LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education initiative)

SEPTEMBER, 2025

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

CONTENTS

TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

KARNATAKA HIGH COURT UPHOLDS CONSTITUTIONALITY OF THE SAHYOG PORTAL

NEWS

The Karnataka High Court has dismissed X Corp's (*formerly Twitter*) petition on the grounds that an intermediary, let alone a foreign one, cannot challenge Indian social media laws and interpretation of Article 19. X Corp. had filed a writ petition under Article 226 against the Union of India in the Karnataka High Court to challenge the Government's extension of blocking powers via Section 79(3)(b) of the Information Technology Act 2000 ("**IT Act**") and the Sahyog portal.

ANALYSIS

The crux of the petition was to check for validity and constitutionality of the Sahyog Portal, while interpreting the relevant provisions. However, Justice M Nagaprasanna, in this CAV order has focused more upon the validity of the challenge brought in by the foreign entity X Corp. It states that the "faceless" foreign intermediary cannot challenge Indian citizen centric laws under the garb of Article 14, when inherently the interpretation of Article 19 is being questioned.

The Sahyog Portal was created to automate the process of sending take down notices to intermediaries by the appropriate government or its agency under Section 79(3)(b) of the IT Act, in order to facilitate the removal or disabling of access to any information, data, or communication link that is being used to commit an unlawful act. In the creation of Sahyog, the government may have broadened the scope of Section 79(3)(b) of the IT Act by not restricting issuance of blocking orders under Section 69A on reasonable grounds.

The ruling significantly deviates from principles laid down in *Shreya Singhal vs. Union of India*, on the premise that the current Indian internet user base has increased manifold since 2015. X contended that requiring social media intermediaries to scrutinise and remove users' information if it is deemed 'unlawful' under Section 79(3)(b) of the IT Act contradicts the *Shreya Singhal* case. It was argued that the government never urged Section 79 as an empowering section, hence an exemption provision could not constitute a source of power.

While a further appeal on the issue is awaited by the foreign intermediary X Corp, the Sahyog portal shall continue to onboard intermediaries for content moderation and regulation in the country. Additionally, the Indian Cyber Crime Coordination Centre ("**I4C**") has instructed all intermediaries to onboard the Sahyog portal for removal of child sexual abuse material ("**CSAM**").

THE DOT HAS RELEASED THE DRAFT RULES FOR TELECOMMUNICATION SERVICE AUTHORISATION

NEWS

The Department of Telecommunications ("**DoT**") released the Draft Rules of Authorisation for Main, Miscellaneous and Captive telecommunication services under the Telecommunications Act, 2023 ("**the Act**") for public consultation. The Draft Rules seek to consolidate various licenses and service authorisation frameworks under a single framework. On DoT's request, Telecom Regulatory Authority of India ("**TRAI**") last year had released recommendations on service authorisation mechanisms which are now being implemented with some changes.

ANALYSIS

The three rules begin with general conditions that apply uniformly to all categories, and then proceed with service-specific terms organised under common headings.

The first general condition we see is that the new rules do not override the old licensing regime under the Indian Telegraph Act, 1885, rather it is upon the service operator to choose between the old and new. The new regime would be a short document granted by DoT instead of a bulky contract between the DoT and licensee as in the old regime. This new document will incorporate references to the provisions of the applicable rules.

It is worth noting that the TRAI recommendations had instead suggested an overhaul of the existing mechanism altogether. Telcos have thus argued that authorisation could potentially grant the government unilateral power to alter conditions without prior notice, which was previously not possible under contractual licensing.

Main services include public/consumer-facing telecom services such as access, internet, long-distance and unified services. The Rules for this category specify a renewable 20-year term for authorisation, subject to eligibility criteria, and other requirements. With increasing interest in satellite-based telecom services, the Rules have comprehensively covered this domain. Additionally, Virtual Network Operators can now enter into agreements with more than one parent Network Service Operator for all types of telecom services except wireless services.

THE DOT HAS RELEASED THE DRAFT RULES FOR TELECOMMUNICATION SERVICE AUTHORISATION

Continued..

This provides a much-needed push for the sector. Miscellaneous services, referred to as Auxiliary in the TRAI recommendations, are services that are not delivered to the public at large and have a light-touch regulatory oversight. Rules for this category have more or less made the existing system more investor-friendly. Though the introduction of a new service authorisation catering to audio conferencing, audiotex, voicemail and cloud-based services is an important leap forward. Captive telecom services include network services for private use. According to the rules, if these entities are found eligible under Rule 4, they will be treated the same as any conventional telecom players despite their private nature.

The rules classify telecom services into four categories; thus, we now await rules for broadcasting services. The consultation period of 30 days is crucial for stakeholders to raise their concerns so that the final implementation process of these rules can be best leveraged.

EU PLANS TO PUBLISH DIGITAL NETWORKS ACT BY DECEMBER 2025

NEWS

The European Union (**"EU"**) plans to present the Digital Networks Act ("**DNA**") in December to reform telecom rules and boost connectivity. This Act comes as the EU's response to the mounting challenges of network investment, competition, and cross-border digital services. The initiative marks a significant step in updating the regulatory environment governing Europe's communication infrastructure since its last revision in 2018. Initial consultations signaled sweeping changes, including structural adjustments to telecom regulation and new obligations for large tech companies. However, the recent proposal is announced as "less ambitious" than earlier drafts, revoking the initial changes. By being a regulation rather than a directive, The Digital Networks Act will be directly applicable in all EU member states.

ANALYSIS

The DNA reflects a balance between competition law, investment incentives, and EU integration goals. The DNA establishes a regulatory framework of telecommunication to ensure a robust, secure, and future-proof digital infrastructure, crucial for emerging technologies. It seeks to revamp the existing system defined in the European Electronic Communications Code (**"EECC"**), as it has become obsolete and no longer guarantees sustainable competition or the necessary investments.

Tact suggests EU level spectrum planning for future use cases (e.g. verticals, 6G, satellites). It brings in market incentives including reduced compliance costs and transparency in investment rules to obtain long-term capital and increase competition. Initially introduced to unify fragmented telecom laws in order to ensure long-term investment, the new drafts work more through existing regulations, with a discretion granted to the national regulators. Critics raise concerns that this may extend the regulatory discontinuity that the Act was intended to eliminate.

The Commission's approach can be seen as a strategy of gradual implementation, allowing time for stakeholders and member states to adapt without immediate disruptions to Europe's telecom markets. Lastly, the implementation of the act will determine whether the DNA can achieve its core goal of building a more competitive, connected, and resilient digital Europe, or whether compromises will limit its long-term impact.

MCA RELEASES THE DRAFT CIVIL DRONE BILL FOR CONSULTATION

NEWS

The Ministry of Civil Aviation ("**MCA**") released the draft Civil Drone (Promotion and Regulation) Bill, 2025 ("**the Bill**"), which is India's first standalone drone legislation to replace the existing Drone Rules, 2021.

All drones above 250 grams must be registered with Directorate General of Civil Aviation (**"DGCA"**) and obtain Unique Identification Numbers, while manufacturers need type certification before selling any drone. The Bill introduces criminal penalties including imprisonment up to three years and fines up to Rs.1 lakh for violations, with several offences now classified as cognizable. Third-party insurance becomes mandatory for all operators unless specifically exempted, with fixed compensation amounts for accidents.

ANALYSIS

The Bill represents a shift from the relatively more liberal Drone Rules, 2021, which had decriminalised most offences and provided exemptions for research, development, and model aircraft operations. The 2021 reforms were specifically designed to encourage innovation. The new bill however, introduces clear guidelines, oversight, penalties and compliance requirements.

Type certification requirements have been extended to manufacturers and sellers, and not just to operators. This could undo the earlier flexibility that allowed startups and research institutions to experiment with prototypes. The Bill removes the specific carve-outs for model remotely piloted aircraft systems, and r&d activities that existed under the 2021 Rules. This creates barriers for educational institutions and innovators who previously operated under simplified frameworks. Further, The expanded definition of "accident" to include property damage alongside injury or death significantly increases liability exposure for operators and insurers, and might adversely impact newer players in the industry.

The Drone Federation of India warns that the Bill could harm reforms that helped India's drone sector grow from Rs. 60 crore in 2020 to Rs. 3,000 crore today. The sector was projected to reach 11.06 billion USD by 2030, and increased compliance costs and criminal liability could dampen this growth trajectory.

The government must balance safety and security concerns with innovation needs. Whilst stronger penalties may deter misuse, the complete removal of research exemptions could kill the innovative ecosystem the 2021 reforms aimed to create. The success of this sector ultimately depends on whether the legislation can address legitimate concerns without sacrificing the innovation-friendly environment that enabled the sector's recent growth.

ONLINE GAMING AND BETTING LAWS

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

MEITY RELEASES THE DRAFT ONLINE GAMING RULES FOR CONSULTATION

NEWS

The Ministry of Electronics and Information Technology (**"MeitY"**) has issued the draft Promotion and Regulation of Online Gaming Rules, 2025 (**"the Rules"**) for public consultation. The Rules aim to establish a comprehensive regulatory framework under the PROG Act.

The rules create the Online Gaming Authority of India (**"the Authority"**) as a statutory body with powers equivalent to a civil court. The rules expound on the Act's classification of games, distinguishing between online social games, e-sports, and online money games. Online money games have been completely prohibited with criminal penalties of up to three years imprisonment and fines up to Rs. 1 crore.

Registration certificates for games and platforms remain valid for a maximum of five years with renewal requiring fresh applications. Further, operators must notify the Authority of any "material changes" that are made post-registration. The rules also establish a three-tier grievance redressal mechanism starting with the service providers, followed by the Grievance Appellate Committee under IT Rules 2021, and finally to the Authority.

ANALYSIS

The draft rules reveal the complexities in India's approach to gaming regulation, particularly the multi-ministerial coordination required for its implementation. MeitY oversees the Authority while the Ministry of Information and Broadcasting ("**MIB**") regulates online social games and the Ministry of Youth Affairs and Sports ("**MYAS**") handles e-sports. This division could potentially lead to jurisdictional conflicts, with both ministries and also the Authority possessing powers to issue guidelines for online social games and e-sports.

The voluntary registration model for online social games creates an interesting regulatory environment. The Rules permit offering games without registration, but registered games gain credibility with business partners, investors, and app stores. This encourages compliance through market incentives rather than regulatory compulsion. However, it is unclear how enforcement will differentiate between legitimate unregistered games and prohibited money games.

The Authority's civil court powers under the CPC represent an unprecedented delegation of judicial functions to a sectoral regulator.

MEITY RELEASES THE DRAFT ONLINE GAMING RULES FOR CONSULTATION

Continued...

The power to summon witnesses, examine evidence under oath, and impose penalties, with land revenue recovery mechanisms, creates quasi-judicial proceedings that may challenge principles of natural justice. The draft rules also don't specify appeal mechanisms from Authority decisions beyond internal grievance procedures.

The penalty determination criteria under the rules includes "amount of unfair gain," "loss caused to users," and "gravity of non-compliance", which are subjective thresholds requiring the Authority to develop consistent standards. The discretionary nature could lead to unpredictable penalty outcomes and should be supplemented by detailed guidelines.

The transitional provisions which provide for fund refunds to users also raises implementation challenges. The rules provide a 180-day immunity for banks facilitating user fund returns, but does not clarify whether this covers winnings, deposits, or both. The Explanatory Note provides for the "repayment of funds collected before PROG Act enforcement," which alludes to deposited amounts, whereas, Rule 24 provides for funds "due to be returned" implying the inclusion of winnings also. This distinction muddies compliance obligations for financial institutions and platform operators.

The rules should address several definitional gaps before finalisation. "User safety features" remains undefined and platforms remain uncertain about compliance obligations. "Material changes" which require notification have also not been defined, potentially including routine game updates and creating unnecessary regulatory challenges.

The increase in compliance obligations and costs, without any relaxation for new entrants, will certainly hamper smaller players. Industry consolidation is likely with larger platforms being able to navigate the new framework.

FINTECH

THE RBI HAS ISSUED THE PAYMENT AGGREGATOR RULEBOOK

NEWS

The Reserve Bank of India (**"RBI"**) has issued the new Reserve Bank of India (Regulation of Payment Aggregators) Directions, 2025, ("**the Directions**") replacing and consolidating earlier circulars. It had previously issued the draft directions for stakeholder comments, which proposed a framework for regulation of Payment Aggregators ("**PAs"**) that handle proximity or face-to-face payments. It also proposed certain changes to the extant direction for PAs. New guidelines were brought in the sectors of 1) rationalisation and definition of various categories of PAs, 2) the authorisation process, 3) the process for carrying out due diligence of merchants by PAs, and 4) permissible operations in escrow accounts.

ANALYSIS

The RBI classified PAs into three categories based on their business models- PA-O (online), PA-P (physical/offline), and PA-CB (cross border). This brought a major change from the earlier guideline where just PA-Online and PA-Physical was regulated. In this, PA-CB gets much clearer regulation, as well as explicit definition. It now defines them as entities that facilitate import and export payments, and subject them to licensing, fund segregation, transaction limits, and strict compliance rules for greater transparency and regulatory oversight. Under the RBI supervision, they must follow specific governance and due diligence standards.

In order to ensure financial stability and risk management capability, entities seeking authorisation as a Payment Aggregator must have a minimum net worth of Rs. 15 crore at the time of application, reaching Rs. 25 crore by the end of the third financial year. Stronger Know your Customer ("**KYC**") and anti-money laundering ("**AML**") processes have been mandated for onboarding merchants, and PA's must classify merchants by turnover size and perform continuous monitoring to manage risk.

THE RBI HAS ISSUED THE PAYMENT AGGREGATOR RULEBOOK

Continued...

Stricter fund segregation has also been added, which mandates that all the funds collected by the PAs to be held in escrow or similar accounts with clearly defined rules on usage, debits and credits.

This has been done to ensure that the customer's and the merchant's funds are separated from the aggregator's own, reducing the risk of misuse. This also enhances fund security, and protects the stakeholder interests if the aggregator faces financial trouble. Even offline transactions must be in compliance with escrow requirements, that further enhances fund security.

In order to protect consumer information, enhanced cybersecurity measures have also been added, where only card issuers and networks can store card data, and other entities must strictly delete such data by specified deadlines.

The new guidelines have brought much needed changes to the older framework. By enforcing a stricter compliance burden, PAs will need to upgrade their KYC, risk monitoring systems, and escrow mechanisms significantly. These measures put customer trust at the centre, and will thus reduce fraud and unauthorised transactions, creating a safer and more trustworthy payments ecosystem

RBI RELEASES NEW DIRECTIONS ON DIGITAL PAYMENT AUTHENTICATION MECHANISMS

NEWS

The RBI has released the Authentication Mechanisms for Digital Payment Transactions Directions, 2025 ("**the Directions**"), requiring all payment system providers to implement two-factor authentication for digital transactions by April 1, 2026. The directions move beyond SMS-based OTPs to include hardware tokens, cards, passwords, PINs, and even biometrics.

For card-not-present ("**CNP**") transactions, of the mandatory two-factor authentication, at least one factor must be dynamic or uniquely provable for each transaction. Card issuers face additional obligations for cross-border CNP transactions by October 1, 2026, and must implement risk-based authentication mechanisms. However, small-value contactless transactions, recurring e-mandates, and gift prepaid instruments remain exempt.

ANALYSIS

The move beyond SMS-OTP dependence addresses concerns like SIM swapping, SMS interception, and network delays, which have enabled fraud. However, the "dynamic or uniquely provable" standard for CNP transactions creates ambiguity. UPI transactions currently rely on device binding and UPI PINs, but neither changes per transaction. Payment apps may need to develop new models to satisfy this requirement, potentially disrupting established user flows. This could drive innovation in authentication protocols but also increases technical complexity for smaller players.

The risk-based approach gives developers significant flexibility, allowing payment providers to develop their own behavioural analytics models and authentication methods. However, the directions also impose complete liability on platforms for non-compliance and resultant losses to customers. This incentivises conservative risk management over user convenience, potentially fragmenting the payment experience across platforms.

RBI RELEASES NEW DIRECTIONS ON DIGITAL PAYMENT AUTHENTICATION MECHANISMS

Continued...

As mentioned before, the directions prescribe risk-based authentication, which relies on behavioural analytics to work suitably. It requires substantial data collection and processing which raises privacy concerns under the DPDPA, an overlap that the directions do not address or even acknowledge. Payment providers must balance fraud prevention with data minimisation requirements, especially keeping in mind the sensitive nature of financial data.

The success of the directions depends on industry coordination around interoperability standards across devices and operating systems. Without common protocols, users could face inconsistent authentication experiences across different platforms. The RBI could issue supplementary guidelines clarifying terms like "capable of being proven" to prevent inconsistent industry interpretation.

CYBERSECURITY AUDITS HAVE BEEN MADE MANDATORY FOR VIRTUAL DIGITAL ASSET PROVIDERS IN INDIA

NEWS

India has recently mandated that all virtual digital asset ("**VDA**") service providers such as cryptocurrency exchanges, wallet operators and other intermediaries must submit to a compulsory cybersecurity audit by government-appointed auditors. This decision has been driven by a series of high-profile crypto thefts and is intended to safeguard its users and tighten the regulatory setup for the sector.

ANALYSIS

VD are tokens, cryptocurrencies and other transferrable, storable or tradable electronic assets having monetary value. As these are outside the traditional banking system, they are susceptible to frauds, hacking and misuse.

Under the new directions, cybersecurity audits shall be executed by auditors empanelled with the Computer Emergency Response Team-India (**"CERT-In"**). By engaging CERT-In approved auditors, the government benefits from independent scrutiny of key systems, such as key management, security of transactions and integrity of data. VDA providers must submit audit certificates to maintain their registration under the Prevention of Money Laundering Act (**"PMLA"**), with immediate compliance required for directors, principal officers, and chief compliance officers.

The enforcement mechanism provides that non-compliance can lead to registration denial or cancellation, effectively shutting platforms out of the Indian market. This mandatory audit requirement will increase customer confidence. Regular testing of key systems ensures that gaps can be identified and fixed before they can be exploited. This new framework clarifies India's intent to strictly oversee and regulate the sector. However, instead of stifling innovation, the government has chosen to set out operational standards that must be met, in alignment with global best practices.

ARTIFICIAL INTELLIGENCE

THE FEDERAL TRADE COMMISSION LAUNCHES AN INQUIRY AND CALIFORNIA PASSES THE SB 243 ON COMPANION CHATBOTS

NEWS

California has enacted Senate Bill 243 (**"SB 243"**) becoming the first state to target "companion chatbots." It mandates AI systems that simulate ongoing relationships to reveal their non-human nature, establish crisis procedures for self-harm, institute safeguards for children, and ensure compliance reporting. Concurrently, the Federal Trade Commission ("**FTC**") has initiated an inquiry into leading AI companies to examine how companion chatbots are created, sold, and regulated, with specific emphasis on harm to children.

ANALYSIS

SB 243 is significant as it is the first attempt at regulating relational AI, but its drafting remains vague. Its definition of "companion chatbot" is predicated on whether or not the system can maintain relational or anthropomorphic interactions, a subjective standard that might extend to ordinary service bots. This overbreadth makes for compliance uncertainty and encourages companies to over-withdraw or stay out of the California market entirely, particularly in light of the burdensome reporting and monitoring requirements. The imposition of a private right of action adds to risk, inviting suit even when injury is hypothetical and leaving judges to demarcate the scope of responsibility.

The FTC's inquiry raises similar concerns of manipulation, child safety, and opaque business models. But in the absence of binding federal regulations, the inquiry presents an investigatory pressure rather than a harmonising norm, which may be the solution. There is hence a fragmentation; California has statutory requirements, while the federal agency uses an ad hoc review. The system also benefits larger players who have compliance capability, while overburdening smaller companies, diminishing competition without necessarily enhancing consumer protection.

The central flaw of SB 243 is its dependence on subjective standards. Liability ought to attach to quantifiable behavior, for example, through overt marketing of companionship, gathering of sensitive relational data, or deployment to minors; instead of a vague definition of "relational interaction." A federal standard is necessary, which would have to include consistent disclosure mandates, child-protection practices, and crisis procedures, combined with certification or safe harbor provisions. This may foster responsibility without discouraging innovation. Unless and until such alignment is achieved, regulation of chatbots may just be driven by regulatory patchwork and litigation rather than by coherent policy.

ITALY BECOMES THE FIRST EU STATE TO PASS COMPREHENSIVE LAW REGULATING USE OF AI

NEWS

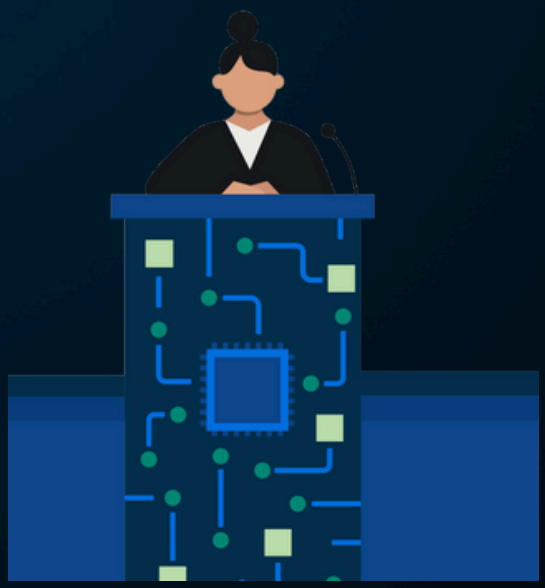
Italy became the first EU member to pass a comprehensive national AI legislation. The parliament passed Law No. 1146-B, which provides criminal penalties for deepfakes and malicious use of AI. This law promotes human supervision and control in many sectors such as healthcare, education, justice, and public administration. It also establishes barriers to AI-access among children under 14 years of age, and proposes punishments of one to five years of imprisonment for harmful AI-generated content.

ANALYSIS

Italy's approach shows the first divergence in domestic AI regulation and the EU AI Act. While the new law aligns with the EU Act in many respects, it has some crucial differences.The criminal sanctions incorporated under the law ensures that the misuse of AI will not only be regulated but also severely penalised. The law prioritises human authority in sensitive areas such as healthcare and justice because AI systems can be opaque sometimes, thus, it becomes crucial to keep humans in charge. The age based restriction which makes parental consent a prerequisite for using AI tools, limits unauthorised AI exposure to minors. The criminal penalties of the new Act are stricter than those prevailing in other jurisdictions, the majority of which rely primarily on civil remedies, administrative fines, or existing criminal frameworks. The enforcement challenges of the new law remain unclear, relying on vague thresholds of "unjust harm" and raising concerns about whether courts have the required expertise to lay down the jurisprudence in this area.

The new copyright provision requires "real human creativity" for AI-assisted works to be protected. This offers certainty to creators and businesses because it distinguishes protectable human-authored content from unprotectable machine-generated output.

The governance structure of the new law has been criticised by the European Commission for designating government agencies as AI oversight bodies in place of independent regulators. This moves away from the EU framework which centers regulatory independence for oversight bodies and



ITALY BECOMES THE FIRST EU STATE TO PASS COMPREHENSIVE LAW REGULATING USE OF AI

Continued...

provides that these bodies "exercise their powers independently, impartially and without bias." This difference is not merely procedural. Independent regulators can better balance innovation and regulation, especially when state interests could conflict with either. Although the Italian AI law aligns with the EU AI Act in establishing broad AI rules, it is yet to provide clarity on the specific duties, timelines, and enforcement steps for businesses. The 12-month deadline to implement decrees creates an environment of uncertainty. During this period, most of the rules are merely proposed guidelines rather than mandatory requirements, therefore, many stakeholders remain unclear about compliance requirements.

The government has also committed €1 billion through a state-backed venture capital fund to foster AI, cybersecurity, and telecommunications innovation. Critics however raise concern about whether the amount was adequate compared to the billions invested by global leaders such as the US, China, and the UK.

With Italy opting to lead with national legislation rather than wait for complete EU implementation, stakeholders now need to navigate a dual regulatory framework. Whether this will lead to fragmentation of the European market remains to be seen after the law's implementation and other states' regulatory approach.

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP, AND INNOVATION

INCOME TAX ACT 2025: A PRIVACY CROSSROAD

NEWS

With the introduction of the Income Tax Act, 2025, ("IT Act") India is at a turning point in terms of data privacy regulation. Described as an act of modernisation, the IT Act replaces a law that was more than six decades old. It promised clarity through simplification and rationalisation. However, visible under the surface, is the motive of state expansion and surveillance, or so say critics.

ANALYSIS

Section 247 of the Act gives Income tax officers the power to search "virtual digital spaces", that is, the power to search in private spaces, like cloud storage, personal messaging apps, and social media accounts, beyond just a physical location.

The said additional power is not just a procedural change, instead it is an indication of the intent to monitor issues of tax fraud and address the issues of financial deceit. If we draw an analogy to other countries like the US, and EU where lack of transparency is mitigated by introducing the requirement of judicial warrants before judicial searches makes the action more rational.

The constitutional challenge centers on whether the provisions pass the Puttaswamy test. The 2017 judgement established that privacy infringements must satisfy three criteria: legality (statutory authority), necessity (legitimate state aim), and proportionality. While the bill obviously meets the procedural test of legality, it does not entirely satisfy the other criteria. While tax compliance is a legitimate state interest, the measures of the Act may not be proportional, keeping in mind the existence of less intrusive alternatives which do not compromise individuals' rights.

The DPDP Act complicates this analysis. It provides wide exemptions for state agencies in matters involving national security, public order, or law enforcement.Tac authorities could arguably fall under these exemptions, meaning that the Data Protection Act might actually be legitimising these extensive digital search powers. This creates an environment where data privacy exists more on paper than in practice.

INCOME TAX ACT 2025: A PRIVACY CROSSROAD

Continued...

These exemptions exist without rational safeguards and by allowing the tax officials to examine Whatsapp messages or Twitter direct messages to determine taxable income, the IT Act contradicts the very essence of privacy jurisprudence in India. The Act risks violating Article 14 as arbitrary state action. Article 19 is also threatened by the chilling effect this Act creates on free expression through unchecked surveillance.

Misuse of the Act's provisions can be prevented by the introduction of judicial warrant requirements, limit searches for financial data involving tax investigations and alignment with DPDP safeguards, ensuring that the fight against tax evasion does not transform into unchecked digital surveillance. However the current political and legal environment make meaningful checks unlikely.

For taxpayers, this means practicing digital hygiene. Tax authorities could eventually access individuals' entire online presence. Casual statements about income, jokes about tax avoidance, or financial discussions in 'private' spaces could now be used as evidence. Without the parliament adding meaningful safeguards, courts will need to determine the Act's legality. The stakes go far beyond tax compliance. If the government can access all digital spaces based merely on suspicions of non-compliance, it could establish a dangerous precedent for broader surveillance powers.

CCI AND MEITY DISCUSSED EMERGING CHALLENGES IN COMPETITION LAW AND DATA PROTECTION

NEWS

The Chairperson of the Competition Commission of India ("**CCI**") met with the Secretary of the Ministry of Electronics and Information Technology ("**MeitY**") to discuss the interface of the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") with the Indian Competition Law regime. The deliberations highlighted the shared commitment of both bodies towards ensuring a "*transparent, competitive, and innovation-friendly digital ecosystem*," while safeguarding the interests of consumers and businesses. Additionally, it addressed the need for a consultative approach to ensure consonance between both the laws.

ANALYSIS

The meeting takes place at a time when there is a growing need to address the potential conflicts between the two regimes, particularly in light of the continuously evolving nature of digital markets. These issues, which were also highlighted in the recent (25th) report of the Parliamentary Standing Committee on Finance, could lead to various jurisdictional conflicts and parallel proceedings. This, in turn, would create an extra burden on both regulators and stakeholders. A recent instance of this tussle was seen in Meta's appeal against CCI's Rs. 213.14 crore penalty on WhatsApp's 2021 privacy policy, wherein it argues that CCI overstepped its jurisdiction by ruling on data privacy issues.

This meeting is a positive sign that the regulators are finally starting to acknowledge the need for coordination to govern India's digital market effectively. Further, given that the Draft Digital Competition Bill was also withdrawn by the Government, albeit for different reasons, such discussions can also pave the way for a more nuanced bill. Thus, a collaborative approach will go a long way in improving both India's data protection and competition regimes.

CONTRIBUTORS

WRITERS

ARANYA SEN
ARNAV RAJ
ANJALI PANDE
DIYA JAIN
ISHANI GARG
ISHITA SAND
MAITHILI DUBEY
PRATYUSH SINGH
SANIDHYA GURUDEV
SANSKRITI VERMA
SUBHASIS SAHOO

EDITOR-IN-CHIEF

PRATYUSH SINGH

DESIGNERS

SANSKRITI VERMA
MAITHLI DUBEY

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION