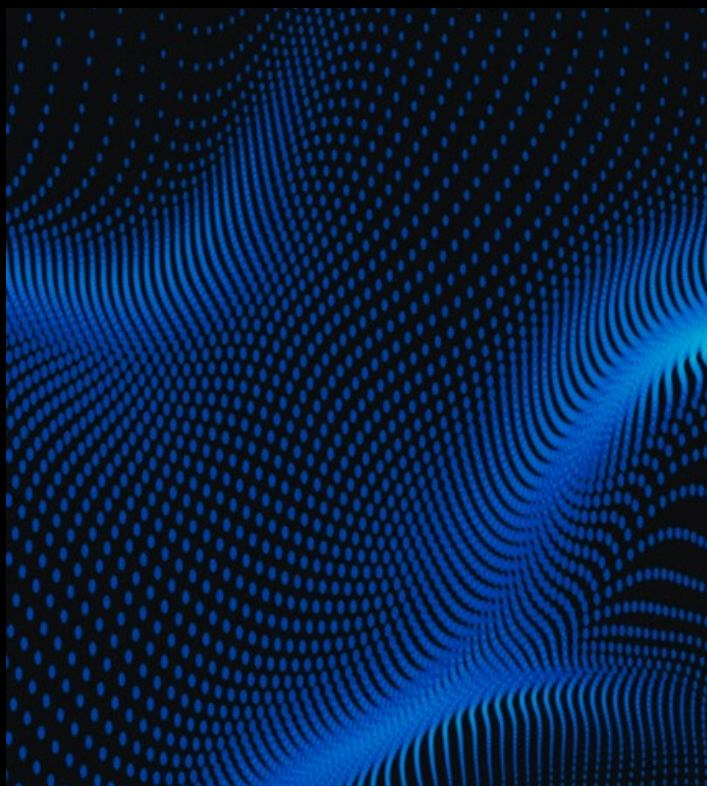
LEXTECH PRESENTS

MONTHLY UPDATES 2025

MARCH-JULY



CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

KARNATAKA'S DRAFT MISINFORMATION REGULATION BILL, 2025

The Karnataka government has introduced a draft Misinformation Regulation Bill, 2025 ("the Bill"), proposing penalties for a person guilty of propagating misinformation with imprisonment not less than three months, which may extend to five years, along with a monetary fine. The Bill introduced recently has dropped fake news from its title, indicating a significant dilution in its provisions from the earlier bill titled Karnataka Misinformation and Fake News (Prohibition) Bill.

The Bill defines "misinformation" as knowingly or recklessly making a false or inaccurate statement in the context in which it appears, excluding opinions, religious or philosophical sermons, satire, comedy or parody or any other form of artistic expression. The bill also provides for setting up special courts comprising sessions judges for the speedy trial of offences with concurrence of the Chief Justice of the Karnataka High Court.

Expansive definitions may raise constitutional concerns under Article 19(1)(a) of the Indian Constitution, given the potential chilling effect on free speech. The draft also prescribes stringent bail conditions, which place a higher burden on the accused. While the government argues the law is necessary to curb harmful online misinformation, it is to be noted that safeguards ensuring precision, independent oversight, and proportionality will be critical for the new law to withstand judicial scrutiny.

KARNATAKA'S HATE SPEECH AND HATE CRIMES (PREVENTION AND CONTROL) BILL, 2025

The Karnataka government is preparing to table the Hate Speech and Hate Crimes (Prevention and Control) Bill, 2025 ("the Bill"). The Bill seeks to curb hate speech and identity-based violence by expanding definitions and enforcement tools. It defines a hate crime as any act causing or inciting emotional, physical, social, economic or psychological harm on the basis of identity markers such as religion, caste, gender, language or sexual orientation. Hate speech is defined broadly to include intentional publication, electronic transmission, or display of identity-based content that could incite harm, including through words, visuals or symbols.

The legislation is a necessary response to rising online and offline hate incidents. However, the bill's expansive language may raise concerns about proportionality, enforceability, and possible overlap with existing provisions of the Indian Penal Code.

DRAFT AMENDMENT TO THE TELECOM CYBER SECURITY RULES, 2024

The Ministry of Communications released draft amendments to the Telecom Cyber Security Rules, 2024, inviting feedback. The proposed rules broaden the regulatory scope to include Telecommunication Identifier User Entities (**"TIUEs"**) such as OTT platforms, fintech apps, and e-commerce services that use mobile numbers for authentication. Key provisions include the launch of a centralised Mobile Number Validation (**"MNV"**) platform to verify user identities.

The draft also mandates IMEI tracking and prohibits reuse of tampered device identifiers. It introduces compliance requirements for manufacturers, importers, and second-hand device resellers. This expanded scope brings numerous digital platforms under the telecom regulatory umbrella, redefining traditional boundaries between telecom regulation and digital services governance. While the framework targets fraud and identity theft, concerns about surveillance, privacy, regulatory overreach, and the burden on startups have come into light due to the labeling of this amendment as strengthening cybersecurity.

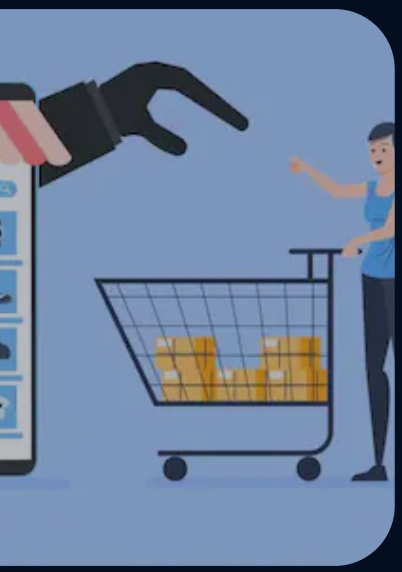
TRAI'S PILOT PROJECT FOR DIGITAL CONSENT MANAGEMENT IN PARTNERSHIP WITH RBI AND BANKS

Telecom Regulatory Authority of India (**"TRAI"**) started a three-month pilot project on Digital Consent Management with RBI-regulated banks. The aim is to curb spam calls and messages, especially those linked to banking frauds. Under this system, banks will record customer consent digitally, and Telecom Service Providers (**"TSPs"**) will use Distributed Ledger Technology (**"DLT"**) to keep these records secure and tamper-proof. Consumers will get SMS alerts from '127xxx' short codes whenever consent is taken, and they can revoke it anytime through SMS, apps, or websites.

Banks will also be required to confirm the genuineness of all uploaded consents. Legally, this furthers the Telecom Commercial Communications Customer Preference Regulations (**"TCCCPR"**), 2018, which allows commercial communication only with explicit consent and classifies other communication as Unsolicited Commercial Communications (**"UCC"**). Previously, such consent was often unverifiable because it was taken offline. This pilot makes a shift towards a transparent and consumer-friendly system. Going ahead, TRAI plans to extend the digital consent framework to other sectors, ensuring safer and more trustworthy commercial communication across industries.

CCPA CRACKS DOWN ON DARK PATTERNS IN E-COMMERCE

The Central Consumer Protection Authority (“**CCPA**”) has intensified its focus on “dark patterns”, deceptive online design tactics that nudge users into unintended purchases or actions. Following the 2023 Guidelines for Prevention and Regulation of Dark Patterns, which identified 13 practices such as basket sneaking, drip pricing, subscription traps, and disguised ads, regulators are now ramping up enforcement.



On May 28, 2025, the Department of Consumer Affairs (**“DoCA”**) convened a high-level meeting with major players including Amazon, Google, Meta, Zomato, and Uber, pressing for strict compliance. Shortly after, the CCPA issued advisories to over 50 online platforms across sectors, directing them to eliminate dark patterns and conduct self-audits within three months. To strengthen oversight, the DoCA also set up a 19 member Joint Working Group, signalling a policy shift towards safeguarding digital consumers from manipulative design practices. Dark Patterns have now come under the policy radar, and significant advisories and regulations are expected soon from the CCPA.

SAHYOG PORTAL AND CONTENT TAKEDOWN NOTICES IN INDIA

Since October 2024, the Government of India’s SAHYOG Portal has emerged as the central channel for issuing takedown requests to online platforms such as X and Meta. The Karnataka High Court is currently hearing X’s (formerly Twitter) challenge to its forced onboarding, making this a pivotal case for India’s digital governance framework.

The core issue lies in SAHYOG’s lack of statutory foundation and its reliance on Section 79(3)(b) of the IT Act to justify bulk takedown notices. Unlike Section 69A’s structured blocking regime with due-process safeguards, SAHYOG allows executive officers to issue orders without reasoned explanations, hearings, or appeals. This bypasses constitutional protections and effectively outsources judicial scrutiny to untrained officials. The portal has also been used to suppress critical journalism and political speech, creating a chilling effect on free expression. The case thus raises a fundamental question of whether the executive streamline compliance at the cost of due process, and does administrative convenience justify curtailing Article 19(1)(a) rights.

CCPA ISSUES GUIDELINES ON ONLINE SALE OF RADIO EQUIPMENT

The Central Consumer Protection Authority (**"CCPA"**) released the Guidelines for Prevention and Regulation of Illegal Listing and Sale of Radio Equipment on E-Commerce Platforms, 2025 (**"the Guidelines"**). The Guidelines aim to curb unauthorised sales of devices such as walkie-talkies, signal boosters, and jammers, ensuring compliance with telecom laws and Wireless Planning and Coordination (**"WPC"**) requirements. E-commerce platforms are barred from listing equipment requiring Department of Telecommunications (**"DoT"**) frequency assignments unless sold by authorised dealers on the Saral Sanchar portal.

Product listings must display operating frequency ranges, Equipment Type Approval (**"ETA"**), and supporting test reports. Sellers must certify authenticity of test reports and compliance with DoT norms, while platforms must remove illegal listings within 24 hours of DoT directives. Non-compliance could attract penalties under the Consumer Protection Act, 2019. Platforms are also required to display consumer advisories on risks of purchasing unauthorised devices.

BIS REVISES E-COMMERCE GUIDELINES AFTER INDUSTRY PUSHBACK

The Bureau of Indian Standards (**"BIS"**) released a revised draft of the E-commerce Principles and Guidelines for Self-Governance, following sharp criticism of its January version. The revisions reflect BIS's attempt to balance regulatory clarity with operational feasibility. The earlier draft blurred the scope of e-commerce entities, limiting it to marketplaces. The revised definition now ensures the rules apply to platform-owned retail as well, closing a potential compliance gap. BIS recognises marketplace platforms as intermediaries, aligning with existing consumer protection frameworks by shifting responsibility for accurate product information to sellers.

Similarly, extending the counterfeit reporting deadline from 48 hours to seven days signals a move away from rigid compliance timelines toward more workable enforcement. However, the deletion of open API and payment disclosure requirements indicates BIS's willingness to prioritise platform autonomy over transparency. While industry pushback has clearly shaped these changes, the absence of references to ASCI guidelines may weaken consumer-facing ad standards. The draft ultimately leans toward industry concerns, raising questions about whether consumer rights have been diluted in the process.

ONLINE GAMING AND BETTING LAWS

DGGI CRACKS DOWN ON OFFSHORE GAMING ENTITIES

The Directorate General of Goods and Services Tax Intelligence (“**DGGI**”) has blocked over 350 websites of illegal offshore online gaming firms and URLs of such platforms in coordination with the MeitY under Section 69 of the IT Act, 2000. It also blocked and attached nearly two thousand bank accounts in coordination with the I4C and the National Payments Corporation of India. Under GST law, ‘Online Real Money Gaming’ (as an actionable claim) is classified as a supply of ‘Goods’ and is subject to a 28% tax. Additionally, they are required to be registered under the current legal framework, a provision which most offshore apps circumvent.

These companies evade taxes by bypassing obligations and concealing taxable pay-ins. Non-compliance by foreign entities distorts competition, harms local businesses, and skews the market. Moreover, funds collected through mule accounts are funneled into illicit activities. DGGI’s proactive actions are not enough to curb this growing menace and uniform, strict regulations need to be established.

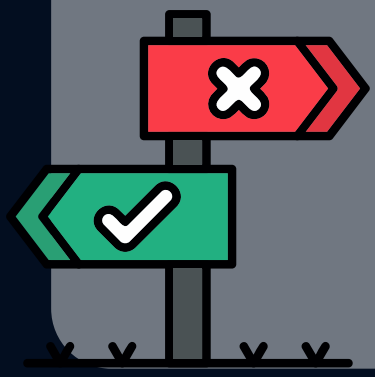



EU TAKES ACTION TO PROTECT CHILDREN FROM HARMFUL PRACTICES IN VIDEO GAMES

The Consumer Protection Cooperation Network (**“CPC Network”**) in coordination with the European Commission has identified commercial practices adopted by Star Stable Entertainment AB in their game that violate consumer protection laws. Particularly, these could be harmful to children such as, making direct appeals to them in advertisements to buy in-game currency items or lack of clear information about aspects of the game which leads to consumers spending more than they intend to.

The company has been asked to remedy these problems. Consequently, CPC Network is publishing a set of guidelines to promote fairness in the online gaming industry’s use of virtual currencies. It outlines clear pricing and pre-contractual information, avoiding hiding costs of in-game digital content, and respecting consumer vulnerabilities, in particular when it comes to children. These will help create a safer experience for children, who are often misled due to their naivety. These principles are not legally binding in themselves, but indicate how authorities will interpret violations of the law. This can serve as the stepping stone for global jurisdictions (including India) on how to make online gaming safer for consumers, especially the young audience.

GAMING INDUSTRY BODIES ISSUE CODE OF ETHICS



Bodies representing online real money gaming companies such as AIGF, EGF, and FIFS have jointly signed a Code of Ethics which all member firms under them will adhere to. This step aims to promote responsible gaming practices and promote user safety. It will enforce consistent standards of user safety and mandate reporting mechanisms and third-party audits for ensuring transparency.

It has been created on the basis of best practices recognised globally. It has strict compliances in place such as age-gating, strict KYC norms, user-set spending limits and self-exclusion. One of the primary challenges with such a self-regulation model will be its non-binding nature and reliance on voluntary compliance. Companies have already been struggling to adhere to different rules imposed by different states across the country. This step, while positive, does reinforce the need for urgent centralised regulation ensuring uniform application across the industry.

CENTRAL GOVERNMENT CONTEMPLATES BRINGING ONLINE GAMING PLATFORMS UNDER ANTI-MONEY LAUNDERING LAWS

The Centre is considering significant steps to bring online gaming platforms under the ambit of Anti-Money Laundering (**"AML"**) laws, including a proposal to mandate the registration of online gaming platforms with the Financial Intelligence Unit. This will lead to higher scrutiny for both onshore and offshore gaming platforms, by stricter KYC norms and tracking of suspicious transactions. It may lead to the classification of online real money gaming platforms as 'reporting entities' under the Prevention of Money Laundering Act (**"PMLA"**), 2002.

Section 2(1)(wa) of the PMLA defines a reporting entity as a banking company, financial institution, intermediary or person carrying on a designated business or profession. The government in March 2023 made activities undertaken by virtual digital assets service providers, they being crypto, NFT and other digital asset providers, as activities under section 2(1)(sa) of the PMLA.

Something similar is expected for online gaming companies. There has been a growing consciousness within law enforcement about a lot of unaccounted money circulating within these apps, which has to be curtailed. Many of the cases were against online betting apps, the most prominent being Mahadev Online Betting. However, if implemented it can play a key role in blocking illegal offshore betting platforms and boosting of legitimate online gaming in India.

HARYANA NOTIFIES NEW ANTI-GAMBLING ACT

Haryana notified the Haryana Prevention of Public Gambling Act, 2025 (**"the Act"**) to prevent and penalise public gambling (including digital gambling platforms). The act will have retrospective effect starting from April 9. Gambling under Section 2(1)(e) means an act of betting or gaming or both. Gaming is playing a game of chance using 'instruments of gambling' which may be electronic devices, proceeds of gambling, etc. The Act is comprehensive and prohibits all forms of gambling that may manifest within online gaming. Its broad definition of a 'bet' restricts both monetary and non-monetary considerations (such as cryptocurrencies and other digital tokens).

Additionally, it also covers opinion trading platforms (players predict outcomes of real-world events such as sports and win rewards) as well. Probo, a popular opinion trading app, has filed a civil petition challenging the new legislation. Notably, games of skills have been excluded from the Act's purview. Section 2(1)(g) defines them as games where skill outweighs chance with success mainly depending on the player's knowledge, training, attention, experience or ability. This definition is vague and the criteria that has been set cannot be used to distinguish between types of games with complete clarity. Experts will likely still have to rely on judicial decisions to understand the distinction, but this can serve as the foundation for a concrete, central legislation.

MADRAS HC'S VERDICT ON STATE'S REGULATION FOR ONLINE REAL MONEY GAMES

The Madras Court has dismissed petitions filed by online real money gaming platforms seeking leniency in response to restrictions imposed under Section 5(2) read with Section 14 of the Tamil Nadu Prohibition of Online Gaming and Regulation of Online Games Act, 2022, and the Online Gaming Authority (Real Money Games) Regulations, 2025. The main contentions were against the bar on under 18 minors from playing games, mandatory KYC norms, blanket bans at night time, and the setting of time bound monetary limits.

The Court dismissed these arguments on the ground that online games directly affect the public health of people at large and it will result in serious social repercussions if left unregulated. The power to regulate such games falls within the ambit of 'public health' which is a State subject under the Seventh Schedule of the Constitution. It was stated the right to conduct trade under Article 19(1)(g) while fundamental cannot deter someone's right to life. It stated that the balance of scales tilts towards adverse effects on the public as compared to individual freedom and autonomy, and hence the state cannot remain a mute spectator.

FATF'S COMPREHENSIVE UPDATE ON TERRORIST FINANCING RISKS AND THE LINK WITH ONLINE GAMING

The Financial Action Task Force ("**FATF**") has released a new report on terrorist financing risks where it stated that online gaming platforms are being increasingly used to disseminate propaganda, engage in radicalisation activities, and even fundraising. The report points out that criminals can quickly launder large amounts of money through thousands of small transactions. Although gaming platforms currently lack transactions of sufficient magnitude, the risk persists and will likely grow as the industry evolves.

Furthermore, in-game voice and text chats are being used to incite lone wolf attacks, and can provide terrorists with a platform to solicit donations and how to conduct such transactions securely. Popular groups like Hezbollah have been known for creating and selling their own games for propaganda purposes. Notably, adolescents make up for a high percentage of the audience for these games. This strengthens the need for central legislation to regulate the industry and prevent irreparable damage to the lives of young adults.


FINTECH

RBI REVISES KYC NORMS TO ENHANCE FINANCIAL INCLUSION AND SIMPLIFY ONBOARDING

RBI has introduced amendments to its Know Your Customer ("**KYC**") framework through the Reserve Bank of India (Know Your Customer (KYC)) (Amendment) Directions, 2025. The amendments are aimed at easing customer onboarding and improving access to banking services, especially for underserved and rural populations. The revised guidelines permit non-face-to-face ("**NFF**") and video-based KYC ("**V-CIP**") processes alongside traditional verification methods, allowing customers in remote and underserved areas to update details via video calls, reducing the need for branch visits.

Banks are also required to send at least three advance notices and three reminders, before and after KYC deadlines to ensure customers stay informed. Additionally, KYC updates can now be done at any branch where the customer holds an account and not just the home branch. Low-risk customers benefit from extended deadlines and relaxed documentation requirements. These measures aim to unlock dormant accounts and ensure timely receipt of benefits linked to social welfare schemes.

However, the shift to lighter KYC controls raises concerns around potential misuse caused due to deepfake technology. While the reforms promise greater convenience and inclusion, they also necessitate that banks strengthen their technology infrastructure and train banking correspondents to implement the updated procedures effectively.

NPCI is developing IoT-Ready UPI Framework for Autonomous Payments via Smart Devices

The NPCI is developing an Internet of Things (**"IoT"**) ready UPI framework that enables autonomous payments through smart devices. This innovative system will allow IoT devices to initiate payments without direct human intervention by using virtual payment addresses (**"VPAs"**) linked to primary UPI IDs. The solution leverages NPCI's "UPI Circle" feature, which permits delegated payments within set limits, facilitating transactions like automated parking fee payments from a connected car or subscription renewals via smart TVs.

With the global IoT payments market projected to grow by 66% and reach approximately USD 5.4 trillion by 2028, the initiative aligns with India's "Payments Vision 2025," which emphasizes developing secure and innovative payment frameworks. While the move promises to expand UPI's versatility and enhance consumer convenience, it presents challenges related to user trust, security, and regulatory oversight. Experts raise concern about the importance of robust authentication and fraud prevention mechanisms to ensure safe adoption of this technology.

RBI Launches 'Theme Neutral' 'On Tap' Facility for Regulatory Sandbox

The Reserve Bank of India (**"RBI"**) has introduced the 'Theme Neutral' 'On Tap' facility under its Regulatory Sandbox framework, aimed at promoting continuous fintech innovation. Since launching the Regulatory Sandbox in 2019 and completing four thematic cohorts, RBI had moved toward an 'On Tap' facility for closed cohorts in 2021. It allowed applicants to submit proposals outside fixed windows but still within defined thematic limits. Now, based on stakeholder feedback and evolving market needs, RBI has expanded this approach further to a 'Theme Neutral' model.

This differs from the previous thematic cohorts and allows innovators to submit applications at any time, without any restrictions of pre-defined themes. It reflects RBI's adaptive stance toward the rapidly evolving FinTech landscape. The adaptive model furthers the goals of enhancing flexibility and timely engagement with FinTech startups. While it is still nascent, it promises accelerated innovation cycles and improvement in evaluation capacity.

NPCI Enforces New UPI Security Guidelines to Mitigate Mobile Number Reassignment Risks

The National Payments Corporation of India ("**NPCI**") has introduced new guidelines for Unified Payments Interface ("**UPI**") transactions, introducing regulatory checks to prevent oversights caused by mobile number reassignment and to curb fraud. The framework is binding on all member banks, Payment Service Providers ("**PSPs**"), and third-party apps and requires weekly updating of mobile number records via the Mobile Number Revocation List ("**MNRL**"), in line with the Department of Telecommunications' ("**DoT**") 90-day dormancy rule. UPI IDs assigned to inactive or reassigned mobile numbers will now be systematically deactivated, placing the onus on users to ensure their records remain current.

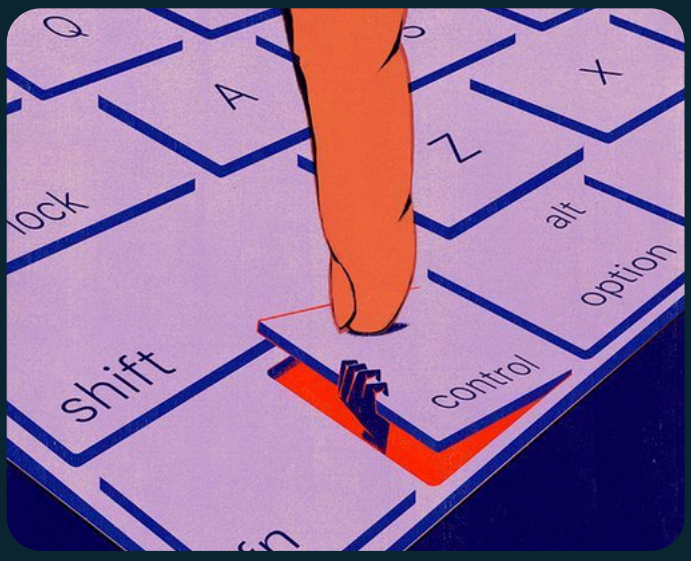
Additional safeguards include a blanket prohibition on capturing user consent for mobile number seeding during or before transactions and makes explicit opt-in mandatory. While the regime is expected to fortify digital payments and reduce operational loopholes, experts caution about the compliance burden on banks and highlight challenges for users with ported or legacy accounts.

RBI Directs NBFC's to Exclude Default Loss Guarantees from Loan Provisioning

The RBI, in Chapter VI of the aforementioned Directions, directs Non-Banking Financial Companies ("**NBFCs**") to exclude Default Loss Guarantees ("**DLGs**") from the calculation of expected credit losses on loans sourced through digital lending platforms ("**DLPs**"). DLGs typically act as credit enhancements, such as fixed deposits or lien-marked securities, that DLPs provide to NBFCs to cover possible borrower defaults. However, this policy shift mandates NBFCs to fully account for expected credit losses without factoring in such credit enhancements.

By excluding these guarantees, RBI is effectively requiring NBFCs to fully recognise credit risk on such loans without relying on DLP-provided collateral. This pushes NBFCs to strengthen their underwriting capabilities and lessens dependency on digital lending partners' risk mitigations. It also represents RBI's intent to tighten risk management standards in the growing digital lending space and ensure realistic loan loss recognition.

The directive is viewed as RBI's effort to enhance financial stability and accountability within the digital lending ecosystem, pushing for more robust risk management by NBFCs. However, for DLPs, this could lead to funding and operational challenges, as NBFCs will become more cautious in sourcing loans through these channels due to higher provisioning costs, potentially reducing their appeal as loan originators.



RBI Notifies Digital Lending Directions, 2025

The RBI notified the Digital Lending Directions, 2025 (**"the Directions"**) to consolidate and strengthen the regulatory framework governing digital lending. The Directions aim to improve transparency, borrower protection, and accountability among Regulated Entities (**"REs"**) and Lending Service Providers (**"LSPs"**).

The Directions require lenders to display clear and comparable loan options with differing terms to facilitate informed decision-making for borrowers. The Directions also provide for Mandatory app registration with the Centralised Information Management System (**"CIMS"**) to detect fraudulent platforms and mitigate concentration risk. The framework also mandates explicit borrower consent for data collection in alignment with the Digital Personal Data Protection Act, 2023. Further, loans must be disbursed directly into borrowers' bank accounts with clear disclosures on loan terms and grievance redressal mechanisms.

The Directions aim to increase transparency in a competitive market. Borrowers will also benefit from uniform disclosures that simplify comparison of loan options. The measures aim to enhance borrower protection, promote responsible lending, and ensure better oversight of digital lending platforms.

RBI Established the Payments Regulatory Board

RBI has notified the creation of the Payments Regulatory Board (**"PRB"**) through the Payments Regulatory Board Regulations, 2025 (**"2025 Regulations"**), marking a key change in India's payment system governance. The PRB replaces the earlier Board for Regulation and Supervision of Payment and Settlement Systems (**"BPSS"**) which operated under a 2008 framework. Unlike the BPSS, which functioned mostly as an advisory and supervisory entity with limited delegated powers, the PRB possesses enhanced statutory authority under the Payment and Settlement Systems Act, 2007, as elaborated in the 2025 Regulations.

The PRB's mandate covers all entities involved in payment and settlement systems, including Prepaid Payment Instrument issuers, Payment Aggregators, and Payment Banks. It is empowered to formulate regulations, issue directions, and ensure the safety, efficiency, and integrity of payment systems nationwide. Thus, it consolidates supervisory responsibilities, streamlines decision-making processes and enables quicker resolution. The regulations intend to provide clearer accountability and stronger regulatory oversight in an era marked by rapid digital payments growth and increasing complexity.

RBI Mandates Adoption of DoT's Financial Fraud Indicator to Combat Cybercrime

The RBI has directed all Scheduled Commercial Banks, Small Finance Banks, Payments Banks, and Co-operative Banks to implement the Financial Fraud Indicator (**"FRI"**) developed by the DoT. This initiative aims to strengthen the fight against cyber fraud impacting digital payments and banking customers across India. FRI operates through real-time data exchange with DoT's Digital Intelligence Platform, integrating information on high-risk mobile numbers identified via cybercrime reports, revoked connections, and intelligence from various stakeholders.

By classifying mobile numbers into risk categories, the FRI empowers banks and fintech players to take swift and targeted preventive measures, including transaction declines, customer alerts, and blocking suspicious activities. The model bridges telecom and financial sectors, creating a defense against fraud and building consumer trust in India's UPI-based payment ecosystem. Experts believe that FRI's AI-driven scoring and feedback mechanism are transformative tools potentially setting a global example for integrated fraud mitigation.


ARTIFICIAL INTELLIGENCE

INDIA SETS UP COMMITTEE TO REVIEW COPYRIGHT LAW FOR GENERATIVE AI

The Department for Promotion of Industry and Internal Trade (**"DPIIT"**) has set up a multi-stakeholder committee to review how India's Copyright Act, 1957, applies to AI-generated works. The committee includes representatives from MeitY, NASSCOM, leading IP lawyers, and academics. The committee's mandate is fourfold: (i) identify copyright challenges posed by generative AI, (ii) assess the adequacy of current provisions under the 1957 Act, (iii) recommend necessary legislative amendments, and (iv) prepare a working paper for policy action.

This review follows rising litigation against AI developers as witnessed in the most recent Delhi High Court case brought up against OpenAI. Indian press agencies and publishers sued OpenAI, arguing that training models on copyrighted material without consent infringes their rights. Such disputes underscore the urgency of clarifying ownership and liability in AI-produced content.

Legally, the committee signals the government's first explicit recognition that generative AI strains India's copyright regime. Its recommendations could shape whether India adopts stronger protections, exemptions, or a new regulatory framework altogether.

'TAKE IT DOWN' ACT ESTABLISHES FEDERAL NOTICE-AND TAKEDOWN FRAMEWORK FOR NON-CONSENSUAL INTIMATE IMAGERY

President Donald Trump signed the bipartisan 'Take It Down Act', the first federal law addressing and limiting the malicious use of AI to create deepfake non-consensual intimate imagery. It mandates 'covered platforms' (including websites, and applications hosting user-generated content) to implement notice-and-takedown procedures. Platforms must remove content within 48 hours of receiving a valid user notification.

The new law strengthens the existing framework created by thirty US states that already have laws in place to address non-consensual intimate imagery. Criminal penalties range from 18 months to three years imprisonment, with enhanced sentences for minor-related offenses. The legislation sets a precedent for AI-specific federal regulation, potentially influencing future algorithmic accountability measures and platform liability standards across digital content moderation.

UK Enacts Data (Use and Access) Act 2025 to Streamline Data Compliance and Fuel Innovation

The Data (Use and Access) Act 2025 (**"the Act"**) received Royal Assent marking a significant step in the United Kingdom's post-Brexit data protection strategy. Rather than replacing the UK GDPR or the Data Protection Act 2018, the Act introduces targeted amendments intended to simplify compliance and encourage innovation. It includes the creation of a new basis for processing under "recognised legitimate interests," adjustments to the rules governing automated decision-making, extended timelines for responding to data subject access requests, and expanded exemptions for the use of cookies. The Act also provides for the development of smart data schemes, digital identity verification services, and a National Underground Asset Register.

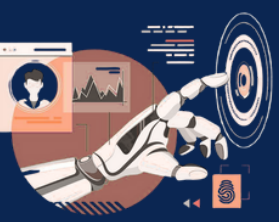
Parliamentary debate focused heavily on the use of copyrighted works in training artificial intelligence systems. The House of Lords sought stronger transparency obligations, but the government declined to include them, instead committing to address the issue in future legislation. The Act reflects a deliberate policy choice: advancing regulatory flexibility and economic competitiveness, while deferring comprehensive resolution of rights-based concerns.

SEBI Released a Consultation Paper on Guidelines for Responsible AI/ML Usage in Indian Securities Markets

The Securities and Exchange Board of India ("**SEBI**") released a consultation paper on guidelines for the responsible use of Artificial Intelligence and Machine Learning ("**AI/ML**") in the Indian securities markets. The draft aims to regulate the deployment of AI/ML technologies by market intermediaries, stock exchanges, and related entities to ensure transparency and accountability. Key provisions include mandatory governance frameworks with designated AI ethics officers, periodic risk assessments addressing data quality, model bias, and systemic impacts, and strict requirements for transparency and explainability of AI models.

Entities are expected to comply with the Digital Personal Data Protection Act, 2024 ("**DPDP Act**") and institute data privacy and security safeguards. A central theme of the guidelines was the upkeep and supervision of any deployed technology. This is reflected in provisions stating that critical AI-driven decisions in trading or compliance must allow for human review. The paper also encourages capacity building through training on AI ethics and regulatory compliance.

THE EUROPEAN UNION UNVEILS NEW ARTIFICIAL INTELLIGENCE CODE AMIDST INDUSTRY PUSHBACK



The European Union has introduced new rules and guidelines under the General-Purpose AI (“**GPAI**”) Code of Practice as a voluntary instrument to help AI developers comply with the AI Act’s legal requirements on transparency, copyright, and public safety. Being a soft-law tool, the main aim is to provide guidance to the industry and help enter into compliance in the interim before the AI Act achieves full effect. By providing an in-depth, easy-to-navigate guide and promoting the multi-stakeholder approach, the EU is not only allowing companies to meet the regulations, but also to foster the further evolution of the latter.

Its primary aim is three-pronged, creating practical requirements on transparency, copyright, and systemic-risk safeguards through documentation of model training, enactment of incident-reporting mechanisms, and the conduct of safety evaluations. The code also effectively operationalises obligations under Articles 53 and 55 of the AI Act, which lay out the obligations of general providers of AI such as Google and OpenAI, which have signed onto the Code.

Legally, the Code provides a “presumption of conformity,” reducing liability risks for compliant providers. While voluntary, it is expected to carry de facto regulatory weight, as adherence will likely be demanded by regulators, courts, and market actors until the final harmonized standards are implemented.


DATA PRIVACY

A NEW ERA OF DATA CONTROL: NEW ZEALAND'S CUSTOMER AND PRODUCT DATA ACT

New Zealand's Customer and Product Data Act is officially in force, marking a monumental shift in how consumer data is managed. The Act establishes a "consumer data right," giving individuals control over their personal and product data, empowering them to securely share it with trusted third parties. This is a significant move away from the traditional model where businesses hold exclusive control over customer information.

This development has strong parallels with India's evolving data privacy landscape. While New Zealand focuses on a "consumer data right," India's Digital Personal Data Protection Act, 2023 ("**DPDP Act**"), establishes a "data principal's right" to control their data. Both frameworks share a common goal of empowering individuals and fostering a consent-based data ecosystem. As India continues to draft and implement its rules, it can draw valuable insights from New Zealand's step-by-step approach. The New Zealand model offers a practical case study for how to introduce a consumer data right, manage industry-specific challenges, and balance innovation with robust security and privacy protections.



India's DPDP Act Falls Short of GDPR Equivalence

The European Data Protection Supervisor (**"EDPS"**) has refused the transfer of personal data by the European Investment Bank (**"EIB"**) to India, which underscores the persistent disparity between the developing privacy laws of India and the strict regulatory environment of the EU and its privacy law, the General Data Protection Regulation (**"GDPR"**). Although in 2023, India passed the DPDP Act, the legislation is not in effect, and the draft regulations are still being discussed in 2025. This lack of enforcement, and institutional practice leaves India without an equivalent degree of protection, which is one of the conditions of adequacy recognition under Article 45 of the GDPR.

Permissible derogations from adequacy recognition as suggested by the EDPS under Article 49 of the GDPR are limited in scope. These are aimed only at exceptional and one-off transfers in the public interest, rather than systemic and routine flows of data. Practically, this compels organisations such as the EIB to use standard contractual clauses (**"SCCs"**) or tailor-made data transfer contracts, pending the future adequacy arrangement. This decision highlights a key aspect; until India proves its strong enforcement, an independent control and efficient remedies of the DPDP Act, its data protection system cannot be trusted by the EU in terms of its free data transfers.

INDIA MOVES TOWARD DYNAMIC PRIVACY WITH REAL-TIME CONSENT CHECKS PROPOSED UNDER DPDP ACT

The proposed real-time Application Programming Interface ("**API**") based Consent Management System ("**CMS**") under the DPDP Act represents a fundamental shift in the Indian privacy scheme. The draft also shifts to intent-based, dynamic consent checks prior to personal data processing, which complies with international best practices of lawfulness, fairness and accountability.

Compliance artifacts are incorporated into the framework and operationalised statutory Data Principal rights, including withdrawal, correcting, and erasing data, by mandating immutable audit trails and user-facing dashboard.

This is legally enforceable as it gives the DPDP Act more power since consent is not merely formal, but a continuous and provable state of processing data. The demand for independence of consent managers of data fiduciaries is also reminiscent of the conflict-of-interest protections found in international regimes such as the GDPR. Further, the industry will be burdened with huge compliance overheads including the redesigning of IT systems, making them interoperable and adding real-time APIs. When applied successfully, the CMS may bring the privacy regime in India at an equivalent position to the GDPR.

NASSCOM WEIGHS COSTS AND BENEFITS OF INDIA JOINING GLOBAL CBPR PRIVACY FRAMEWORK

Nasscom's cautious stance on India's potential joining of the Cross Border Privacy Rules ("**CBPR**") forum highlights the fine line between supporting digital trade and avoiding regulations that burden it. CBPR, which was elaborated by the US government, is a voluntary, certification-based framework. It enables participating countries and companies to demonstrate compliance with recognised privacy standards, thereby fostering trust and interoperability in global data exchanges. The privacy enforcement Global Cooperation Arrangement for Privacy Enforcement ("**Global CAPE**") that accompanies it introduces an enforcement aspect with which regulators cooperate.

Legally, the Indian involvement may be an indicator of following the international privacy standards, which will build trust in its DPDP Act. However, there are very pertinent questions: such certification could overlap duplicate compliance requirements already imposed by the DPDP Act and various sectoral regulators, potentially increasing compliance costs. India has to evaluate whether the CBPR recognition would simplify the international data flows or just increase an extra regulatory level. An agreed-upon pathway (with interoperability objectives of CBPR combined with domestic legislation) may provide India with a tactical edge in international data regulation.

IAMAI RAISES CONCERN OVER IMPACT ON STARTUPS AND MSMES DUE TO DPDP COMPLIANCE.

The Internet and Mobile Association of India ("**IAMAI**") has raised concerns regarding the operational challenges posed by the DPDP Rules, 2025 especially on startups and micro, small, and medium enterprises ("**MSMEs**"). IAMAI's submission to MeitY highlights that the extensive compliance requirements under the DPDP Act and draft rules could disproportionately impact smaller entities at the cost of innovation and growth.

The ambiguity in the designation criteria for "Significant Data Fiduciaries" ("**SDFs**"), where companies processing large volumes of personal data face stricter obligations.

IAMAI contended that vague definitions around data volume and sensitivity may unfairly burden Indian startups, by subjecting them to compliances intended for larger entities. Additionally, stringent restrictions on cross-border data transfers risk isolating Indian companies from international markets, adversely affecting India's digital economy, including outsourcing services. The association called for delayed implementation timelines of up to 24 months to enable equitable adaptation and called for more explicit guidelines to clarify compliance expectations.

CONTRIBUTORS

WRITERS

TRISHNA AGRAWALLA

ANJALI PANDE

PRATYUSH SINGH

ANJALI DHAKAD

MAITHILI DUBEY

SUBHASIS SAHOO

EDITOR

PRATYUSH SINGH

DESIGNERS

DIYA JAIN

ISHANI GARG

MAITHILI DUBEY

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTAGRAM LINKEDIN EMAIL