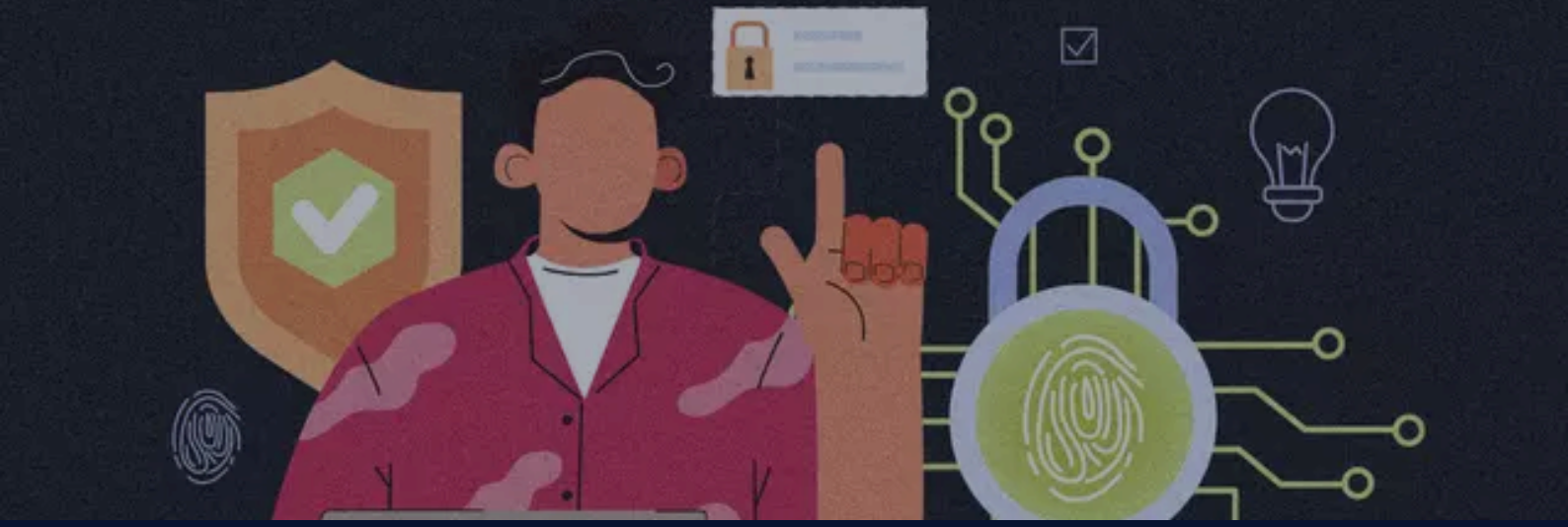
"Online real money game' and 'winnings' under Section 3 of the Regulations are defined as per the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. In a significant step towards minor protection, Section 4(i) of the regulations explicitly prohibits minors from playing online real money games. The Regulations mandate a two-step user verification procedure, as the creation of an account would require a Know Your Customer ('KYC') and further an AADHAR verification by way of sending a one-time password ('OTP') to the AADHAR-linked phone number. The requirement of AADHAR and OTP-based authentication may pose significant privacy concerns despite the underlying objective of ensuring regulatory compliance. Moreover, this does not guarantee eliminating access from minors since using AADHAR details of an adult is not always off-limits for them. The range of restrictions spans further as Section 4(viii) seeks to implement 'blank hours' between 12AM to 5AM IST, prohibiting logins during these hours. Online game providers are supposed to display pop-up cautionary messages on the login page with the words "ONLINE GAMING IS ADDICTIVE IN NATURE" and to players if they play continuously for more than an hour. On the face of it, this seeks to curb gaming addiction. However, implementing such measures rarely ever achieves the desired objective, since factors like user autonomy and loss of business come into play. The Regulations have raised concerns in the Tamil Nadu gaming industry as they came into force on the date of their publication in the state gazette, leaving companies with little to no time for ensuring compliance. The parent statute of the Regulations, that is the Tamil Nadu Prohibition of Online Gambling and Regulation of Online Games Act, 2022, prescribes potential criminal liability for the operators in cases of non-compliance under Section 16(3). Besides, shutting down of logins in the blank hours can also deprive the companies of players from other states, who are not subject to this law.

THE WAY FORWARD

The TNOGA and regulatory authorities in other states should consider introducing a voluntary approach rather than sticking to imposing stringent restrictions. The legislative objective alone would not suffice if the desired outcome is not attained. States should consider sensitizing people, especially the youth about unhealthy gaming habits and mandate consent-based mechanisms to be implemented by the online game providers so that players have a sense of autonomy while also making informed decisions.

FinTech

SECTION 3



RBI'S EXCLUSIVE DOMAIN INITIATIVE FOR INDIAN BANKS TO ENHANCE CYBER SECURITY

NEWS

RBI has recently introduced the exclusive domain naming system 'bank.in' for Indian banks and 'fin.in' for non-bank financial entities to enhance cyber security in the Indian banking sector. The move aligns with RBI's broader regulatory vision of strengthening the digital financial ecosystem against cyber threats.

LEGAL TALK

RBI aims to mitigate domain spoofing, a common cyber fraud where malicious actors create deceptive domain names resembling genuine bank websites by creating a centralized and verifiable domain space. These exclusive domains will provide a unique digital identity, making it easier for users to recognise legitimate platforms. Through exclusive domain names, RBI aims to enhance consumer protection by reducing the risk of phishing scams and other cyber frauds. It mandates banks and other institutions to register with the Institute for Development and Research in Banking Technology ('**IDRBT**'). However, the registrations would be restricted to only legitimate financial institutions, which would significantly reduce digital fraud targeting customers. Further, by mandating financial entities to operate under these verified domains, RBI aims to strengthen consumer trust and uphold transparency in digital banking services. The failure to comply with secure domain usage may result in regulatory penalties and increased scrutiny, which reinforces the need for banks and NBFCs to prioritize consumer data protection and cyber hygiene measures.

THE WAY FORWARD

The introduction of '.bank.in' is expected to significantly strengthen India's digital banking security framework by reducing cyber threats and reinforcing customer trust in online banking services. Additionally, fintech firms and payment service providers collaborating with banks may also need to align with this security standard, further tightening India's digital financial infrastructure. Through this, customers can expect a safer, more transparent, and fraud-resistant banking experience, reinforcing India's commitment to a resilient and secure digital financial system.

SEBI INTRODUCES AI COMPLIANCE FRAMEWORK FOR MARKET INTERMEDIARIES

NEWS

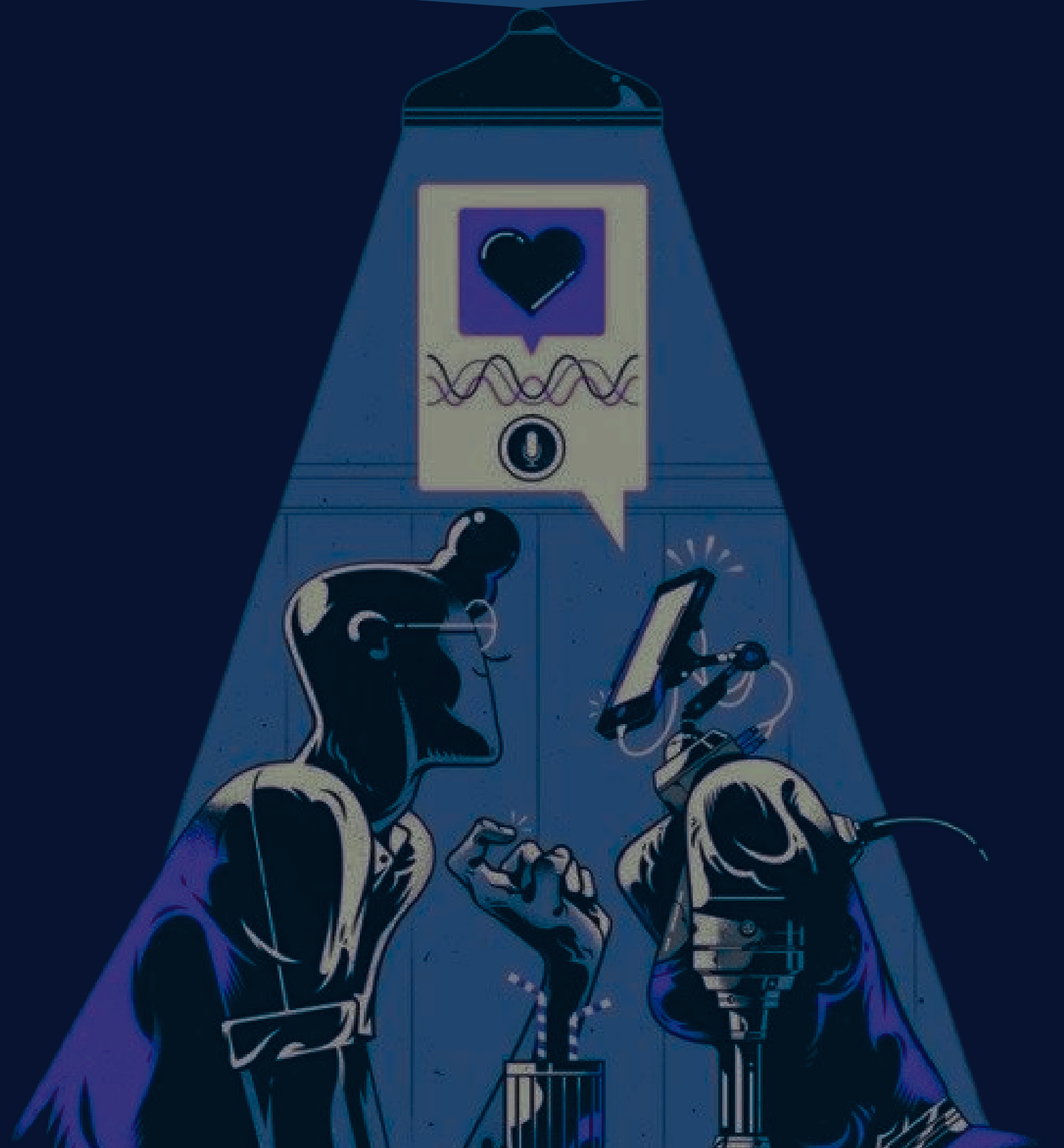
On February 10, 2025, the Securities and Exchange Board of India ('**SEBI**') notified the Securities and Exchange Board of India (Intermediaries) (Amendment) Regulations, 2025, amending the Securities and Exchange Board of India (Intermediaries) Regulations, 2008. This amendment introduces key provisions outlining the responsibilities of SEBI-regulated entities that employ artificial intelligence ('**AI**') and machine learning ('**ML**') tools and techniques.

LEGAL TALK

The amendment applies universally—irrespective of whether AI/ML tools are developed in-house or sourced from third parties, and regardless of their extent of use in business or investor services. This broad applicability ensures there are no regulatory gaps, subjecting all AI/ML deployments to scrutiny and accountability. These entities must also implement stringent measures to protect the confidentiality and integrity of investors' and stakeholders' data. They must implement strict measures to protect investor and stakeholder data, especially when held in a fiduciary capacity. Further, the regulations also compel firms to prevent data manipulation at every stage of processing, aligning with global data protection principles similar to those found in privacy frameworks such as the European Union's General Data Protection Regulation 2018 ('**GDPR**'). This mandate raises the level of responsibility for entities using AI/ML, making these systems not just operational tools but legally accountable parts of risk management. Entities are required to assume full responsibility for the outcomes produced by AI/ML systems, meaning that they are required to continuously validate AI outputs to ensure accuracy and reliability, mitigating risks of inaccurate or biased decisions. Additionally, the amendment ensures that accountability cannot be outsourced merely by contracting third-party technology providers. The end-user firm remains liable for any adverse effects resulting from the algorithm's decisions. This marks a regulatory shift by holding users accountable for AI-driven decisions, rather than the technology itself, ensuring AI remains transparent and does not operate as an unchecked "black box" in financial decision-making. Beyond technical compliance, firms must ensure AI/ML adoption aligns with securities laws, market conduct rules, and cybersecurity regulations. Lastly, the regulations necessitate the development of internal governance frameworks specifically tailored to AI/ML such as periodic audits and assessments of AI systems to ensure compliance and equipping personnel with essential expertise to manage and oversee AI-driven processes.

THE WAY FORWARD

While these regulations may increase compliance costs, they enhance market credibility and investor trust. By setting a strong AI governance framework, SEBI ensures transparency, accountability, and responsible innovation in financial markets. The amendments under Regulation 16C introduce a high standard for data governance, accountability, and legal compliance in AI/ML-driven processes. By mandating strict oversight and proactive risk management, SEBI aims to protect investor interests while fostering innovation within a structured regulatory framework. This balanced approach is essential to maintaining market integrity as financial ecosystems continue to embrace AI and digital transformation.



UAE INTRODUCES DRAFT REGULATIONS FOR TOKENIZED ASSETS INTEGRATING BLOCKCHAIN AND FINANCIAL MARKET

NEWS

The United Arab Emirates Securities and Commodities Authority ('**SCA**') has released a draft regulation focusing on security tokens and commodity token contracts, providing clear legal definitions and frameworks for these digital assets. The draft regulations regulate the offering, issuance, promotion and registration of securities and commodity contracts on distributed ledger networks.

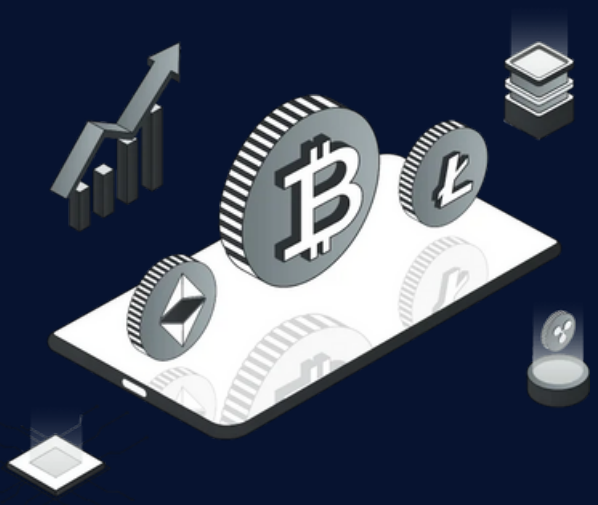
LEGAL TALK

The draft regulation delineates security tokens as digital representations of traditional securities, such as equities or bonds, and commodity token contracts as digital forms of physical commodities like gold or oil. Under the regulations, these tokens are treated as contractual rights exercised, traded, and transferred exclusively through distributed ledger technology ('**DLT**'). The regulations set minimum technical standards for DLT to ensure transparency and integrity, requiring issuers to record the content of token rights and registration agreements on the blockchain. Article 9 of the draft regulation mandates that issuers of security tokens and commodity token contracts disclose financial risks and undertake due diligence to protect investors. The framework under article 6(3) clarifies that in case of a conflict between the blockchain (contract owner) and the token issuer, the blockchain's claim takes precedence, ensuring a decentralised and trust-based enforcement mechanism. Article 11 also establishes clear rules for trading and settlement, limiting transactions to licensed exchanges or SCA-recognized Alternative Trading Systems ('**ATS**'), with over-the-counter trading restricted to bonds and sukuk tokens. The draft regulation reflects the UAE's strategic intent to balance innovation with investor protection by embedding blockchain technology within a clear legal framework.

Its structured approach demonstrates a forward-looking stance, ensuring the integration of digital assets does not erode the core principles of financial market regulation. Investor protections are central to the framework, aligning digital securities with traditional financial markets. Token issuers must provide disclosures on token structures, financial risks, and compliance status, while token holders receive legal rights equivalent to those of traditional securities investors. These safeguards reinforce transparency and regulatory oversight in digital asset markets. In India, tokenised assets, including security and commodity tokens, currently lack a dedicated legal framework akin to the UAE's draft regulations. While securities are regulated by SEBI under the Securities Contracts (Regulation) Act, 1956, and virtual digital assets ('**VDAs**') fall under the purview of the Income Tax Act post the 2022 Union Budget, there is no formal recognition of security tokens or commodity token contracts. Unlike the UAE's clear rules on trading venues and blockchain-based enforcement, India's approach remains fragmented, with regulatory uncertainty surrounding the intersection of blockchain technology and traditional financial instruments.

THE WAY FORWARD

The new framework eliminates ambiguities by explicitly defining digital securities and setting dedicated compliance requirements. With a strong emphasis on investor protection, the draft regulations provide much-needed clarity and establish a structured approach to integrating digital assets into the UAE's financial system. Given that the time frame for comments for the draft has expired, it is expected that the final regulations will consider the interests of all parties involved.



ARTIFICIAL INTELLIGENCE

SECTION 4

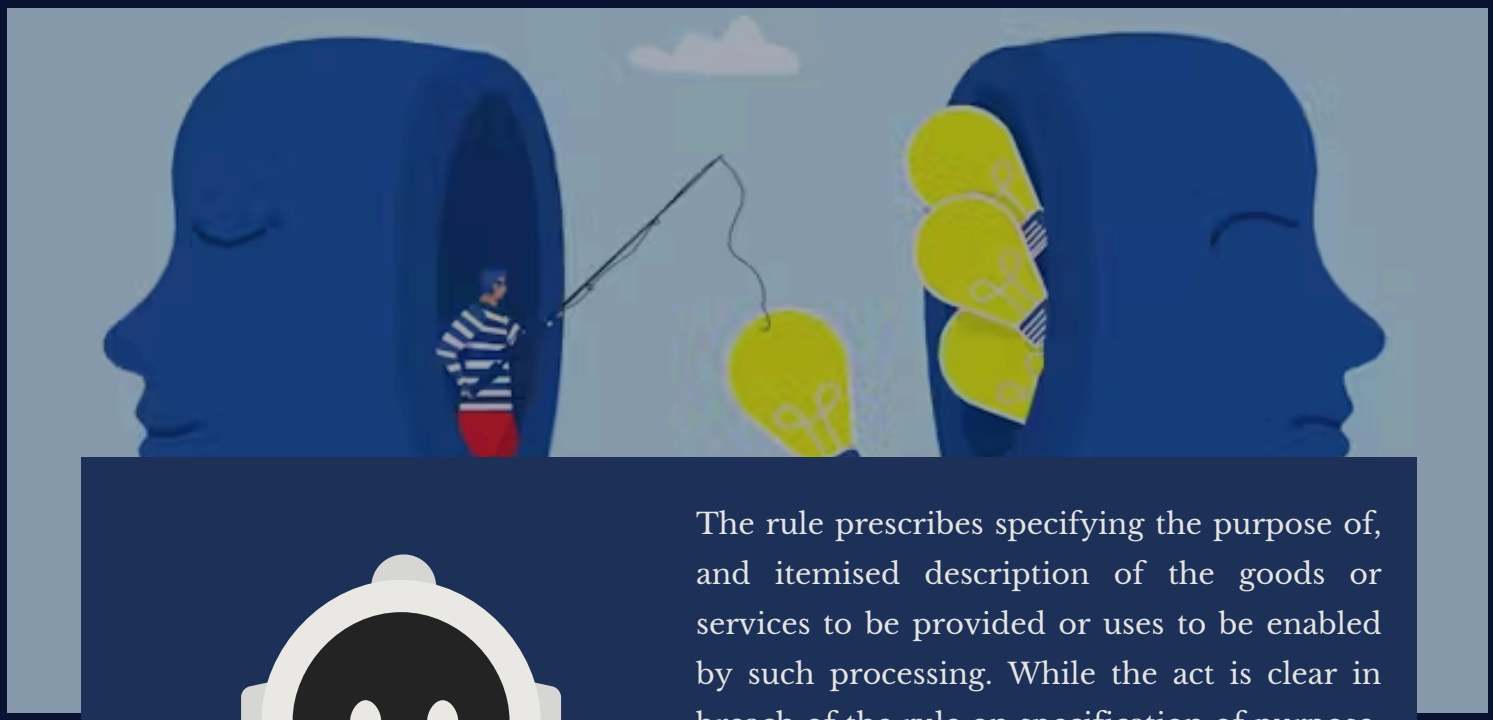
INDIAN SLUMBER ON DEEPSEEK; A CALL FOR URGENT ACTION

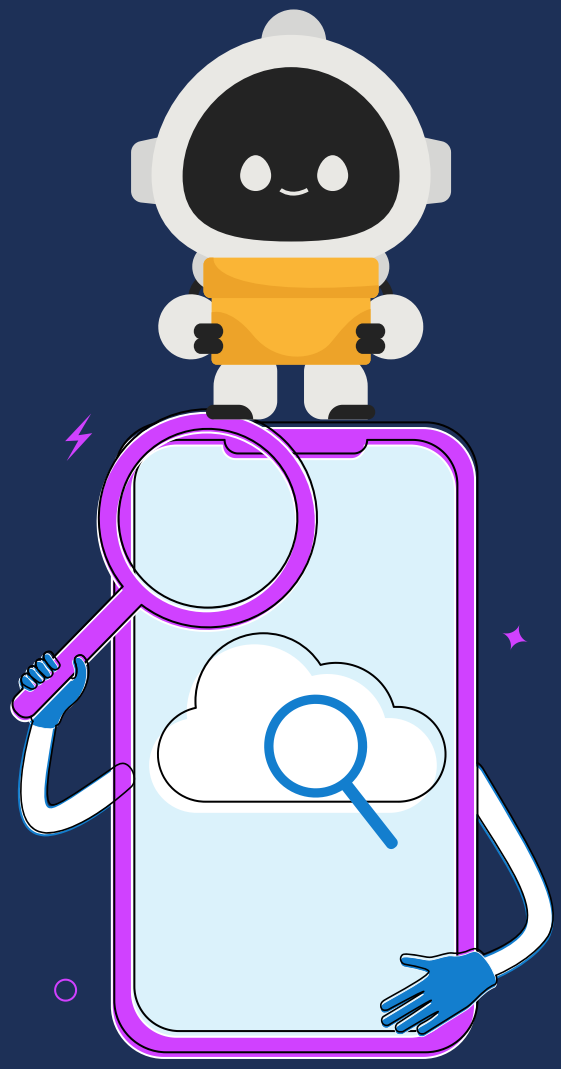
NEWS

In a recent development the Delhi High Court took cognizance of a Public Interest Litigation concerning the privacy issues that operations of Deepseek AI may cause in India. The app collects data in three forms- 'user prompts' (including images, documents, chat history), 'automatically collected information' (device data, metadata of other applications, cookie tracking) and information from 'other sources' (crowdsourced or publicly available data).

LEGAL TALK

The court, while commenting on the general risks associated with Gen-AI directed the government to file a response to understand the course of action they seek to adopt. The government on the other hand is also not alien to this threat and has already started scrutiny of the function of the Chinese controlled application that is causinge market disruptions in the world of AI. The Indian government has tasked the Computer Emergency Response Team (CERT-In) under the aegis of Ministry of Electronics and Information Technology, to undertake an enquiry of potential harms by tracking user behaviour and data storage mechanisms. While the concerned PIL states multiple violations of the current Indian data protection regime, it is also important to understand the violations in the light of the new Digital Personal Data Protection Rules of 2025 (**'DPDP Rules'**), which reflect international standards of data protection and resonate with Indian legislative intent. While the rules are not in force yet, this occurrence makes further case for quick and informed implementation of these rules. The Rule 3 under DPDP Rules talks about the notice that the data fiduciary has to give to a data principal. In this case the data fiduciary is Deepseek and the users are the data principals.





The rule prescribes specifying the purpose of, and itemised description of the goods or services to be provided or uses to be enabled by such processing. While the act is clear in breach of the rule on specification of purpose, currently at the nascent stage that they are operating, seeking device data and other personal data is inconsequential for any other purpose than behavioural monitoring, which can bring us to the issue of child safety but this is a never-ending spiral as the app continues its unregulated operations. Operation of the app is also a cause of concern in the light of national safety issues involved. The DPDP Rules under its rule 14 envisions a framework wherein data processing outside of India would only be enabled by compliance with the state induced framework. This has become a major security requirement in the digital age as many of the government servers also operate on software provided by foreign data fiduciaries and any lapse may be prejudicial to national security.

THE WAY FORWARD

Foreign governments have already started taking actions against the operations of AI, with certain nations prohibiting the operations to others restricting the same to civilian data. Urgent action by the government is crucial in addressing the privacy and security risks posed by Deepseek. Immediate regulatory measures can prevent unauthorized data collection and cross-border transfers, safeguarding national security and user privacy. Swift intervention can also ensure compliance with India's emerging data protection laws, such as the DPDP Rules. This proactive approach will help maintain public trust in digital services while fostering a secure digital environment for all users in India. Timely action is indispensable to prevent long-term consequences.

DATA PRIVACY

SECTION 5

CRITICS SAY THE NEW GOOGLE FINGERPRINTING POLICY PUTS PROFITS OVER PRIVACY

NEWS

Google's new policy of browser fingerprinting has raised eyebrows among the data privacy experts who critique it as a blatant disregard for user privacy. Google says that the way people use the internet has changed, and thus it was pertinent to bring in this change, which has been implemented by many other companies, retracting its earlier statement that it subverts user choice and is wrong.

LEGAL TALK

Browser fingerprinting is a tracking method that efficiently replaces cookies. It allows online advertisers to collect data about users, including their IP addresses and real-time information about their devices like timezone, browser type, etc. This change complicates users' ability to manage the data collected about them. There are privacy concerns regarding this, as browser fingerprints are capable of tracking the users online movements such that even if the user moves from one website to another, the advertiser would be able to distinguish their activity discreetly without the knowledge of the users. Through this data collection, the online advertiser would be able to tailor their offerings and create unique user profiles. Since fingerprinting is used for tracking individuals, it spontaneously falls under the category of personal data processing and therefore comes under the ambit of Article 5 of GDPR and Sec. 4 of the DPDP Act, 2023. Both these laws emphasize lawfulness, fairness, and transparency in data processing. Therefore, before implementing this change, Google has to ensure that it is complying with these principles. The problem with this is that browser fingerprints cannot be managed as easily as cookies, which can be deleted or blocked by the user and are manageable through browser settings; conversely, fingerprints operate in the background and collect data about a user's online behavior. This is a threat to the principle of fairness and transparency. Google should also go through the balancing test wherein it could verify for itself if it's new policy of tracking users would override their fundamental rights, primarily privacy and whether it is in consonance with the expectations of the data subjects and clearly lay out its legitimate interest argument to the users and most importantly share detailed information (scope, purpose, legal basis of processing) with the user who would be subject to such fingerprinting. Lastly, the consent of the users is a mandate.

THE WAY FORWARD

To address fingerprinting concerns, websites should adopt transparent data collection disclosures, obtain explicit user consent (revocable at any time), and offer granular control over data sharing. Privacy-enhancing technologies ('**PETs**') should be developed and implemented to minimize identifiable data exposure. Finally, user education and awareness campaigns are crucial to empower individuals to protect their online privacy.

CONTRIBUTORS

WRITERS

ANJALI PANDE

PRATYUSH SINGH

SUBHASIS SAHOO

ANUSHKA GUHA

ANANYA SONAKIYA

ARUNIMA RAMAN

KALYANI KIRAN

BHAVYA BHASKAR

ALOK SINGH MOURYA

EDITORS

HARSH MITTAL

LAVANYA CHETWANI

DESIGNERS

TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL