Luthra and Luthra

LAW OFFICES INDIA

Telecommunications, Media and Technology (TMT) Newsletter

January-March 2026 Edition

Luthra and Luthra
LAW OFFICES INDIA

INSIDE

EMERGING TECHNOLOGIES

- **Indian Computer Emergency Response Team (CERT-In), in collaboration with SIA-India, releases Cyber Security Framework and Guidelines for Space including Satellite Communication**
- **DPIIT Revises Definition of "Deep Tech Startup" Under Fresh Startup Notification, 2026**

CASE LAW & LITIGATION UPDATES

- **Hon'ble Supreme Court of India Rules that Telecom Spectrum, cannot be subjected to Insolvency Proceedings under the Insolvency and Bankruptcy Code, 2016**
- **Hon'ble Supreme Court Holds Telecom Licensees Liable to Pay Spectrum Reserve Price from the Date of Licence Cancellation, Rejecting TDSAT's Diluted Interpretation**

TELECOMMUNICATIONS

1. Telecom Regulatory Authority of India (TRAI) releases Consultation Paper on Review of Rating of Properties for Digital Connectivity Regulations, 2024

TRAI on February 27, 2026 released a Consultation Paper on Review of Rating of Properties for Digital Connectivity Regulations, 2024 **(DCR 2024)**. The DCR 2024, notified on October 25, 2024, consolidates the framework for assessing digital connectivity readiness within properties. Digital connectivity within properties has emerged as an area key importance between service providers and consumers alike.

The framework sets out parameters for evaluating digital connectivity readiness of properties and covers Residential, Government Properties, Commercial Establishments, Stadiums/Sport Arenas, Transport corridors and more.

The DCR 2024 is supplemented via the Rating Manual, Digital Connectivity Rating Agencies **(DCRAs)** and Property Managers.

This Consultation Paper arises from stakeholder feedback on improving and refining the DCR 2024 framework. A few key highlights of proposed changes include:

Expanding the five-star scale to a nine-level system, using half-star increments to reflect connectivity more precisely - TRAI noted that the existing five-star scale diluted the incremental improvements to the property as each incremental star required approximate a 15-point increase. A nine-star scheme provides more granularity to the digital readiness of a property.

Design-Stage Assessment - Introducing evaluation and certification for properties under construction and aligning them with properties completely constructed – a new certificate "designed for xx stars" is being proposed to address the projected level of readiness, provided the measures identified in the design plan are actually implemented.

Optional Connectivity Audit - Recognition of an optional connectivity audit for evaluation and improvement purposes without apply for rating of digital connectivity. This would help Property Managers in identifying areas of improvement and take on changes without having the property labelled to a specific rating level.

The changes are being proposed via amendments to the DCR 2024 and the Rating Manual.

The amendments, if enacted, will widen the reach of the current framework including properties under construction and pre-rating corrective measures within its ambit. This is especially beneficial for the real-estate sector as a significant portion of real-estate transactions are undertaken at the construction stage itself. The time window for sending comments has been closed for this consultation paper.

2. TRAI released the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026

TRAI on March 13, 2026 released the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 **(Draft Regulations)**, inviting comments from industry stakeholders.

The Telecom Commercial Communications Customer Preference Regulations, 2018 **(TCCPR)** were issued by TRAI on July 19, 2018 to address the growing instances of Unsolicited Commercial

Communications (**UCC**) such as spam calls and messages. The same have been amended from time to time to bring them up to speed with the evolving challenges in the Telecom sector.

The Draft Regulations propose amendments to specifically address issues pertaining to - reporting of UCC to the DLT platform of access providers, the UCC complaints reported by the customers through their phone dialer apps and third-party call management apps and the obligation on the providers of such apps to comply with regulatory provisions. The Draft Regulations also realign provisions of the TCCPR with the Telecommunications Act, 2023 **(Telecom Act)** including a revised definition of regulatory sandbox, replacing the 'Telegraph Act, 1885' with the 'Telecom Act' and 'telegraph' with 'telecommunication' wherever applicable.

A few key highlights of the proposed changes include:

Changes to the definition of Relationship and Explicit consent – Telemarketers can send commercial communication to recipients only via Explicit Consent or by virtue of having Inferred Consent on account of an existing Relationship with the same.

Relationship was earlier defined as a prior or existing business/commercial or social connection with a subscriber, based on transactions in the past twelve months, inquiries/applications in the past three months, or voluntary two-way communication initiated by both sides for social reasons, and not already terminated by either party.

The proposed amendment reads down and clarifies the definition of Relationship notably (a) limiting duration of Relationship to only the duration/discharge of contract between the parties, by removing the conflicting provision under clause 2 (bb) (ii) where a Relationship was inferred to exist basis any purchase/transaction between the sender and the receiver in the last twelve months (b) removing inquiry from the definition of Relationship and (c) removing sub-clause (iii) on existence of Relationship 'for social reasons' to avoid UCCs under the garb of inquiry or for social reasons.

Further, a new definition of Explicit Consent is also proposed that expands it to include consent obtained via any verifiable means outside the Consent Registration Function framework and subsequently registered in the Consent Register. This addition enables orderly migration and digitization of legacy offline consents to the Consent Register, which were excluded earlier.

Changes in treatment of Application to Person (A2P) Calls – The Draft Regulations introduce a new definition for A2P calls covering, calls initiated by application, software system, or automated platform without direct human dialing and delivered to an individual telecom subscriber, including using autodialing, robocalls and/ or prerecorded/ artificial voice technologies. Further, the Draft regulation also introduces a termination charge of Rs. 0.05 (five paisa only) per minute for A2P calls, as a deterrent against misuse of A2Ps calls for UCC.

Leveraging AI/ML-based UCC detection systems – An AI/ML-based action matrix to capture senders of UCC is also proposed. Every access provider shall identify and flag the calling line identification of senders of suspected UCCs, and share the same with the distributed ledger technology **(DLT)** platform within two hours for the originating access providers.

Every originating access provider shall then (a) notify the sender via SMS/mail that their communication has been flagged as a suspected UCC and (b) share the unique KYC identifiers of the suspected sender

onto DLT platform to all access providers who in turn, (c) will check all communication shared by the said sender for suspected UCCs flags across all assigned Calling Line Identities **(CLIs)** and (d) share the same back onto the DLT. If more than five suspected UCC flags have been identified against the sender in the preceding ten days, then the concerned access providers shall take actions against the sender. These actions range from a re-KYC of the sender, barring the sender from using the access providers' network to blacklisting of the sender devices used in making UCCs by access providers for up to one year.

Change to the Treatment of Call management apps – Call management apps are expressly barred against tagging/blocking/filtering calls from designated numbers. The proposed amendment further expands the scope of this restriction to include "give any treatment to such calls different from those applicable for genuine communication" to ensure a balance between commercial interest of the telemarketers and preservations of consumer rights. Any contravention by any call management app in this regard will be treated as a violation of the said application's obligations under the Information Technology Act, 2000 and may lead to removal of their safe harbor protection.

The amendment further imposes an obligation on the Call management apps to send a report to the DND registry maintained by the access providers of all UCC marked as spam by their customers.

Streamlining grievance redressal and complaint mechanisms – The proposed amendment introduces an additional a time-limited appellate process for complaint redressal to be set up by every Access Provider. This Appellate Authority shall be a designated employee working at the senior management level of the respective Access Provider. Further, the name and contact details of such designated officer shall be duly published at a prominent place on the official website of the concerned access provider.

The Draft Regulations are indicative of TRAI's continued commitment to refining balance between commercial interest of telemarketers, preservation of consumer rights and the rights of other stakeholders. The Draft Regulations are open for counter-comments till April 27, 2026.

3. TRAI released Consultation Paper on Review of Tariff for Domestic Leased Circuits (DLCs)

TRAI on January 23, 2026 released a Consultation Paper seeking stakeholder comments on the review of tariff for Domestic Leased Circuits (DLCs). DLCs are dedicated communication links used by enterprises and institutions for secure and reliable data transmission.

The Consultation Paper comes in wake of the Draft Telecommunications (Authorisation for Provision of Main Telecommunication Services) Rules, 2025, wherein the scope of providing DLCs was expanded to include entities having Internet Service Provider **(ISP)** authorization. Thereby significantly expanding the existing market.

This inclusion necessitated a rework of the existing tariff framework and also raised concerns arising from operational synergies/dependencies associated with smaller ISPs (such as ISPs with ISP-B or ISP-C authorizations) and other industry stakeholders (such as infrastructure providers and ISP-NLDO relationships.

TRAI explores several key sectoral questions via this consultation paper such as the (a) the likely impact on competition and tariffs in the DLC sector, if the ISPs are permitted to provide DLCs in the future? (b) whether MPLS-VPN DLCs should be brought under the tariff regulation framework? (c) the need for

revision of distance-based pricing and (d) need for prescribing separate ceiling tariffs for remote and hilly areas? among others.

The window for submitting comments to the Consultation Paper is now closed. We expect TRAI to release their recommendations basis this consultation soon.

4. **TRAI issues Recommendations on The Auction of Radio Frequency Spectrum in the Frequency Bands Identified for International Mobile Telecommunications (IMT)**

TRAI on February 24, 2026 issued recommendations regarding the auction of radio frequency spectrum in various bands identified for International Mobile Telecommunications (IMT) (**Recommendations**). These recommendations were sought by the Department of Telecommunications (**DoT**) via their letter dated May 15, 2025 and stem from the several key sector developments since the auction of spectrum in certain frequencies in June 2024, including the release of spectrum assigned administratively to TSPs, availability of spectrum for reframing and on account of consideration by the DoT of auction of spectrum in the certain frequency bands.

As part of the consultation process, prior to the release of these Recommendations TRAI had released a consultation paper on the "Auction of Radio Frequency Spectrum in the Frequency Bands Identified for International Mobile Telecommunications (IMT)" on September 30, 2025 followed by submission of comments and counter-comments and a stakeholder open house discussion on December 12, 2025.

The recommendations outline the framework for assigning spectrum through auction, including aspects related to frequency bands, reserve prices, block sizes, and auction methodology wholistically addressing (a) stakeholder concerns on the terms and conditions for the auction of frequency bands identified for IMT and (b) issues related to valuation and reserve price for the spectrum.

A few key highlights of the Recommendations include:

Spectrum Auction – Entire available spectrum in the existing frequency bands (viz. 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2300 MHz, 2500 MHz, 3300 MHz and 26 GHz) should be auctioned, this auction should be on a telecom circle basis and the validity of spectrum so auctioned should be for 20 years. Certain quantum of spectrum in specific bands should be set aside for ISP, M2M and captive use.

Valuation and Reserve Price – Valuation of the spectrum was determined basis (a) for bands where the frequency is being offered for the first time, a fresh valuation exercise shall be undertaken by the DoT (b) For LSAs where the spectrum was put to auction in the previous auction, the auction determined prices duly indexed should be used for arriving at the reserve prices for the next auction.

Through these recommendations, TRAI seeks to address concerns regarding over-supply of spectrum and introduces a market-driven approach to spectrum allocation while maximizing the sale of erstwhile unsold spectrum.

BROADCASTING & MEDIA

5. **Ministry of Information and Broadcasting (MIB) Notifies TV Rating Policy (TRP) 2026 to Strengthen Transparency, Accountability and Credibility of Television Audience Measurement in India**

MIB on March 27, 2026 released the **TV Rating Policy 2026** to strengthen independence, transparency, and accountability in television audience measurement across linear TV and digital viewing platforms.

Key Highlights:

Easier Entry - Net worth requirement for TV rating agencies reduced from ₹20 crore to ₹5 crore. Only companies incorporated in India under the Companies Act, 2013 with a minimum net worth of Rs. 5 crore can register as Television Rating Agencies.

Cross-Holding & Conflict-Free Governance - Strict crossholding and conflict-of-interest restrictions apply between rating agencies on one side and broadcasters, advertisers, and advertising agencies on the other, with at least 50 percent independent directors mandated on the Board. Registration is granted for a 10-year period, backed by Bank Guarantees totalling ₹1 crore.

Enhanced Accuracy, Privacy and Panel Expansion - Ratings must be technology-neutral and capture viewership across cable TV, DTH, terrestrial TV, OTT platforms, connected TVs and other feasible platforms. Agencies are required to deploy at least 80,000 metered homes within 18 months of registration, with a phased increase of 10,000 homes per year up to 1,20,000, while ensuring representative coverage and excluding landing page viewership from ratings. Privacy safeguards and compliance with the Digital Personal Data Protection Act, 2023 are expressly mandated.

Transparency & Data Access - Agencies must publish detailed rating methodologies, coverage details, ownership patterns, audit reports, rate cards, and grievance statistics on their websites. Rating data is to be made available to all interested stakeholders on a transparent, non-discriminatory basis, subject to fair-usage conditions.

Dual-Audit System - Quarterly internal audits and annual independent audits, plus field inspections by the Ministry.

Landing Page Rules - Landing page viewership are to be excluded from ratings, but can be used only as a marketing tool.

Grievance Redressal & Compliance - Each agency must put in place a multi-tier grievance redressal system, including appointment of one or more Nodal Officers, acknowledgement of complaints, resolution within prescribed timelines, and an Appellate Authority to handle unresolved or escalated grievances. Aggregate grievance data must be maintained and published for accountability. Nodal officers to resolve complaints in 10 days; penalties for violations range from suspension to cancellation including forfeiture of bank guarantee ranging from ₹25 Lakhs to 75 Lakhs for subsequent violations.

The TRP Policy 2026 replaces the 2014 guidelines, reinforcing a **fair, competitive, and well-governed broadcasting ecosystem.** If effectively implemented, the TRP Policy 2026 is expected to enhance confidence in India's television audience measurement ecosystem by tightening governance standards, expanding the measurement universe, and providing clearer enforcement guidance and penalties against errant rating agencies.

6. **MIB highlights Strengthened Anti-Piracy Measures Under Cinematograph (Amendment) Act, 2023, Including Up to 3 Years Imprisonment and Fines up to 5% of Production Cost while giving blocking orders to Telegram**

On March 18, 2026, the MIB through a written reply in the Lok Sabha and an accompanying PIB press release, outlined how the Cinematograph (Amendment) Act, 2023, read with provisions of the Information Technology Act, 2000 **(IT Act)** and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, **(IT Rules, 2021)** is being used to strengthen the legal framework against online film piracy.

Key Measures:

Institutional Mechanism - MIB has established an institutional mechanism through designated Nodal Officers of MIB and Central Board of Film Certification to receive complaints, in a prescribed format, from copyright holders, their authorized representatives and other complainants regarding exhibition of pirated or infringing copies of films on the internet. Upon receipt of such complaints, intermediaries are notified by the appropriate government or its agency under Section 79(3)(b) of the IT Act to remove or disable access to the identified links, consistent with the intermediary due diligence and takedown obligations under the IT Rules, 2021 relating to content that infringes intellectual property rights.

Legal Framework - New Sections 6AA and 6AB of the Cinematograph Act, 1952 prohibit unauthorized recording and transmission of films. Section 7(1A) provides that contravention of these provisions is punishable with a minimum of three months' imprisonment and a fine of Rs. 3 lakh, which may extend to three years' imprisonment and a fine of up to 5% of the audited gross production cost. Section 7(1B)(ii) of The Cinematograph Act, 1952 further enables the Government to notify intermediaries hosting pirated content under Section 79(3) of the IT Act. Platforms must ensure their resources aren't used to infringe copyrights, trademarks, or other proprietary rights.

Enforcement Actions - Acting under the above framework, the Government notified the Telegram app as an intermediary under Section 79(3)(b) on March 11, 2026, directing it to remove or disable access to 3,142 channels publishing unauthorized content owned by or licensed to various content owners, OTT platforms and film producers. In parallel, access to approximately 800 websites hosting pirated content has been disabled through internet service providers.

These actions reflect a coordinated, statute-backed approach to tackling digital film piracy by combining criminal penalties under the Cinematograph (Amendment) Act, 2023 with intermediary liability and proactive takedown measures under the IT Act and the IT Rules, 2021.

FINTECH

7. Reserve Bank of India (RBI) Strengthens Grievance Redressal: Issues Internal Ombudsman Directions and Integrated Ombudsman Scheme, 2026

The RBI on January 14, 2026 through a press release, announced the issuance of the Reserve Bank of India (Internal Ombudsman) Directions, 2026, finalizing the draft Master Direction on internal ombudsman frameworks for regulated entities first released on October 7, 2025.

The press release confirms that six separate Directions have been notified for (a) commercial banks, (b) small finance banks, (c) payments banks, (d) non-banking financial companies, (e) non-bank prepaid payment instrument issuers, and (f) credit information companies, with the objective of strengthening internal mechanisms for resolution of customer grievances within these entities.

Key Highlights:

Entity-specific coverage and thresholds - Each category of regulated entity is covered by its own set of Internal Ombudsman Directions, which apply above specified asset-size or business-volume thresholds. This creates a harmonised baseline for second-level complaint review across large, retail-facing institutions while permitting proportionate treatment of smaller entities that fall below the thresholds.

Strengthened internal review and escalation - Covered entities are required to put in place a robust Internal Ombudsman framework, including appointment of an independent Internal Ombudsman at a sufficiently senior level with a fixed tenure and safeguards against arbitrary removal. Complaints that are rejected or only partially allowed by the internal grievance redress mechanism (subject to limited exclusions such as matters under investigation or sub-judice disputes) are to be automatically escalated to the Internal Ombudsman for a reasoned decision before closure.

Governance, reporting and linkage with external ombudsman - These directions prescribe timelines and procedures for referring complaints to the Internal Ombudsman, communicating decisions to customers, and reporting key metrics (such as volume, reversal rates and root-cause trends) to senior management and the board.

Together with the RBI's broader overhaul of its external ombudsman scheme, these directions are intended to create a more structured grievance redress ecosystem, improving accountability of regulated entities and reducing the need for customers to escalate disputes to the RBI Ombudsman.

8. RBI Issues Draft Amendment Directions for 'Advertising, Marketing and Sales of Financial Products and Services by Regulated Entities'

RBI via notification dated February 11, 2026 released draft amendment directions on 'Advertising, Marketing and Sales of Financial Products and Services by Regulated Entities.' **(Draft AMS Amendment Directions)**. The Draft AMS Amendment Directions seek to move beyond the existing customer appropriateness and suitability instructions, which currently has a limited applicability, and instead tries to establish a harmonised conduct framework for all banks and non-banking financial companies **(NBFCs)**, including co-operative banks and all-India financial institutions, when they advertise, market and sell their own or third-party financial products and services.

Key Highlights:

Board-approved policy and suitability standards - Regulated entities **(REs)** must adopt a comprehensive, board-approved policy governing advertising, marketing and sales across physical and digital channels, covering both in-house and third-party products.

Mis-selling safeguards, incentives and "dark patterns" - The draft directions define and prohibit mis-selling, restrict forced bundling of third-party products with core banking services, and bar RE staff and direct sales / marketing agents from receiving incentives directly or indirectly from third-party product providers. REs must ensure that customer interfaces (including mobile apps and web journeys) do not deploy manipulative "dark patterns" and are subject to internal testing and audit. Where mis-selling is established, REs would be required to refund amounts paid and compensate customers for resultant losses under a board-approved policy.

Third-party distribution oversight and next steps - The draft directions also tighten governance around direct sales agents, direct marketing agents and other outsourcing / referral arrangements, including clearer identification of such agents, calling-hour and "do-not-disturb" safeguards, training and monitoring requirements, and stronger grievance-redressal processes.

9. RBI Issues Draft Amendment Directions for 'Review of Framework of Limiting Customer Liability in Digital Transactions'

On March 6, 2026, the RBI issued draft Amendment Directions titled "Review of Framework of Limiting Customer Liability in Digital Transactions" pursuant to the Statement on Developmental and Regulatory Policies dated February 6, 2026. The draft amends the existing Responsible Business Conduct Directions for different categories of banks and seeks to update RBI's 2017 framework on unauthorised electronic banking transactions in light of the scale of digital payments and the evolving fraud landscape.

Key Highlights:

Broader coverage and clearer definitions - The draft Directions broaden the framework from "unauthorised electronic banking transactions" to a wider category of "fraudulent electronic banking transactions" across channels such as internet and mobile banking, cards, UPI and other electronic funds transfers. They also spell out what constitutes authorised versus fraudulent transactions, including cases where customers are coerced into approving a transaction or are tricked into sending money to scammers impersonating legitimate recipients.

Rebalanced liability and small-value compensation - The draft proposes a graded liability framework that preserves zero liability for customers where fraud occurs due to bank deficiencies or third-party breaches, subject to timely reporting, and clarifies when customers will bear limited liability in cases involving their own negligence. In addition, a common small-value compensation mechanism is proposed under which individual customers who suffer genuine fraudulent losses up to a specified threshold (currently up to ₹50,000) may receive capped, one-time compensation (up to ₹25,000) where the fraud is reported both to the bank and to the National Cyber Crime Reporting Portal / helpline within a prescribed time window.

Bank duties, negligence and third-party breaches - The draft Directions clarify what will be treated as negligence on the part of banks (for instance, failure to maintain secure systems, non-issuance of transaction alerts or lack of reporting channels), and on the part of customers (such as sharing passwords/OTPs or ignoring fraud alerts). They also define "third-party breaches" to include failures at intermediaries such as payment gateways, telecom service providers or third-party application providers and link such failures to the liability framework, placing greater responsibility on banks to manage their outsourced and partner arrangements.

10. RBI releases Master Direction on Unique Identifiers in Financial Markets

On March 27, 2026, the RBI issued the Master Direction – Reserve Bank of India (Unique Identifiers in Financial Markets) Directions, 2026 **(Directions)**, consolidating its earlier instructions on implementation of the Legal Entity Identifier **(LEI)** and Unique Transaction Identifier **(UTI)** across financial markets regulated by RBI. The framework seeks to standardise the use of global identification standards for counterparties and over-the-counter **(OTC)** derivative transactions, improve data quality for risk monitoring, and simplify access to applicable regulatory requirements.

LEI coverage and conditions - Section A of the Directions, which comes into force with immediate effect, mandates LEI for all OTC transactions undertaken by entities (other than individuals) in RBI-regulated markets for Government securities, money market instruments, foreign exchange instruments and derivatives. For non-derivative foreign exchange transactions, LEI is required only where the transaction value is at least USD 1 million (or equivalent). Market participants must obtain LEIs from Local Operating Units recognised by RBI and ensure that their LEI remains current; entities without a valid LEI are not permitted to transact in these markets.

UTI framework and scope - Section B, effective from January 1, 2027, prescribes a uniform UTI regime for all OTC derivative transactions entered into under RBI's governing directions on foreign exchange derivatives, rupee interest rate derivatives, forward contracts in Government securities and credit derivatives, among others. UTIs must be generated in line with CPMI–IOSCO's technical guidance, using a maximum 52-character identifier comprising the LEI of the generating entity and a unique transaction code, and must remain the single reference for the derivative contract over its lifecycle.

Generation waterfall and consolidation of instructions - The Directions set out a waterfall to determine the UTI-generating entity (prioritising the central counterparty, electronic trading platform, clearing member or a mutually agreed party, with the Clearing Corporation of India Ltd. – Trade Repository stepping in where necessary, including in cross-border scenarios). An Annex lists legacy circulars on LEI and UTI that are now superseded, bringing RBI's earlier scattered instructions into a single Master Direction and aligning Indian practice more closely with global data reporting standards.

11. The Financial Intelligence Unit-India (FIU-India) updated the Anti-Money Laundering (AML) & Counter-Financing of Terrorism (CFT) guidelines for Reporting Entities providing services related to Virtual Digital Assets (VDAs)

FIU-India on January 8, 2026 released updated AML & CFT Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets. These guidelines, issued by the FIU-IND, consolidate and streamline AML, CFT, and Counter Proliferation Financing **(CPF)** requirements for Virtual Digital Asset Service Providers **(VDASPs)**. They incorporate prior circulars, such as the 2025 VDA SP registration framework and Principal Officer guidance, into a unified document to enhance operational compliance under the Prevention of Money Laundering Act **(PMLA)**.

Key aspects cover mandatory FIU-IND registration via FINGate, robust Customer Due Diligence **(CDD)**, transaction monitoring, Suspicious Transaction Reporting **(STR)**, record-keeping, and the Travel Rule for VDA transfers. This update aligns VDASPs with standards applied to banks and financial institutions, emphasizing practical KYC implementation and risk-based oversight.

INFORMATION TECHNOLOGY & DATA PROTECTION

12. Ministry of Electronics and Information Technology (MeitY) introduces amendments to the IT Rules, 2021

The Ministry of Electronics and Information Technology (MeitY) has proposed amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) on April 21, 2026. These build on the Amendment Rules notified on 10 February 2026 (effective from February 20, 2026), which introduced the first set of rules specifically governing AI-generated

content including requirements for labelling, traceability and expedited takedown of unlawful synthetic media. MeitY has since issued two further draft amendments dated March 30, 2026 and April 21, 2026, which are open for public consultation until May 7, 2026.

Context - February 2026 Amendment Rules

In February 2026, MeitY notified the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which amended the IT Rules, 2021 to create a regulatory framework for "synthetically generated information" (**SGI**), a term that covers deepfakes and other AI-generated media. Key features of the amendment includes -

- Introduction of the concept of SGI, covering audio, visual or audio-visual AI-generated or algorithmically altered content that looks realistic or is indistinguishable from real persons or events, with exceptions carved out for good-faith editing, accessibility tools, research and educational use, etc. Text-only AI outputs are not treated as SGI (though they remain subject to the general unlawful content framework).
- Due-diligence requirements for online platforms and apps (intermediaries) that enable users to create, host or share SGI. These include displaying a clear and prominent label on synthetic content, embedding permanent metadata or a unique technical identifier to trace the content back to where it was created/modified, and an obligation not to remove or tamper with those labels or identifiers.
- Heightened obligations for large social media platforms (called "Significant Social Media Intermediaries" or SSMIs that are platforms with over 50 lakh registered users in India), such as requiring users to declare whether their content is AI-generated, deploying reasonable and appropriate technical measures (including automated tools) to verify those declarations, and ensuring swift takedown of unlawful synthetic content (timelines provided are 2-3 hours for specified cases).

The March and April 2026 draft amendments should be read as *further refinements* and additions to this existing framework.

Key proposals in the March 30, 2026 draft amendments

The March 30, 2026 draft amendments primarily clarify and expand the due-diligence duties of online platforms under the IT Rules, 2021. In particular:

Retention of records - Rules 3(1)(g) and 3(1)(h) - The draft clarifies that the requirement to retain information related to content that has been removed or taken down, along with associated records, for a minimum of 180 days, is a floor -- not a ceiling. Platforms must continue to comply with any longer or stricter retention periods required under sector-specific laws (for example, in telecom or financial services), and the IT Rules do not override those obligations.

- **Compliance with MeitY guidance (Part II) -** A new Rule 3(4) expressly requires platforms to comply with written clarifications, advisories, orders, directions, standard operating procedures (SOPs), codes of practice and guidelines issued by MeitY for implementing their obligations under the IT Rules. These instruments must state their legal basis, scope and applicability, and must be consistent with the IT Act and IT Rules. Importantly, compliance with such MeitY guidance will be treated as part of the

intermediary's "due diligence" under Section 79 of the IT Act. —This means that ignoring MeitY guidance could jeopardise a platform's legal protection (safe harbour) from liability for user-generated content.

- **News and current affairs content (Part III) -** The rules are refined to clarify that the Digital Media Ethics Code (the framework governing online news and current affairs) applies not only where a registered "publisher" posts content, but also where ordinary users post news or current affairs content on a platform. In other words, platforms hosting user-generated news content - not just professional news outlets - now fall more squarely within the digital media oversight framework.
- **Inter-Departmental Committee (IDC) - Rules 14(2) and 14(5) -** The IDC under the IT Rules, 2021 is an appellate body that reviews complaints about online content and is empowered to direct content removal. Its powers are being broadened so that, in addition to acting on user complaints, it can take cognisance on matters directly referred to it by MeitY - effectively allowing the government to proactively escalate content-related issues without waiting for a user to first file a complaint.

Additional proposal dated April 21, 2026 – Rule 3(3)(a)(ii)

The consolidated draft circulated on April 21, 2026 introduces an additional requirement relating to on-screen labelling of AI-generated content, by inserting a new sub-clause under Rule 3(3)(a) of the IT Rules, 2021.

Rule 3(3)(a)(ii) – Continuous on-screen label for synthetic content

The existing requirement that synthetic or manipulated audio-visual content (including AI-generated or deepfake material) be "clearly and prominently" labelled is being strengthened.

The new rule clarifies that the label must remain continuously and clearly visible on-screen throughout the entire duration of the content -- it is not sufficient to show the label only at the start, at the end, or in a description box below the video.

This change tightens what platforms need to do in practice: they must ensure a persistent, always-visible on-screen label indicating that content is synthetic or AI-generated - not just a one-time disclosure. This aligns with global best practices on transparency and traceability for deepfake content and builds on the labelling and metadata requirements introduced in February 2026.

Practical implications for intermediaries -

From a practical standpoint, platforms and intermediaries should consider the following:

- **Data retention and logs -** Platforms should review, and where necessary update, their policies for retaining records of content that has been removed or disabled. The clarified minimum is 180 days, but platforms must also check whether their specific sector (e.g., banking, telecom) requires longer retention periods under other laws.
- **Digital media oversight for news and current affairs -** Platforms that host news or current affairs content including posts by ordinary users who are not registered news publishers, should assess whether they fall within the Digital Media Ethics Code framework under Part III of the IT Rules, and prepare for greater scrutiny from the IDC, which can now act on Ministry-referred matters proactively.

- **AI-generated content labelling and user experience** - To comply with both the February 2026 requirements (prominent labelling and embedded metadata) and the April 2026 proposal (continuous on-screen display), platforms will likely need to update their user interfaces, content upload processes, media processing systems and moderation tools. Specifically, this includes:
    - designing and implementing persistent visual labels that remain on-screen for the full duration of any synthetic or manipulated video or image content;
    - aligning audio-based disclosures and embedded metadata or provenance identifiers with the requirements of the IT Rules, 2026; and
    - ensuring that users cannot strip, hide or modify labels or provenance identifiers once content has been generated or uploaded to the platform.

13. MeitY outlines Legal Safeguards to prevent potential harms from AI and related technologies

MeitY, on March 11, 2026, outlined a comprehensive framework of legal safeguards to prevent harms arising from AI and related technologies, with a particular focus on protecting children. India's AI strategy, rooted in the government's vision of democratising technology, is complemented by robust regulatory mechanisms.

Key safeguards include

IT Act, 2000 - Requires intermediaries to prevent hosting of harmful content involving children and mandates removal within 3 hours of government or court notification (2 hours for non-consensual sexual/intimate content).

India AI Governance Guidelines - Promote human-centric and responsible AI development, recognising children as a vulnerable group. Recommend risk assessment frameworks and monitoring of AI-related harms.

CERT-In & ISEA Programme - CERT-In regularly disseminates online safety awareness. Information Security Education and Awareness Programme (ISEA) has conducted 4,309 workshops covering 9.63 lakh participants, including 1,186 workshops specifically for school children covering 3.38 lakh students. Around 15 crore beneficiaries covered through indirect mode.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011("SPDI Rules") and Digital Personal Data Protection (DPDP) Act, 2023- The SPDI Rules require organisations to collect personal data only for stated purposes, obtain consent before sharing, and publish privacy policies. Sensitive personal data must not be published or disclosed by third parties. The DPDP Act which is set to supersede the SPDI Rules, provides an omnibus data protection framework including detailed consent and notice requirements, security standards, data principal rights, grievance redressal and dispute resolution mechanisms. Specifically , fiduciaries need to collect verifiable parental consent before processing children's data, which will include data collected via AI-powered toys and platforms. The DPDP Act further prohibits tracking, behavioural monitoring, and targeted advertising directed at children.

Toy Safety & Harmful Content Regulation - Toys must comply with the Toy Quality Control Order and BIS standards. Harmful or explicit content involving children is regulated under the IT Act, IT Rules, and POCSO Act.

NCPCR Studies & Cyber Safety Guidelines - (National Commission for Protection of Child Rights) NCPCR has published studies on effects of mobile phone usage by children and released guidelines on cyber safety, online safety awareness, and prevention of bullying and cyberbullying in schools. For details, refer to links attached.

National Cyber Crime Reporting & Indian Cyber Crime Coordination Centre (I4C) - Ministry of Home Affairs (MHA) operates the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) with special focus on crimes against children. The I4C ensures coordinated action against cybercrime including child sexual exploitation.

CSAM Blocking & International Cooperation - ISPs directed to dynamically block Child Sexual Abuse Material (**CSAM**) websites using global databases (Internet Watch Foundation, UK & Project Arachnid, Canada). An MoU between NCRB and National Center for Missing and Exploited Children (NCMEC) (USA) enables sharing of tipline reports on online child sexual exploitation for prompt action by States/UTs.

14. MeitY Issues Advisories to Intermediaries on Content Due Diligence Obligations

MeitY on February 9, 2026 issued an advisory (No. 2(6)/2024-CL&DG-Part(1)) reminding all intermediaries, including AI platforms, AI tool providers, and social media intermediaries, of their due diligence obligations under the IT Act, 2000 and IT Rules, 2021 in relation to the generation, hosting, and dissemination of information concerning religious matters or otherwise unlawful information. MeitY observed that certain AI-based platforms were generating and disseminating content relating to religious scriptures, beliefs, practices, and institutions in a distorted, misleading, or inaccurate manner, including algorithmic alteration of sacred texts, with potential to hurt religious sentiments, create communal disharmony, and disturb public order. Intermediaries were advised to deploy technology-based measures including algorithmic safeguards, content moderation mechanisms, and culturally informed content review processes, undertake an immediate review of their training datasets, model outputs, and grievance redressal mechanisms, and ensure expeditious removal of unlawful content within prescribed timelines, failing which safe harbour protection under Section 79 of the IT Act would not be available.

Subsequently, MeitY on issued a second advisory March16, 2026 (F. No. 2(6)/2026-CyberLaws) addressed to all intermediaries, intimating that their computer resources were being used for generation, hosting, publication, transmission, sharing, and uploading of abusive, defamatory, objectionable, derogatory, and misleading synthetically generated information (SGI), in violation of the IT Act, 2000 read with IT Rules, 2021 as amended on 10 February 2026. The advisory invoked Rules 3(1)(c), 3(1)(ca), 3(1)(cb), 3(1)(d), 3(3), and 4(1A), and directed intermediaries to immediately desist from hosting such content, forthwith enforce user terms of service including suspension and termination of violating accounts, and remove or disable access to all violative content without vitiating evidence. Non-compliance was cautioned to result in loss of safe harbour under Section 79(1) of the IT Act and liability under the IT Act and the Bharatiya Nyaya Sanhita, 2023.

EMERGING TECHNOLOGIES

15. Indian Computer Emergency Response Team (CERT-In), in collaboration with SIA-India, releases Cyber Security Framework and Guidelines for Space Sector including Satellite Communication

CERT-In under MeitY, in February 2026 has issued a comprehensive cybersecurity framework for India's space including satellite communication (**SatCom**) ecosystem. The framework addresses the growing cyber risks arising from the expanding commercial satellite sector, integration of SatCom with terrestrial networks, and software-defined payloads.

The framework covers all three segments - Space, Ground, and User, and mandates a **"security-by-design and defense-in-depth"** approach across the entire SatCom lifecycle, from design and launch to decommissioning.

Regulatory and policy framework -

The Indian Space Policy 2023 (ISP 2023) and the subsequent Norms, Guidelines, and Procedures (NGP) by IN-SPACe provide a comprehensive regulatory framework for authorizing private sector (Non-Government Entity - NGE) space activities in India, detailing which activities need permission (like satellite operations, launches, ground systems), the criteria for approval, application processes, and conditions (like FDI limits, registration, incident reporting) to foster a robust, transparent, and responsible Indian space ecosystem. From a cyber security standpoint, space entities have the following regulatory obligations-

- **Incident Reporting and Response** - Compliance with CERT-In cybersecurity standards including reporting cybersecurity incidents to CERT-In **within 6 hours** of detection, log retention for a minimum rolling period of **180 days**, periodic audits, among other requirements as directed by CERT-In
- **Security Baseline -** Ensure compliance with catalogue of Indian Standards for Space Industry, Norms, Guidelines and Procedures (NGP) released by the Department of Space. Hardware, firmware, and cryptographic modules must be certified as per recognized standards (e.g., FIPS 140-3, Common Criteria, ISO/IEC 27001, ECSS-E-ST-80C). Further, detailed security standards have been provided for entities in the space sector under these Guidelines.
- **Data Protection** - Compliance with the **Digital Personal Data Protection Act, 2023** for user data handling
- **Supply Chain Assurance** - Procurement should only from trusted sources under India's **Trusted Telecom Directive and NSDTS.** Further, supply chain risk assessments and third-party audits shall be mandatory before integration or deployment.
- **Miscellaneous** - Entities need to appoint a **Chief Satellite Security Officer (CSSO/CISO)** for governance and compliance. Further, implementation of **post-quantum cryptographic algorithms** in a phased rollout. Space entities need to maintaining **Bill of Materials** (SBOM, QBOM, CBOM, AIBOM, HBOM) as per CERT-In technical guidelines.

The framework further mandates dedicated **Network Operations Centers (NOC)** and **Security Operations Centers (SOC)**, integration with CERT-In for anomaly alerts, Zero-Trust Architecture across

all network components, and periodic cyber resilience drills including tabletop exercises and red-team simulations.

Security testing is required across all mission phases from design validation and pre-launch penetration testing to in-orbit vulnerability scanning and end-of-life secure decommissioning. The document also provides a **Self-Assessment Maturity Checklist** for organizations to evaluate their security posture across Identify, Protect, Detect, Respond, and Recover functions.

16. DPIIT Revises Definition of "Deep Tech Startup" Under Fresh Startup Notification, 2026

Ministry of Commerce and Industry on February 4, 2026, notifies revised startup recognition norms, including a new framework for Deep Tech Startups

The Department for Promotion of Industry and Internal Trade (**DPIIT**) has issued a fresh notification superseding February 19, 2019 notification on startup recognition. It defines a Startup as an entity incorporated or registered in India as a private limited company, partnership firm, LLP, multi-state cooperative society, or state/UT cooperative society, provided it is within 10 years of incorporation/registration, has turnover not exceeding ₹200 crore in any financial year since incorporation/registration, and is working toward innovation, improvement of products/processes/services, or a scalable business model with high potential for employment generation or wealth creation. Entities formed by splitting up or reconstruction of an existing business are excluded.

Key Highlights:

- Deep Tech Startups are now separately recognised and have a dedicated application process.
- For such entities, the startup period extends up to 20 years from incorporation/registration.
- Their turnover limit is raised to ₹300 crore.
- A Deep Tech Startup must be working on solutions based on new scientific or engineering knowledge, have high R&D spend, own or develop significant novel IP, and face long development cycles, high capital needs and technical uncertainty.
- DPIIT will determine Deep Tech status based on a framework, parameters and documents submitted by the applicant.

Recognition and certification -

- Eligible entities must apply on the DPIIT portal.
- Applications must include the certificate of incorporation/registration and a write-up explaining innovation, scalability, or wealth/employment potential.
- Deep Tech applicants must submit additional documents proving the required attributes.
- DPIIT may recognise the entity or reject the application with reasons.
- Startups to have specific conditions and restrictions in their investments and use of funds.

CASE LAW & LITIGATION UPDATES

17. Hon'ble Supreme Court of India Rules that Telecom Spectrum, cannot be subjected to Insolvency Proceedings Under the Insolvency and Bankruptcy Code, 2016

The Hon'ble Supreme Court of India, in its landmark judgment in *State Bank of India v. Union of India and Others* (Civil Appeal Nos. 1810 of 2021), decided on February 13, 2026, held that spectrum allocated to telecom service providers cannot be treated as an "asset" of the corporate debtor under the Insolvency and Bankruptcy Code, 2016 **(IBC)** as spectrum is a finite natural resource held by the Union of India in public trust, governed exclusively by telecommunications laws which the IBC cannot override.

The court further noted that access to and use of such resource is regulated in a transparent, non-discriminatory manner, so that, it its utilized to the benefit of the nation, rather than being treated as objects of private ownership or unfettered commercial exploitation.

Telecom licensees hold only a limited, conditional, and revocable right to use spectrum and acquire no proprietary or ownership interest in spectrum therefore the same cannot be treated as an "asset" within the meaning of IBC.

License fees, spectrum usage charges, and AGR dues payable to the DoT are part of the contract do not qualify as "operational debt" under Section 5(21) of the IBC, as they arise from a sovereign grant of privilege and not from a commercial transaction.

The order clarifies the contractual relationship between the licensor and the licensee, and reaffirms that spectrum is a national resource allocated subject to overarching regulation grounded in constitutional law and must not treated solely as a piece of contractual conscope of rights vested with the licensee as part of the telecom license does not, does not affect a transfer of ownership or proprietary interest. Therefore, spectrum assigned to the licensee cannot be construed as an "asset" under the IBCstruct.

18. Hon'ble Supreme Court Holds Telecom Licensees Liable to Pay Spectrum Reserve Price from the Date of Licence Cancellation, Rejecting TDSAT's Diluted Interpretation

The Hon'ble Supreme Court of India, in its ruling in *Union of India v. Sistema Shyam Teleservices Limited* (Civil Appeal No. 12219 of 2018), decided on February 20, 2026, held that Sistema Shyam Teleservices Limited (SSTL) was liable to pay the reserve price fixed for the November 2012 spectrum auction from February 2, 2012 - the date its Unified Access Service licenses were quashed as per the Hon'ble Court's order in *Centre for Public Interest Litigation vs Union of India and others* (Writ Petition (Civil) Nos. 423 of 2010 and 10 of 2011), overruling the TDSAT's observation.

The order further clarifies that the interest on such reserve price shall also be only payable from the date the said charges became recoverable, i.e., 21 days from the date when the show-cause notice was raised by the DoT and not from the date of the order quashing the licenses.

In light of the above, the DoT was directed to issue a revised demand to be paid by SSTL within three months from the same being raised.

Luthra and Luthra
LAW OFFICES INDIA

This newsletter is only for general informational purposes, and nothing in this edition of the newsletter could possibly constitute legal advice (which can only be given after being formally engaged and familiarizing ourselves with all the relevant facts). However, should you have any queries, require any assistance, or clarifications with regard to anything contained in this newsletter, please feel free to contact Vikash Kukreti, at the below mentioned coordinates.

KEY CONTACTS

VIKASH KUKRETI
Partner
Email - vkukreti@luthra.com

GAURAV TIWARI
Senior Associate
Email - gtiwari@luthra.com

AKASH TAHENGURIA
Associate
Email - atahenguria@luthra.com

OFFICES

NEW DELHI
1st and 9th Floors, Ashoka Estate,
24 Barakhamba Road, New Delhi - 110 001
T: +91 11 4121 5100
F: +91 11 2372 3909
E: delhi@luthra.com

MUMBAI
20th Floor, Indiabulls Finance Center,
Tower 2 Unit A2, Elphinstone Road,
Senapati Bapat Marg, Mumbai - 400 013
T: +91 22 4354 7000
F: +91 22 6630 3700
E: mumbai@luthra.com

BENGALURU
3rd Floor, Onyx Centre, No. 5, Museum Road,
Bengaluru - 560 001
T: +91 80 4112 2800 / +91 80 4165 9245
F: +91 80 4112 2332
E: bengaluru@luthra.com

HYDERABAD
Serene Towers,
House No. 8-2-623/A,
Road No. 10, Banjara Hills,
Hyderabad, Telangana - 500034
T: +91 40 7969 6162
E: hyderabad@luthra.com

CHENNAI
Prestige Palladium Bayan,
8th Floor, Greams Road, Nungambakkam Division,
Egmore, Chennai - 600 006,
Tamil Nadu
T: +91 95604 88155
E: chennai@luthra.com