LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

JANUARY 2025 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

सत्ये स्थितो धर्म

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

BUREAU OF INDIAN STANDARDS RELEASES DRAFT PRINCIPLES AND GUIDELINES FOR E-COMMERCE SELF-GOVERNANCE

NEWS

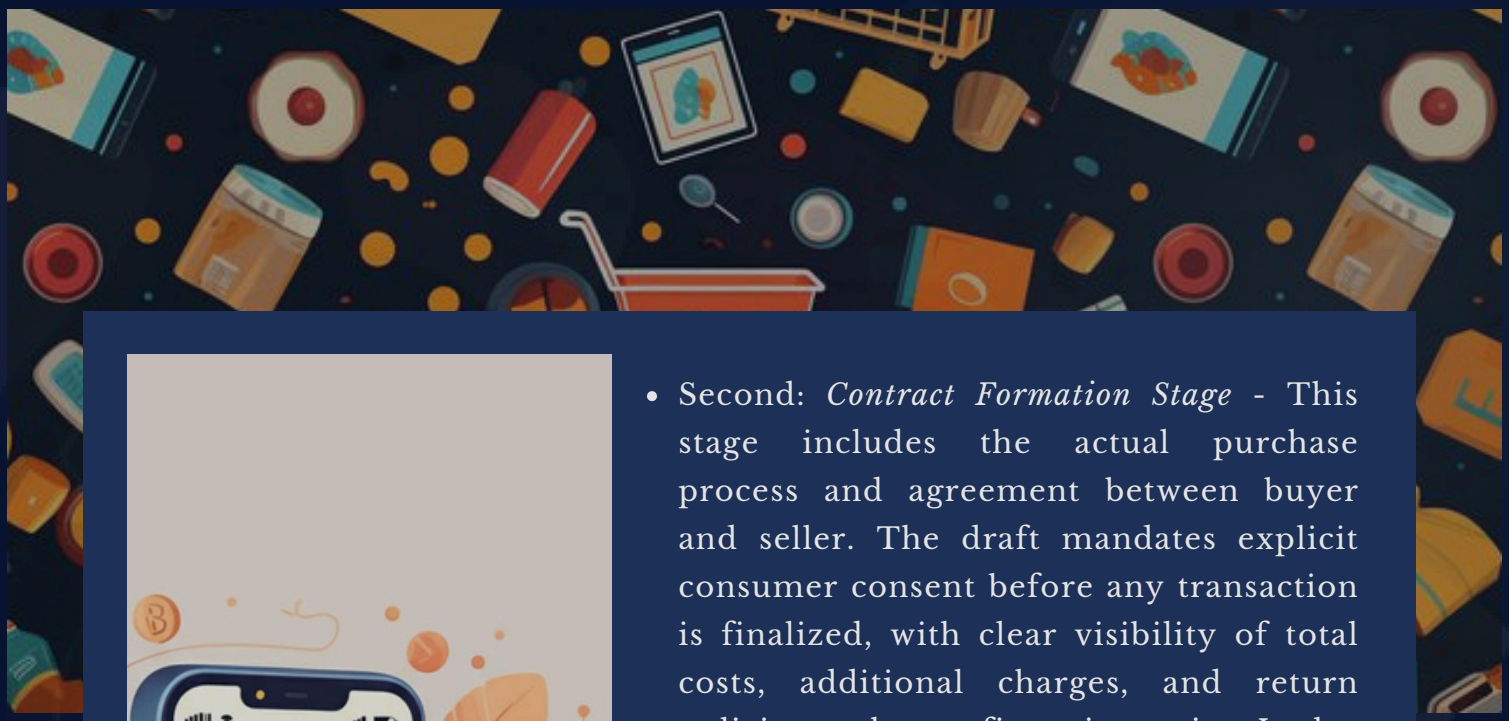
The Bureau of Indian Standards ('**BIS**') has released a draft proposal for self-governance in e-commerce, aiming to promote transparency and consumer protection. The draft guidelines set out principles applicable to different stages of e-commerce transactions, including pre-transaction, contract formation, and post-transaction, along with general self-governance norms. The framework emphasizes fair business practices, explicit consumer consent, and compliance with data protection laws, marking a significant step in regulating India's growing e-commerce sector.

LEGAL TALK

The draft guidelines align with existing consumer protection laws, particularly the Consumer Protection Act, 2019, which governs unfair trade practices as defined under Section 2 (47) and consumer rights in e-commerce. Data privacy obligations under the guidelines ensure compliance with the Digital Personal Data Protection Act, 2023, mandating that personal data be used strictly for transactional purposes. Additionally, the obligation for explicit consumer consent for marketing communications strengthens protection against unsolicited commercial messages under existing telecom and IT regulations. These provisions collectively aim to create a fair and accountable e-commerce ecosystem, ensuring that platforms operate with consumer interests at the forefront.

The draft guidelines break down the e-commerce transaction process into three stages:

- First: *Pre-Transaction Stage* - This stage covers all interactions before a purchase is made, including product discovery, seller verification, and information disclosure. Platforms are required to implement diligent KYC verification for sellers, ensuring they meet compliance standards. Additionally, they must facilitate detailed product descriptions, including price breakdowns, safety warnings, return policies, and customer reviews, so that consumers can make informed decisions.



- Second: *Contract Formation Stage* - This stage includes the actual purchase process and agreement between buyer and seller. The draft mandates explicit consumer consent before any transaction is finalized, with clear visibility of total costs, additional charges, and return policies at the confirmation point. It also stresses the need for a transparent and accessible cancellation, return, and refund mechanism, especially for cash-on-delivery transactions.

- Third: *Post-Transaction Stage* - Once a purchase is completed, platforms must ensure consumer protection through clear timelines for refunds, replacements, and exchanges. Additional safeguards against counterfeit products must be in place, along with a robust grievance redressal mechanism compliant with the Consumer Protection Act, 2019. Platforms are also required to provide timely delivery notifications and take responsibility for third-party logistics services.

THE WAY FORWARD

While the BIS draft presents a strong foundation for self-regulation, several aspects require further refinement. The implementation of KYC requirements for third-party sellers could be standardized to prevent excessive compliance burdens while maintaining due diligence. Furthermore, the enforcement of transparency norms, such as unbiased search rankings and fair treatment of sellers, should be backed by an appropriate grievance redressal mechanism. To enhance consumer protection, mandatory dispute resolution mechanisms should be included, ensuring quicker resolutions in case of grievances. The regulatory framework must also provide clear penalties for non-compliance to ensure accountability among e-commerce players.

PRESIDENT TRUMP INTERVENES TO PAUSE THE BAN ON TIKTOK: BYTEDANCE ORDERED TO DIVEST OR FACE SHUTDOWN

NEWS

The Supreme Court of the United States ('SCOTUS') upheld a law banning the Chinese-owned social media app TikTok. Although the ban was set to begin on January 19, President Trump granted a 75-day extension for TikTok to comply with a law mandating its sale or ban. This ruling would have significant implications for the approximately 170 million TikTok users in the US, many of whom rely on the app for entertainment, connection, and creative expression.

LEGAL TALK

The SCOTUS upheld the Protecting Americans from Foreign Adversary Controlled Applications Act ('Act') while rejecting TikTok's appeal. The Act, enacted on April 24, 2024, mandates that ByteDance, TikTok's Chinese parent company, must divest its US operations within nine months or face a ban. TikTok would be prohibited from functioning in the US unless ByteDance completes a qualified divestiture, ensuring no control or relationships with foreign adversaries. The Act classifies TikTok as a foreign adversary-controlled application due to ByteDance's ownership, preventing its distribution, maintenance, or updates in the US without divestiture. Failure to comply will result in penalties for service providers like Apple and Google, leading to a gradual degradation of the app until it becomes unusable. The law is a response to national security concerns regarding Chinese access to sensitive user data, which could be exploited for surveillance or influence campaigns. Previous attempts by the Trump Administration to regulate TikTok, including a failed executive order, prompted Congress to pass the Act amid escalating scrutiny of foreign data-handling practices.

It is pertinent to recall that India was the first country to issue a nationwide ban on TikTok in June 2020, alongside 58 other apps, following a border conflict with China. The Indian government invoked its authority under Section 69A of the Information Technology Act, 2000 ('**IT Act**') to block applications that posed potential risks to national security. Notably, ByteDance did not contest this ban in Indian courts. Section 69A of the IT Act authorizes the Central Government or its authorized officers to block public access to information deemed necessary for national sovereignty, defence, security, friendly foreign relations, and public order or to prevent incitement to cognizable offences. However, such an action requires a written order detailing the reasons for the block, and the blocking procedure must adhere to prescribed safeguards.

For this situation, the SCOTUS justified the speculative ban by emphasizing the necessity for policymakers to anticipate future developments, even in the absence of complete empirical evidence. With no sale in sight, TikTok's final legal battle failed on Friday when the Supreme Court ruled that the regulation does not violate the First Amendment. Unlike India, the US approach allows for negotiation as ByteDance has been given time to comply with divestiture requirements before enforcement of the ban.

THE WAY FORWARD

The SCOTUS judgment has been criticized as a low point for the First Amendment. The ruling establishes a dangerous legal precedent, allowing governments to censor speech on platforms by alleging national security concerns. India had also justified its ban, affecting approximately 200 million users, on grounds of privacy and national sovereignty. However, the anticipated backlash from Indian users was minimal; while content creators in rural areas lost significant traffic, domestic alternatives to TikTok struggled to gain traction. In contrast, US platforms like Instagram and YouTube benefited from increased Indian users post-ban. A potential US TikTok ban could limit the flow of user data to China, but TikTok has denied claims of data mishandling and has proposed strict data governance measures.

The TikTok ban presents significant implications for media freedom in the global sphere. Other governments may attempt to control speech on Facebook, X, and YouTube by presenting their speech restrictions as simply a matter of 'ownership' by American businesses. The precedent of potentially banning a platform based on ownership rather than content raises essential questions about the future of digital media. These instances illustrate a fundamental challenge in modern governance: balancing security interests with the preservation of open communication channels. A more practical solution involves creating a comprehensive legislative framework that establishes rigorous standards for data privacy, algorithms, and content moderation applicable to all social media platforms, both domestic and foreign. Such legislation would render debates about TikTok moot, compelling all companies to comply with local laws—an idea that remains elusive in the US but could be more feasible in India.

FinTech

SECTION 2

RBI ISSUES NEW GUIDELINES ON PREVENTING FINANCIAL FRAUDS VIA VOICE CALLS AND SMS

NEWS

The Reserve Bank of India ('RBI') has issued stringent guidelines aimed at combating the rising tide of financial fraud associated with mobile numbers in digital transactions. This initiative comes in response to the increasing exploitation of mobile numbers for fraudulent activities, particularly through voice calls and SMS.

THE WAY FORWARD

The implementation of these guidelines is a critical step towards securing India's digital financial ecosystem. It is required that financial institutions prioritise compliance efforts by investing in technology and training personnel to adhere to the new protocols effectively. Close cooperation between banks and telecom operators will be essential for maintaining accurate records in the MNRL and ensuring that fraudulent numbers are promptly revoked. It is also required to conduct regular audits and establish monitoring mechanisms within financial institutions to assess compliance with these guidelines.

LEGAL TALK

As per the guidelines issued, the Regulated Entities ("REs") are required to utilise the Mobile Number Revocation List ('MNRL'), developed by the Department of Telecommunications ('DoT'), to ensure their customer databases are free from invalid or deactivated mobile numbers. As a database of potential harm-causing individuals, this list will help in tracking and revoking access linked to such numbers. This measure helps prevent unauthorized access and enhances fraud detection by tracking numbers associated with potential threats. Further, the entities must also develop Standard Operating Procedures ('SOPs') for updating the registered mobile numbers ('RMN') after verification and monitoring accounts linked to revoked numbers. This would ensure that the accounts linked to these revoked mobile numbers are not constantly monitored and not misused as Money Mules in cyber fraud. The guideline also mandates businesses to streamline their communication practices as per Telecom Regulatory Authority of India ('TRAI') regulations. It requires transactional/service calls to exclusively use the '1600xx' numbering series and promotional voice calls to be routed through the '140xx' numbering series. By mandating distinct numbering series for transactional/service calls and promotional voice calls, the guideline enforces transparency in communication practices which helps the customers to easily identify the nature of incoming calls by differentiating the legitimate communications from fraudulent ones. It improves transparency, allowing customers to differentiate legitimate communications from fraudulent ones. Additionally, businesses must adhere to the "Important Guidelines for sending commercial communication using telecom resources through Voice Calls or SMS" ensuring compliance with TRAI. Compliance with TRAI's guidelines for commercial communication via calls and SMS ensures that businesses maintain lawful communication practices, reducing spam and fraudulent activities. Under the guidelines, financial institutions are also tasked with enhancing customer awareness regarding these new measures through various communication channels, including emails and SMS in regional languages. These guidelines enhance the security of digital transactions and protect consumers from fraud.

EU INTRODUCES DORA REGULATIONS TO STRENGTHEN DIGITAL RESILIENCE IN FINANCIAL SECTORS

NEWS

The European Union has implemented the Digital Operational Resilience Act ('DORA') to enhance cybersecurity and ensure the financial sector's stability against technological disruptions and cyber threats. Covering banks, insurers, payment providers, and key third-party vendors, DORA aims to unify the EU's digital risk management approach amid growing reliance on technology.

LEGAL TALK

DORA establishes a comprehensive framework for managing digital risks, filling gaps left by existing financial laws like Second Payment Services Directive ('PSD2') and General Data Protection Regulation ('GDPR'). Its key provisions focus on mandatory IT system testing, incident reporting, and third-party oversight. The regulation aims to address systemic risks arising from the heavy reliance on a few key service providers, where a single vulnerability, as demonstrated by the global CrowdStrike-Microsoft IT outage, can trigger widespread disruptions.

DORA consolidates and elevates ICT risk management across the EU, mandating organizations to adopt stringent measures such as resilience testing, robust risk management frameworks, and prompt incident reporting. Institutions must regularly test their digital infrastructure, manage risks associated with third-party providers, and enhance information-sharing mechanisms to mitigate cybersecurity threats. Critical service providers must register with EU authorities and comply with oversight requirements, ensuring accountability.

-Member States are responsible for enforcement and can impose significant penalties, including personal liability for senior management in cases of non-compliance. DORA's binding nature requires uniform implementation across the EU, but its broad scope also impacts entities outside the financial sector that serve regulated firms.

Although DORA does not directly apply to the UK, its principles align with the UK's operational resilience rules, which require firms to identify critical services, establish impact tolerances, and conduct scenario testing. Recent penalties, such as the fine imposed on TSB for IT governance failures, emphasize the importance of compliance.

The European Supervisory Authorities (ESAs) will enforce these measures, collaborate with national regulators, and maintain a centralized database of digital incidents for better cross-border analysis. DORA's extraterritorial scope ensures that even non-EU-based providers serving EU institutions must adhere to these standards.

THE WAY FORWARD

For organizations under DORA, aligning existing systems with their requirements will be a substantial undertaking, involving gap analyses, contract updates, and enhanced training. While challenging, the regulation is expected to strengthen trust and set a global benchmark for operational resilience in an increasingly interconnected financial ecosystem.

STREAMLINING OF CRYPTO REGULATIONS WITH MICA TAKING FULL EFFECT

NEWS

The European Union ('EU') has ushered in a new era of cryptocurrency regulation with the Markets in Crypto-Assets Act ('MiCA'), which becomes fully enforceable on December 30, 2024. This landmark legislation provides a unified framework across the EU's 27 member states, fostering innovation while ensuring security and transparency in the crypto asset space.

LEGAL TALK

MiCA is a comprehensive regulatory framework introduced by the EU to address the growing crypto market across its states. It aims to provide a unified approach, simplifying compliance for crypto-asset service providers ('CASPs') like exchanges and custodial services. MiCA covers various types of crypto assets, including Electronic Money Tokens ('EMTs') and Asset-Referenced Tokens ('ARTs'), with a focus on investor protection, market stability, and the prevention of illegal activities like money laundering and terrorist financing. By establishing clear regulatory guidelines, MiCA seeks to promote innovation while ensuring the safety and transparency of the crypto ecosystem. Before MiCA, the EU's crypto industry faced fragmented regulations, requiring businesses to obtain multiple licenses to operate. MiCA resolves this by introducing a unified licensing framework, aligned with existing financial regulations. Its goals include protecting investors, preventing market manipulation, combating illegal activities like money laundering and terrorism financing, and creating a safer, more transparent crypto market. It ensures that CASPs adhere to strict compliance standards, including Anti-Money Laundering ('AML') and Counter-Terrorist Financing ('CTF') measures. Moreover, MiCA defines crypto assets as digital representations of value or rights stored and transferred using distributed ledger technology ('DLT'). It classifies crypto assets into three categories, EMTs, ARTs, Other Crypto Assets. However, MiCA does not automatically regulate non-fungible tokens ('NFTs'), but NFTs may be subject to its rules if they exhibit certain characteristics, such as being issued in large series or functioning similarly to utility tokens or financial instruments. For instance, fractionalized NFTs, where ownership is divided into multiple tokens, may require MiCA authorization. MiCA does not apply to fully decentralized platforms, such as Decentralized Autonomous Organizations ('DAOs'), Decentralized Finance ('DeFi') projects and Decentralized Applications ('dApps'). However, defining decentralization can be complex. Projects offering interfaces to EU users may still need to comply with MiCA, and businesses should seek legal advice to ensure compliance. Exploring strategies like progressive decentralization or governance minimization may be necessary for compliance.

Furthermore, MiCA regulates a wide range of businesses, CASPs, which must comply with its requirements. These entities include but are not limited to Custodial Wallets, Exchanges, EMT or ART Issuers. These entities must adhere to strict operational and compliance standards under MiCA to maintain security and consistency in the EU's crypto market. Another thing about MiCA is Tokenization, i.e., a transformative aspect of crypto assets, where a physical or digital asset (like fiat currency, gold, or real estate) is represented on a blockchain. This enables faster payments, better integration with digital wallets, and enhanced security. Stablecoins are a major focus under MiCA, and they are designed to maintain a stable value by being pegged to real-world assets like fiat currencies or commodities. Stablecoins offer secure, transparent, and fast transactions. Their efficiency is further enhanced by smart contracts, which enable automated payments when predefined conditions are met. This revolutionizes payment systems, reducing delays and ensuring reliability.

THE WAY FORWARD

MiCA offers a comprehensive and unified regulatory framework for the crypto industry, setting a global standard with clear guidelines for crypto-assets like stablecoins and tokenized assets. It contrasts with India's fragmented regulatory approach, where various bodies such as the RBI and SEBI provide inconsistent and sometimes conflicting guidelines. MiCA mandates stringent AML and CTF measures, creating a secure and transparent environment for CASPs, a feature India lacks in its current regulatory setup. Additionally, MiCA's specific regulations for stablecoins and tokenized assets stand in stark contrast to India's lack of clarity on these areas. While MiCA excludes decentralized platforms like DAOs, DeFi, and dApps from direct regulation, this nuanced approach could inspire India to consider the evolving nature of decentralization. In conclusion, MiCA provides a clear regulatory roadmap, whereas India's crypto regulation is still in need of a more consistent and cohesive framework. India could benefit from adopting MiCA's principles to define crypto-assets, establish compliance standards, and regulate both stablecoins and decentralized platforms, fostering innovation while protecting consumers.

ARTIFICIAL INTELLIGENCE

SECTION 3

MEITY'S SUBCOMMITTEE REPORT ON AI GOVERNANCE GUIDELINES DEVELOPMENT

NEWS

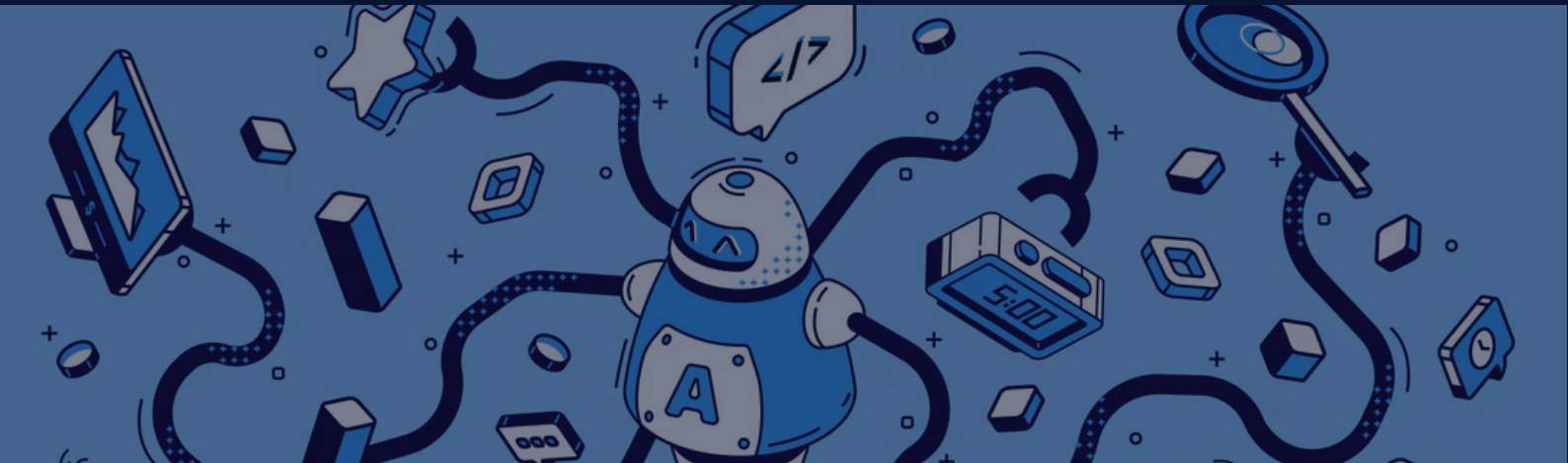
On January 6, 2025, a subcommittee established by the Ministry of Electronics and Information Technology ('**MeitY**') released a report titled "AI Governance Guidelines Development" for public consultation. This report is part of a larger initiative led by the government aimed at tackling the need for a unified, whole-of government approach to ensure compliance and effective governance as the global AI ecosystem continues to expand.

LEGAL TALK

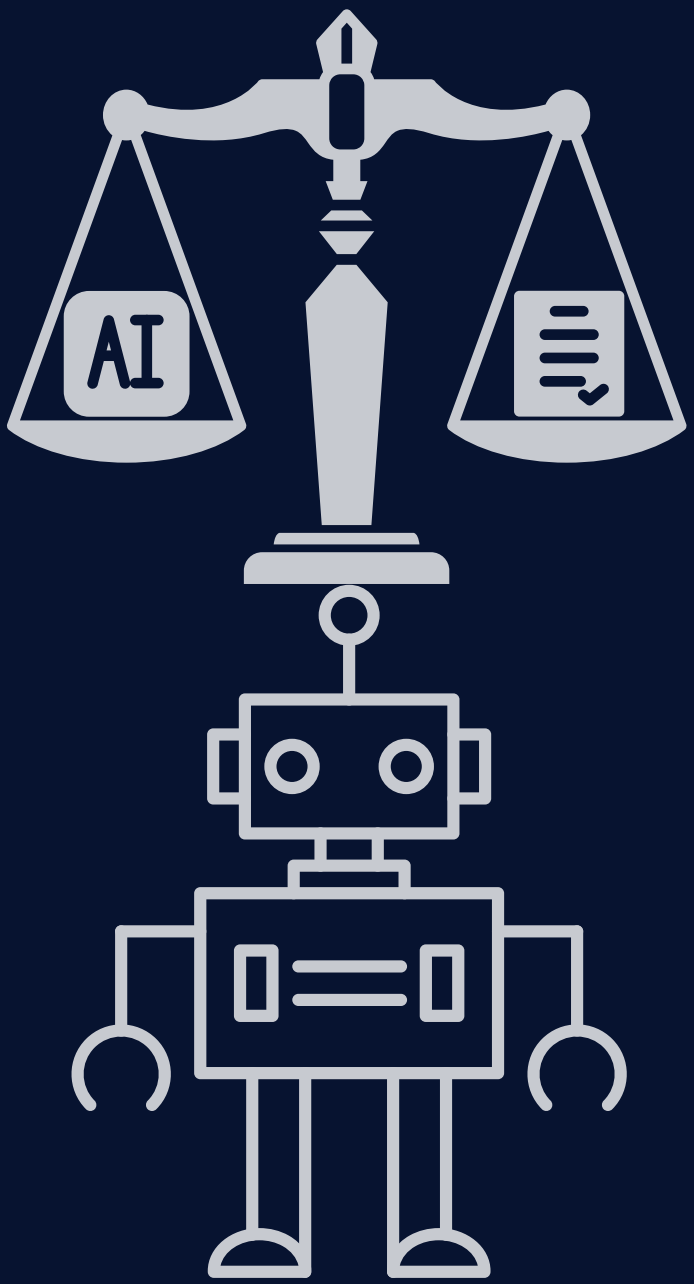
The AI Governance Principles focus on ensuring transparency, accountability, safety, privacy, fairness, and human-centred values in the development and use of AI systems. They emphasize inclusivity, sustainable innovation, and the integration of digital-by-design governance to address risks effectively. To implement the same, the report recommends three main approaches, namely:

- **Lifestyle Approach:** This emphasises managing risks at every stage of an AI system's existence. During the **development stage**, risks related to designing, training, and testing AI systems are identified and mitigated. The **deployment stage** focuses on overseeing the operational use of AI systems to ensure they function as intended and comply with ethical standards. The **diffusion stage** considers the broader societal and cross-sectoral impacts as AI systems are widely adopted, ensuring their long-term consequences are managed responsibly.
- **Ecosystem Approach:** This approach recognizes the interconnected roles of various stakeholders in the AI ecosystem, such as data providers, developers, deployers, and end-users. This avoids focusing solely on individual actors, instead enabling a collective approach to addressing risks and achieving accountability at every stage of AI's lifecycle.
- **Techno Legal Measures:** These integrate technology and regulatory frameworks to ensure effective monitoring, compliance, and risk mitigation. For instance, blockchain tracking can provide traceability for AI-generated content, while AI compliance systems can automate the detection of biases or harmful outputs in real-time, effectively reducing the burden on traditional enforcement mechanisms and creating an environment that fosters self-regulation and shared accountability.

The report also identifies significant gaps in the existing legal and regulatory frameworks, emphasising the need to address them for effective governance. It recognizes that while current laws and regulations like the IT Act, 2000 broadly apply to AI systems, they were not designed with the unique risks and challenges posed by AI in mind. For example, the use of deepfakes, though penalized under current laws, lacks robust mechanisms for detection and prevention.



Another major concern was the absence of appropriate mechanisms and the rapid evolution of AI technology, which often surpass existing regulatory approaches. The report went on to highlight other areas requiring urgent attention such as Intellectual Property Rights, particularly regarding the recent trend of AI systems making use of copyrighted material to train their Large Language Models and defining ownership of AI-generated outputs. Additionally, transparency and accountability mechanisms are weak, with limited tools to trace data, models, and actors throughout the AI lifecycle, hindering the opportunity to attribute responsibility. Finally, a fragmented regulatory approach, with uncoordinated efforts by different bodies, aggravates inefficiencies and leaves these concerns overlooked. Finally, the report went on to provide comprehensive recommendations to strengthen AI governance in India. Key suggestions include:



- **Establish a Whole-of-Government Coordination Mechanism:** This ensures harmonized efforts across regulators and government agencies, aligning with data protection standards under Rule 22 of the Draft DPDP Rules, 2025, which emphasizes collaboration between authorized persons and fiduciaries for data-related purposes, such as addressing national security and sovereignty concerns. However, the success of this initiative depends on inter-agency collaboration, and whether it can withstand the bureaucratic hurdles it may face.

- **Creation of a Technical Secretariat for AI Governance**: A dedicated Technical Secretariat would serve as a coordination hub for the governance group, effectively centralising expertise and enhancing risk management. It would pool multidisciplinary expertise, map India's AI ecosystem, conduct risk assessments, and develop standards and frameworks for responsible AI use.

- **AI Incident Database**: The creation of such a database by the Secretariat would help monitor real-world AI risks, providing a much-needed centralized system for documenting and analysing risks. This aligns with existing data breach notification requirements under Rule 7 of the Draft DPDP Rules, 2025, which requires data fiduciaries to notify affected principals and the Board of any personal data breaches. While advantageous for pattern recognition, concerns over data confidentiality and underreporting could arise without strong safeguards.

- **Encouraging Voluntary Industry Commitments:** Although a pragmatic approach that promotes innovation, industry flexibility, and trust between the regulators and industry players, relying too heavily on self-regulation risks inconsistent implementation and insufficient accountability, necessitating oversight to ensure adherence.
- **Leveraging Technological Solutions for Governance:** This proposal offers innovative ways to trace AI outputs, such as watermarking and labelling. Yet, implementing these tools at scale could pose technical and financial challenges. While platforms like Google DeepMind's SynthID offer watermarking as part of subscriptions or on a per-use basis, making it relatively affordable, such simple watermarks may be vulnerable to tampering. This reflects the need for robust alternatives such as cryptographic signatures, which provide stronger safeguards but are more complex and costly to implement. Additionally, feasibility varies by data type—watermarking images is generally simpler and cheaper compared to text or audio due to their visual nature.
- **Integrating AI-Specific Measures into the Digital India Act:** Finally, this step would strengthen regulatory mechanisms, particularly for grievance redressal and adjudication. However, AI evolves rapidly, and rigid legislative measures risk becoming obsolete, requiring frequent updates or amendments to remain relevant. This could strain administrative resources and slow the regulatory response to emerging risks.

THE WAY FORWARD

To unlock AI's full potential in India, a comprehensive and forward-looking governance framework must be implemented with a focus on trust, accountability, and inclusivity. This requires the adoption of a unified, whole-of-government strategy that bridges existing regulatory gaps through collaboration between policymakers, industry stakeholders, and civil society. Emphasizing transparency, ethical AI development, and regulatory adaptability will be key to fostering innovation while safeguarding public interest. By integrating technological advancements with clear legal frameworks, India can build a resilient AI ecosystem that drives economic growth, enhances public trust, and ensures equitable access to AI-driven opportunities.

“HIGH IMPACT” VS “HIGH RISK”; NOVEL APPROACH ON SOUTH KOREA’S AI BASICS ACT

NEWS

In a recent development, South Korea's National Assembly passed the AI Basic Act (the “Korean Act”, establishing a comprehensive legal framework for artificial intelligence that will take effect in January 2026. This landmark legislation consolidates nineteen separate proposals into a unified attempt aimed at promoting innovation while ensuring ethical standards and safety in AI applications. The Act emphasizes the protection of human rights and dignity, aligning with global trends in AI governance, such as those seen in the EU AI Act. Key features of th AI Basic Act include the creation of a National AI Committee and an AI Safety Research Institute to oversee policy implementtion. The legislation categorizes AI systems based on their risk levels, particularly focusing on "high-impact" applications in critical sectors like healthcare and public safety. It mandates transparency measures, such as labeling generative AI outputs, to mitigate misinformation. By fostering collaboration with private sector players and promoting capacity building within the industry, the South Korean government aims to position the nation as a leader in responsible AI development while enhancing its global competitiveness.

LEGAL TALK

In the context of this law, "high-impact" refers to AI systems that may significantly affect or pose risks to human life, physical safety, or fundamental rights. This classification is akin to the "high-risk" designation in the EU AI Act and encompasses various critical sectors. While the primary focus of the EU “High Risk” applications is towards sensitive areas like biometric identification and critical infrastructure, the Korean Act is focused more on critical sectors such as healthcare, energy supply, and law enforcement. This becomes visible in the specifics of the act. Article 35 of the Korean legislation imposes a duty on businesses incorporating high-impact AI systems into their products or services must endeavour to conduct a prior assessment of the potential impact on fundamental rights of people. For products of services intended for government use, priority must be given to those employing high-impact AI systems that have undergone such impact assessments. This wide use of “High Impact” that is going to significantly affect or pose risks to human life, physical safety, or fundamental rights become important in the light of enhanced variance in uses of AI and technologies that are developing each day. This could be identified as an ideal threshold to be expected out of every organisation basing its functioning on AI. Further, the Korean Act has moved one step further on AI disclaimers than most jurisdictions. Many jurisdictions now require internet businesses like social media apps to put up a disclaimer to the AI generated imagery on the platform. The Korean act, through Article 31, prescribes a transparency requirement where businesses incorporating high-impact or generative AI systems into their products or services must provide users with advance notice that the products or services they provide are AI-powered.

THE WAY FORWARD

In conclusion, South Korea's AI Basic Act establishes a robust framework for regulating high-impact AI systems, emphasizing the need for prior assessments of potential impacts on fundamental rights. The Act's transparency requirements, particularly regarding user notification of AI-generated content, further enhance accountability in AI applications. As AI continues to evolve rapidly, these regulatory measures are essential for ensuring that organizations responsibly harness AI's potential to benefit society.

DATA PRIVACY

SECTION 4

MEITY RELEASES DRAFT RULES OF DPDP ACT FOR PUBLIC CONSULTATION

NEWS

The much anticipated DPDP rules were released by the Ministry of Electronics and Information Technology on 3rd January 2025. The draft rules are open for public consultation. The release of the draft rules affirms the intent of the authorities to take data responsibility and ensure the protection of the digital personal data of citizens. Similar to the Act, the rules also exclusively utilize female-centric pronouns.

LEGAL TALK

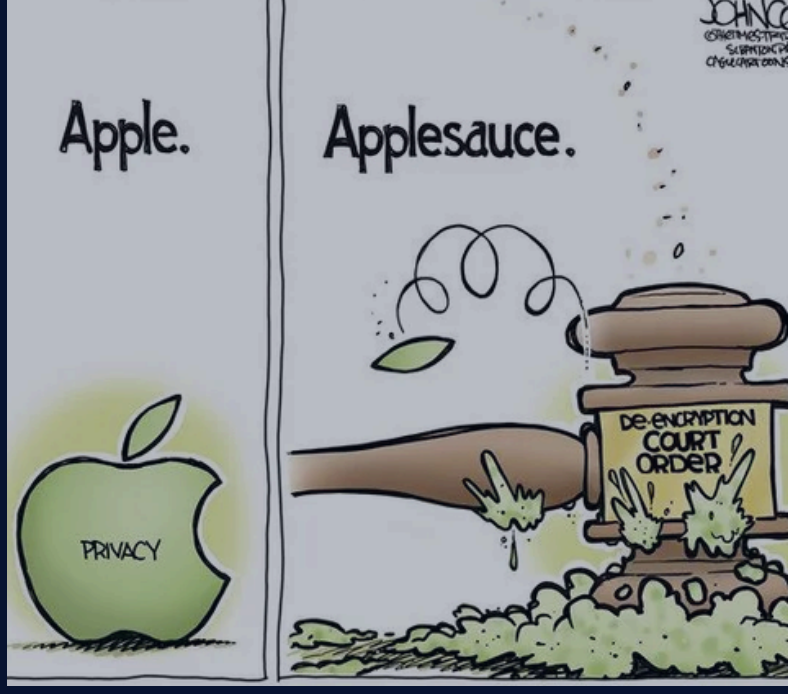
Rule 10 which talks about processing of a child's personal data has created a lot of buzz in the industry as the rule provides only two kinds of scenarios of how it would obtain a parent's consent. If the parent is a user on the Data Fiduciaries platform, then the details that they have already provided will be used to verify the details; if the parent is not a registered user on the platform, then the detail will be obtained through a Digital Locker service provider. The Rule misses out on the aspect that in digital spaces it would be difficult to determine whether the user is a minor or the person providing consent is the parent of the child or not. It would be easier for the child user to input wrong information whose verification is the burden of the platform, this would push these platforms to verify everyone's age. India has high instances of families sharing devices and this verification of everyone's age would result in age-gating and restricting internet access to the users. Moreover to establish parent-child relationship the intermediaries would have to rely on the IDs of the users like Aadhar card or passports which raises concerns with regards to privacy, which is hypocritical in itself.

Rule 14 makes cross-border data transfers harder because there are restrictions on it and if such data has to be transferred then it could only be done through special or general orders of the government. This rule takes a different approach from the Act, as the Act allows such cross-border transfers thereby raising ambiguities. In April last year, USA had enacted the Reforming Intelligence and Securing America Act (RISAA) which compels US-based corporations to share data of foreign citizens with American agencies, since the rules restrict cross-border transfers, American companies operating in India will be distressed. Broad exemptions for state and its instrumentalities, start-ups and significant data fiduciaries has been a major concern ever since the Act came into force. Rule 5 is also silent as to who these bodies would be, what thresholds or requirements they would have to meet to fit into this category, and for how long such exemptions would be applicable. Additionally the terms "sovereignty and integrity of India" and "security of the state" can be interpreted widely but these terms remain undefined in the rules. This leads to lack of checks and balances on the governmental authorities demanding sensitive information. Rule 15 gives exemptions for processing of personal data when it is for the purpose of research, archiving and statistical purpose, this is ambiguous as AI work is mostly statistical, therefore whether AI models which are trained on personal data for research will be exempted from the provisions of the act is unclear.

THE WAY FORWARD

To effectively address the shortcomings with regards to handling of child data, cross-border transfers, and exemptions, there is a need to clearly define vague terms like "sovereignty", and "integrity". The research exemptions should clarify regarding the usage of AI and if such AI based research comes under the ambit of the exemption then a data governance framework for such research must be developed. Cross-border transfer rules must align with the Act to avoid putting pressure on social media giants who are crucial for India's growth in the digital space and to avoid international conflicts. Additionally, to verify the age of a child user, a questionnaire curated to find if a user is a child or an adult could be worked out as a layered authentication mechanism.

APPLE SETTLES SIRI PRIVACY LAWSUIT OVER ACCIDENTAL RECORDINGS



NEWS

Apple agreed to a $95M settlement over claims of Siri recording users without consent, thus violating privacy. Plaintiffs cited unintended recordings triggering ads and whistleblower reports of private conversations being overheard. Apple denied wrongdoing, citing privacy efforts but settled to avoid litigation. Class members may receive up to $20 per Siri-enabled device.

LEGAL TALK

Apple's $95 million settlement in the Siri privacy lawsuit underscores the tension between technological advancement and consumer privacy. The lawsuit alleged that Siri improperly recorded and stored conversations without user consent, raising concerns about compliance with federal and state privacy laws, particularly the California Invasion of Privacy Act 1967("CIPA"). CIPA mandates consent from all parties before recording, making Apple potentially liable if Siri violated this requirement. This case highlights broader legal principles, such as expectation of privacy and informed consent. Privacy laws require transparency in data collection, while regulations like the General Data Protection Regulation 2018 ("GDPR") in the EU emphasize user control and consent. Apple's defence likely centred on Siri's recordings being incidental or necessary for product improvement, whereas plaintiffs argued that such practices violated privacy rights. Apple's decision to settle was a strategic move to avoid prolonged litigation, greater financial exposure, and reputational damage. The $20 per affected device compensation acknowledges the harm but does not admit liability. This also helps Apple mitigate regulatory scrutiny and reinforce its pro-privacy stance. This settlement sets a precedent for regulating AI-driven technologies and strengthens demands for stricter consumer data protection. Ongoing lawsuits against companies like Google may further shape privacy legislation. Future laws may require clearer disclosures, opt-in consent for recordings, and stronger enforcement mechanisms to prevent misuse of user data. This case underscores the urgent need for comprehensive privacy laws to address AI-driven data collection. A federal data protection law, similar to GDPR, could standardize privacy safeguards. Stricter regulations on transparency, consent, and data handling will be essential as AI continues to evolve. Apple's settlement serves as a warning to tech companies: privacy must remain a priority in innovation.

THE WAY FORWARD

To strengthen consumer privacy, companies must implement transparent data policies, ensuring clear disclosures and explicit opt-in consent for recordings. Stricter compliance with privacy laws like CIPA and GDPR should be enforced, with regular audits and penalties for violations. AI-driven technologies must integrate privacy-by-design principles, limiting data retention and enabling easy user control over stored information. Governments should push for comprehensive federal data protection laws, standardizing privacy safeguards across industries. Consumers must be educated on data rights, and regulators should enhance oversight to prevent misuse. A collaborative effort between tech firms, policymakers, and users is crucial for ethical AI development.

CONTRIBUTORS

WRITERS

ANJALI PANDE

SOUVICK SAHA

ANANYA SONAKIYA

KALYANI KIRAN

SATVIK MITTAL

ARUNIMA RAMAN

ALOK SINGH MOURYA

BHAVYA BHASKAR

SUBASHISH SAHOO

EDITORS

HARSH MITTAL

LAVANYA CHETWANI

DESIGNERS

SAMRIDHI BAJORIA

MAITHILI DUBEY

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL