LEXTECH

INSTITUTION'S
INNOVATION
COUNCIL
(Ministry of Education Initiative)

AUGUST, 2025

MONTHLY NEWSLETTER

**LEXTECH: CENTRE FOR LAW,
ENTREPRENEURSHIP, AND
INNOVATION**

NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

- TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

- ONLINE GAMING & BETTING LAWS

- FINTECH

- ARTIFICIAL INTELLIGENCE

- DATA PRIVACY

TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

PARLIAMENTARY PANEL CALLS FOR STRICTER OVERSIGHT OF SAFE HARBOUR AND OTT PLATFORMS IN CYBER CRIME REPORT

NEWS

The Parliamentary Standing Committee on Home Affairs ("**the Committee**"), in its *254th Report on Cyber Crime – Ramifications, Protection and Prevention* ("**Cyber Crime Report**"), has recommended tighter checks on safe harbour under the IT Act, 2000 and stronger oversight of Over-the-top ("**OTT**") platforms.

ANALYSIS

The Committee's proposals mark a significant moment for India's digital regulation. On safe harbour, it called for amending Section 79 of the IT Act to impose graded penalties on platforms that ignore lawful takedown orders and to mandate registration and local presence of intermediaries. It also recommended compensation for victims harmed by platforms' inaction and periodic review of protections in light of emerging technologies like AI and blockchain. This represents a departure from the constitutional framework set in *Shreya Singhal v. Union of India* wherein the apex court had made clear that intermediaries only acquire "actual knowledge" upon receiving a court order or an order under Section 69A, insulating them from vague or informal government demands.

By contrast, the Committee's recommendation that platforms act on "alerts" or notices from government agencies risks expanding liability triggers beyond judicially vetted orders. This would place intermediaries in a position where over-compliance becomes the rational choice, diluting the carefully drawn boundary of Shreya Singhal. While the Committee insists on retaining judicial oversight in principle, its model effectively introduces executive discretion into the takedown process, undermining due process protections.

On OTT regulation, a similar dilution emerges. Under the IT Rules, 2021, OTT platforms follow a system of self-classification with grievance redressal. The Committee's proposal to create an expert review panel, empowered to set cultural norms and impose penalties, risks transforming a post-facto redressal model into a form of state-led content control. The opposition warned that this framework could extend censorship to news and documentaries, and stressed that funneling vast amounts of content through quasi-certification would create bottlenecks and harm industry viability. Both dissenting notes highlight how the Committee's vision would import a pre-certification logic into the digital ecosystem, eroding the autonomy that self-regulation was designed to preserve.

Taken together, the report's recommendations mark a shift from judicially anchored safeguards toward greater executive and bureaucratic discretion, raising serious questions about free expression in India's digital future.

KARNATAKA BRINGS ALGORITHMIC TRANSPARENCY INTO GIG WORK LAW

NEWS

The Karnataka Assembly passed the *Platform-Based Gig Workers' Social Security and Welfare Bill*, 2025 ("the Bill"). It introduces protections for gig workers, including payout fairness, safer working conditions, and platform accountability. Section 13 requires platforms to explain in "simple language" how automated systems affect fares, ratings, and work assignments. Section 14(2) bars platforms from deactivating workers without a written reason and 14 day notice, except in cases of bodily harm.

ANALYSIS

The Bill is a landmark in India, being the first to bring algorithmic transparency into gig work. For workers who often face sudden deactivations or inexplicable shifts in earnings, provisions on written reasons and disclosure of algorithmic impact provide a baseline of accountability. It signals that platform governance can no longer be left entirely to private contracts and opaque codes. However, the Bill stops short of granting substantive rights. "Simple language" is undefined, making it easy for platforms to comply superficially without truly informing workers. Fines beginning at ₹5,000 are too weak to act as deterrents. The Bill does not grant workers rights to contest or appeal decisions made by algorithms, nor does it provide a pathway for collective redress or protection against retaliation when questioning platform practices.

Provisions on payment monitoring are vague, with no clarity on whether the government's proposed software will offer workers visibility or merely aggregate data for regulators. Unlike the EU's framework, which mandates human oversight of automated decisions, Karnataka's law offers only transparency in principle, not accountability in practice. Without stronger enforcement mechanisms, worker consultation, or explicit rights to challenge algorithmic harms, the Bill risks becoming symbolic as an important recognition of the problem but not a solution.

CCPA FINES RAPIDO FOR MISLEADING 'AUTO IN 5 MIN' AD, ORDERS CASH REFUNDS

NEWS

The Central Consumer Protection Authority ("**CCPA**") imposed a penalty of Rs. 10 lakh on the operator of the ride-hailing app Rapido. The Authority found Rapido's "Auto in 5 min or get Rs. 50" campaign misleading, since users received limited use "Rapido Coins" instead of real money. The CCPA ordered the ad's discontinuation and directed Rapido to reimburse all affected users in actual currency, invoking its powers under Sections 10, 20, and 21 of the Consumer Protection Act, 2019 ("**the Act**").

ANALYSIS

The CCPA's order underscores a stricter reading of the *Guidelines for Prevention of Misleading Advertisements and Endorsements, 2022* ("**the Guidelines**") The campaign's headline promise created a reasonable expectation of cash reimbursement, but hidden restrictions like coins redeemable only on bike rides that expire in seven days, meant the offer concealed material information and contradicted its own guarantee. Section 4 of the Guidelines requires advertisements to be truthful, not exaggerated, and free of disclaimers that undermine the main claim and Rapido's campaign failed on each count. Importantly, section 4(2) of the Guidelines that provides for an exemption for incidental lapses was ruled out, as the scheme ran for 548 days generating over 1,200 complaints.

The CCPA signalled that structural mismatches between headline claims and actual benefits constitute unfair trade practice by directing reimbursement and imposing a penalty under Section 21 of the Act. This case, alongside scrutiny of Uber and ONDC nudges, shows regulators are moving beyond isolated incidents towards broader crackdown of systemic patterns of consumer manipulation in digital platforms.

CERT-IN ISSUES THE COMPREHENSIVE CYBER SECURITY AUDIT POLICY GUIDELINES, 2025

NEWS

The Indian Computer Emergency Response Team ("**CERT-In**") issued the Comprehensive Cyber Security Audit Policy Guidelines, 2025. ("**the Guidelines**") The guidelines have been made applicable to the CERT-In enrolled Auditors and both public and private organisations, whose infrastructure is subject to auditing. Failure to adhere to these guidelines could lead to a fine of over Rs. 1 crore or imprisonment extending up to 1 year or more.

ANALYSIS

A major change brought in by the 2025 guidelines is the broadened scope of audits. It has introduced compliance audits, vulnerability assessments, source code reviews, application security testing, and other measures. It aims to create a framework for the comprehensive evaluation of the cyber-security infrastructure. Further, Auditors are supposed to avoid relying on automated and tool-based testing methods as they have a high probability of missing out on critical manual or non-automated elements. All vulnerabilities found through the audits have to be classified into either of the two frameworks – Common Vulnerability Scoring System ("**CVSS**") based on the severity or Exploit Prediction Scoring System ("**EPSS**") based on the likelihood of being exploited in real-world scenarios.

The guidelines stipulate that one annual audit is mandatory, and additional audits can be conducted as per requirements, such as organisational size and complexity of infrastructure. Additionally, prior audits are required before making any major changes like system overhauls, technology migrations, etc., as these can potentially affect sensitive data during or after the process of transition.

The guidelines also bestow a supervisory role on the CERT-In, which may participate in the auditing process to assess its quality. All auditors must inform the auditee of CERT-In's involvement beforehand. Auditors are also required to share the audit information with CERT-In within 5 days.

THE DEPARTMENT OF TELECOMMUNICATIONS RELEASES DRAFT NATIONAL TELECOM POLICY, 2025

NEWS

The Department of Telecommunications ("**DoT**") has circulated the Draft National Telecom Policy, 2025 ("**2025 Policy**") for public consultation. This builds upon the National Digital Communications Policy 2018 ("**2018 Policy**") and addresses challenges and opportunities of next generation technologies such as Artificial Intelligence, 5G/6G, quantum communications, internet of things, blockchain and satellite networks for the next five years.

ANALYSIS

Unlike the 2018 policy, the 2025 draft policy is narrowly focused on telecom and sets specific targets. As also listed in its preamble, the draft policy is structured around six missions which are discussed below.

Connectivity and Innovation: The draft aims to achieve 90% 5G coverage and full 4G access by 2030, along with expanded fibre and Wi-Fi networks. These targets depend on spectrum allocation and licence rules under the Telecommunications Act, 2023. For innovation, it proposes Centres of Excellence, support to 500 startups and MSMEs, and a national innovation body.

Domestic Manufacturing: The draft proposes a 150% increase in domestic output and a Telecom Manufacturing Zone. Implementation would require statutory notifications under the Customs Act, 1962. Particularly under Section 25, to extend duty exemptions on imported telecom and semiconductor equipment. The Special Economic Zones Act, 2005 would also need notifications and possible amendments to operationalise frameworks such as single-window clearances, tax holidays, and customs exemptions for telecom manufacturing zones. Past schemes like the Telecom & Networking Products PLI had limited success, with only half of the approved companies claiming incentives. The scheme disbursed Rs. 1,162.04 crore by the end of FY25, against the Rs. 12,195 crore approved for five years.

Security and Privacy: NTP-25 calls for biometric verification, cybersecurity audits, satellite monitoring, and a National Telecom SafeNet. Compliance would apply to telecom operators, equipment vendors, and satellite service providers. Biometric checks would require conformity with Digital Personal Data Protection Act, 2023. Cybersecurity obligations must align with the IT Act, 2000 and CERT-In Directions to avoid overlapping mandates. Satellite monitoring would likely require coordination with the Department of Space and licensing under the Telecommunications Act, 2023.

THE DEPARTMENT OF TELECOMMUNICATIONS RELEASES DRAFT NATIONAL TELECOM POLICY, 2025

Continued..

Sustainability and Ease of doing Business: The draft policy sets the "30-30-30" sustainability targets i.e. 30% reduction in the telecom sector's carbon footprint and powering 30% of towers with renewable energy by 2030. These would need to be framed against existing obligations under the Environment Protection Act, 1986 and standards notified under the E-Waste (Management) Rules, 2022, which already impose duties on producers and bulk consumers for responsible disposal and energy efficiency. Lastly, the draft promises simplified grievance redressal and faster approvals via online portals and AI tools.

ONLINE GAMING AND BETTING LAWS

GST COUNCIL INTRODUCES A 40% "SIN TAX" SLAB FOR ONLINE MONEY-BASED GAMING
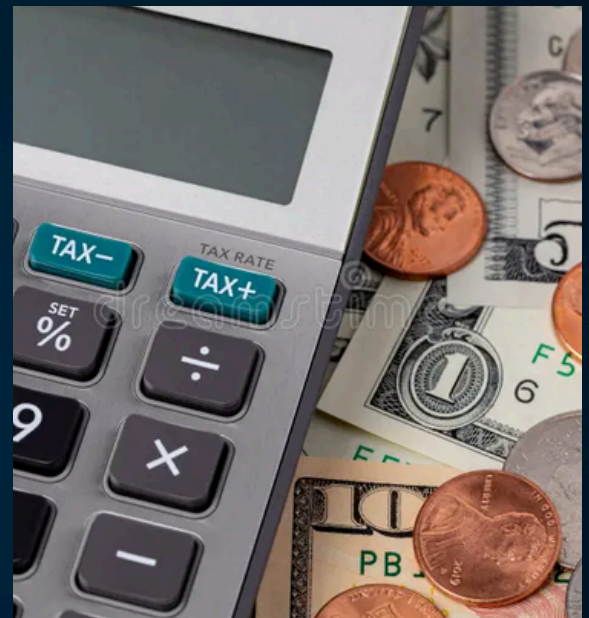
NEWS

The GST Council has introduced a new 40% tax slab for online money gaming, betting, gambling, and related activities. This is especially relevant in light of the recent Promotion and Regulation of Online Gaming Bill, 2025, which banned all online money-based gaming. The new tax structure simplifies India's GST framework from the earlier four slabs, to two standard rates (5% & 18%) while introducing the additional 'sin tax' of 40%.

ANALYSIS

The dual approach of legislative prohibition coupled with punitive taxation creates a paradox with the state simultaneously banning and taxing the same activities. This violates principles of legal coherence and may constitute arbitrary state action. The SC's pending decision on the retrospective application of 28% GST also raises concerns of regulatory inconsistency within the new dual framework. Such retrospective tax liabilities, exceeding Rs. 1.5 lakh crore, remain unresolved within the new framework, creating complex compliance scenarios where companies could face both historical and prospective tax liabilities, while also facing operational bans.

The GST Council's decision also highlights procedural irregularities. The creation of a new and higher slab, specifically including online money-based gaming, appears to be an attempt to circumvent the revenue loss from the gaming ban while retaining punitive taxes. Such a dual approach indicates inconsistent policy objectives and may be procedurally unsound, potentially exceeding the constitutional limitations on indirect taxation.

KARNATAKA GOVERNMENT PROPOSES A NEW BILL FOR CURBING ONLINE GAMBLING

NEWS

The Karnataka Government has proposed the 'The Karnataka Police (Amendment) Bill, 2025'. After the honourable SC's judgment in [All India Gaming Federation v. State of Karnataka, 2022](), this is the second attempt by the government to curb online gambling, betting and related activities.

ANALYSIS

Karnataka has emerged as one of the [leading gaming hubs]() of India and accounts for about 25% of the Indian online gaming market. It generates around ₹1,350 crore in annual taxes, and its gaming market is poised for rapid growth in the next five years.

The draft bill codified the distinction between games of chance and skill. It defines a game of chance as one where the outcome mainly depends on luck or randomness. This includes activities like gambling, betting, and wagering. On the other hand, a game of skill is one where the result mostly depends on the player's ability including things like knowledge, practice, or strategy. This amendment clarifies that games of chance are banned. However, games of skill can continue if they follow rules and [obtain required licenses.]() These licences will be issued for a period of three years and can be renewed if they meet compliance standards. Here, the operators need to maintain transparency and fairness in algorithms which are subject to audits or checks. Additionally, platforms need to establish grievance redressal mechanisms.

Further, the bill also sets up the Karnataka Online Gaming and Betting Regulatory Authority ("**KOGBRA**") which will issue licenses, block illegal websites and apps, and create awareness about the risks of betting. The penalties for violating the restrictions include a jail term of three years and a fine, which may extend to Rs. 1 lakh. While promoting or advertising illegal betting can lead to six months in jail or a Rs. 10,000 fine.

THE PARLIAMENT PASSES THE PROMOTION AND REGULATION OF ONLINE GAMING BILL, 2025

NEWS

The Parliament has enacted the Promotion and Regulation of Online Gaming Bill, 2025 ("the Bill") to establish a 'uniform' national framework for online gaming. The Bill categorically prohibits "online money games," which includes any online games involving monetary stakes, regardless of skill, while promoting "e-sports," which must involve no wagering and be determined solely by skill. It also provides for the creation of a central regulatory authority empowered to classify games, issue and revoke licenses, and enforce compliance through penalties and imprisonment. The Bill also imposes strict curbs on advertising, celebrity endorsements, and financial transactions related to real-money gaming. These measures address concerns over fraud, money laundering, and national security risks.

ANALYSIS

The Bill marks a major shift from the previous state-driven framework of online gaming regulations toward a centralised regime. While the Bill does distinguish between the types of games, its expansive definitions risk application to legitimate skill-based platforms. The term "real-money game" is unqualified and lacks specific metrics to determine the "predominant" nature of the platform, creating uncertainty for developers. It could contradict landmark rulings that distinguish games of skill, which are protected under Article 19(1)(g), from games of chance.

Traditionally, the regulation of wagering and games fell within state legislative powers, under Entry 34, and the establishment of a central regulatory authority raises concerns about the federal subject matter. Moreover, the Bill's reliance on Union List entries, such as telecommunications and inter-state trade, to justify its ambit, cannot grant competence when the Seventh Schedule vests exclusive authority with states.

The Bill also provides for compliance to be secured by way of fines and imprisonment, with the offences being cognizable and non-bailable. Alternative and proportional enforcement measures like stricter licensing conditions, age restrictions and limits of stake amount, have not been included in the bill. Such non-inclusion of proportional measures could risk the Bill's provisions being arbitrary. Authorities also have the power to search digital devices and block online content without warrants, overriding the procedural safeguards. In its current form, the Bill introduces a framework without regard for state powers, undoes the proper distinction between skill and chance, and confers wide enforcement powers. These factors make it likely to challenge on grounds of legislative competence, breach of federal structure, arbitrariness and lack of procedural safeguards.

FINTECH

NPCI DIRECTS UPI PLATFORMS TO DISCONTINUE P2P "COLLECT" REQUESTS

NEWS

The National Payments Corporation of India ("**NPCI**") has directed banks and payment service providers to discontinue UPI Peer-to-Peer ("**P2P**") "collect" requests from October. Users will no longer be able to initiate or process collect transactions through UPI platforms. The decision builds on NPCI's 2019 circular, which had capped P2P collect requests at Rs. 2,000 to curb fraud.

ANALYSIS

P2P collect requests accounted for 36% of UPI transaction volume, with 7.07 billion transactions totaling Rs. 17.74 lakh crore. However, 86% of P2P transactions exceed ₹2,000, indicating that most users rely on direct "send" methods for higher-value transfers. Since the 2019 cap forced transactions above Rs. 2,000 to be processed through direct payments, users have already adapted to alternative initiation methods for large amounts, likely reducing the potential disruption caused by discontinuing collect requests.NPCI's move is in furtherance of measures to mitigate concerns of fraud, but it erodes UPI's P2P convenience. Small merchants and gig workers, who depend on "collect" services for micro-payments below Rs. 2,000, may face difficulties, potentially preferring cash or informal credit arrangements. NPCI should monitor transaction patterns and volume post the implementation of these directions, and consider targeted exemptions or the introduction of new low-value "request" mechanisms to further UPI's goal of enabling easier digital payments.

ARTIFICIAL INTELLIGENCE

RBI ISSUES FRAMEWORK ON RESPONSIBLE AND ETHICAL AI (FREE-AI) FOR FINANCIAL SECTOR

NEWS

The Reserve Bank of India ("**RBI**") introduced the [FREE-AI framework](#) in response to the growing use of AI in India's financial sector, aiming to balance innovation with consumer protection. The framework lays out seven guiding principles, such as fairness, accountability, transparency, and safety. It organizes them into six structural pillars, with 26 actionable recommendations including mandatory audits, indigenous model development, and disclosure when customers interact with AI. Implementation is intended through voluntary adoption by banks and Non-Banking Financial Companies ("**NBFCs**") under RBI's supervisory guidance, with gradual integration via AI sandboxes, capacity-building measures, and a proposed Standing Committee to oversee ongoing compliance and risk management.

ANALYSIS

The introduction of this framework is a positive step towards the regulation of AI in India without inhibiting its growing relevance in the economy. However, the current framework remains vague on how the structure proposed will be implemented. "Accountability" is emphasized as a guiding principle; however, there is no clarification or provision entailing who will bear liability if AI does cause harm. The framework may also need to harmonise with the existing DPDP Act as both do provide broad obligations, but lack sufficient provisions on the emerging risks of AI. Consumers may still be exposed to risks of privacy infringement through AI which aren't categorised as violations due to a lack of comprehensive and explicit requirements for data provenance and purpose limitations. The recommendatory and non-binding nature of the framework may also compromise the effectiveness and implementation of the reforms put forth. The framework will benefit from imposing enforceable obligations, which may be achieved through enabling legislation or sanctions with a statutory body overseeing the compliance with the framework. Ultimately, the FREE-AI framework does set the foundation for ethical guardrails for AI in India's financial sector. Even so, there is a need for developing the framework from its current principle-based and voluntary model to enforceable regulatory standards to achieve truly transformative results.

KERALA HIGH COURT ISSUES GUIDELINES REGARDING USE OF ARTIFICIAL INTELLIGENCE TOOLS IN DISTRICT JUDICIARY
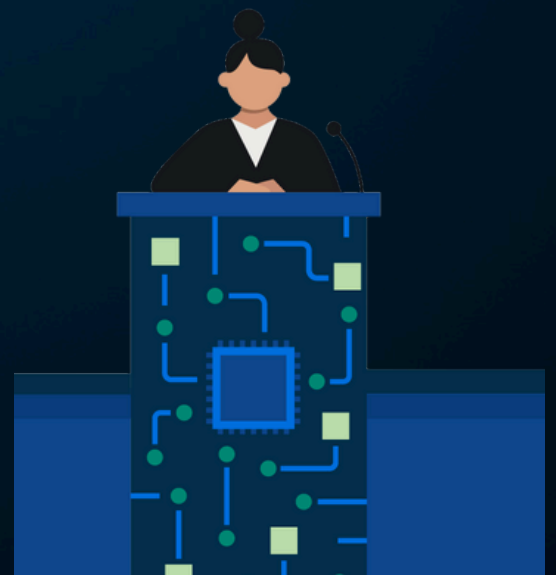
NEWS

The Kerala HC became the first judicial body to adopt a [detailed policy](#). regulating the use of AI tools in the district judiciary. The policy permits the use of AI only as an assistive tool for research and administrative function and prohibits its use for purposes beyond that. Strict measures have been proposed such as mandating human verification for AI outputs, banning unapproved cloud-based tools to protect confidentiality, and mandatory audit trails for AI use. The policy also proposes compulsory training in AI ethics and risks for judicial officers and staff with violations attracting disciplinary action.

ANALYSIS

The policy reflects a pragmatic yet cautionary approach to the use of AI in court; recognising the utility of AI for administrative and research functions while still strictly prohibiting its usage for judicial decision-making. This intervention is a significant step towards ensuring accountability and due process in the integration of AI in the judicial system. Measures such as maintaining records of all AI use through the human verification process will enhance procedural fairness, however, the implementation remains unclear as to whether the required audits will be conducted through an external audit mechanism or an internal body. The ban on unapproved cloud-based AI tools is also a positive step towards maintaining the confidentiality of sensitive data and privileged communication.

The policy also vaguely refers to usage of approved AI tools being restricted to "only for the purpose of which they are supplied or provided" under Guideline-7. Moreover, the policy does not make any reference to the requirements under the DPDP Act, such as data minimisation and storage limitations, and only imposes broad duties for confidentiality.

Overall, the Kerala HC's initiative is a very relevant step with the increasing use of AI in the judiciary and it would benefit from statutory backing and harmonisation with the existing data protection and privacy laws.

XAI SUES APPLE AND OPENAI OVER CHATGPT-IOS INTEGRATION DEAL

NEWS

Elon Musk's xAI has filed an antitrust lawsuit against Apple and OpenAI, alleging an "unlawful agreement" to monopolise the generative AI market by integrating ChatGPT directly into iOS. The complaint asserts that Apple's deal with OpenAI made ChatGPT the only generative AI chatbot natively accessible on iPhones, preventing competitors such as xAI's 'Grok' chatbot from reaching users. xAI further claims that Apple uses its App Store ranking and review processes to disadvantage rival AI apps, demoting competing chatbots and thereby reinforcing OpenAI's dominant position.

ANALYSIS

xAI's complaint raises questions under the Sherman Act, which prevents contracts that unreasonably restrain trade. xAI has challenged whether Apple and OpenAI's exclusive partnership constitutes an unlawful arrangement that leverages Apple's control to protect OpenAI's market share. The complaint also contends that the App Store uses algorithmic demotion for competing AI apps, which amounts to exclusionary conduct.

This lawsuit exists in the context of Musk's long feud with OpenAI, dating to his 2023 departure and subsequent lawsuits alleging breach of nonprofit promises and false advertising. By impleading Apple, xAI has broadened the dispute to mobile integration practices which impact market behaviour. If the court finds the integration deal anticompetitive, it could restrain how device manufacturers embed AI services, prompting regulators to reassess exclusive arrangements between platform providers and AI developers.

Contrarily, Apple and OpenAI may defend the integration as pro-competitive, arguing that embedding AI directly into iOS enhances user experience, without adversely impacting the distribution of competing apps. The outcome of the case will set an important precedent on how antitrust law governs emerging AI technologies and platform integration.

DATA
PRIVACY

username

OK

IAMAI CLAIMS THAT AMBIGUITIES IN SECTION THE DPDP ACT COULD POSE UNDUE COMPLIANCE BURDEN ON INDIAN AI FIRMS

NEWS

In a submission to the Ministry of Electronics and Information Technology ("**MeitY**"), the Internet and Mobile Association of India ("**IAMAI**") has contended that the ambiguities in Section 3(c)(ii) of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), which excludes certain publicly available personal data from the Act's scope, may restrict innovation and negatively impact India's AI development. It has urged the government to exempt companies that train AI models from compliance with this section by either using its powers under Section 17(5) or by amending the Act.

ANALYSIS

According to Section 3(c)(ii), the DPDP Act does not apply to personal data that is made publicly available by the data principle or any other person under a legal obligation. IAMAI contends that while this exclusion is a welcome provision for AI companies, its current language might raise serious compliance burdens.

Their first contention was that while the section excludes voluntarily disclosed data from the Act's purview, it is very difficult to ascertain if the data disclosed is voluntary, as platforms' privacy settings change continuously. Secondly, they argue that it is hard to track if the data was legally disclosed and subsequently reuploaded online. These issues, according to them, would disproportionately affect smaller firms, especially those that are training AI models tailored to Indian languages and contexts.

However, their request for exemption is not a solution without flaws. One of the potential issues is that such a request treats data more like infrastructure than something protected by individual rights. Further, looking at the global perspective on compliance burden of small firms, it is found that while the EU has proposed easing compliance for SMEs in GDPR, it is also taking steps to increase oversight of data processing by AI. This aims for a balanced stance as against an unfettered pro-AI development data protection regime, which is implied by IAMAI's request.

CONTRIBUTORS

WRITERS

ANJALI PANDE
ARANYA SEN
ARNAV RAJ
DIYA JAIN
ISHANI GARG
MAITHILI DUBEY
SHRUTI SRIRAM
SUBHASIS SAHOO

EDITOR-IN-CHIEF

PRATYUSH SINGH

DESIGNERS

ISHITA SAND
MAITHILI DUBEY
SUSHREE TEJOSWI

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

INSTRAGRAM   EMAIL   LINKEDIN