The Dialogue®
INFORM ENGAGE IDEATE

WRITTEN COMMENTS

Draft Telecom Cybersecurity Amendment Rules

JULY, 2025

WRITTEN COMMENTS

DRAFT TELECOM CYBERSECURITY AMENDMENT RULES

Author - *Pranav Bhaskar Tiwari*

The Dialogue® is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue® has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information
www.thedialogue.co

Suggested Citation
Tiwari, P.B. (July 2025). Written Comments: Draft Telecom Cybersecurity Amendment Rules The Dialogue®

Catalogue No
TD/PR/WC/0725/03

Publication Date
July 31, 2025

Contents

List of Abbreviations

Abbreviation	Full Form
TIUE	Telecommunication Identifier User Entity
TSP	Telecoms Service Provider
OTT	Over-the-Top (communication or content platforms)
MNV	Mobile Number Validation
KYC	Know Your Customer
DoT	Department of Telecommunications
MeitY	Ministry of Electronics and Information Technology
MIB	Ministry of Information and Broadcasting
RBI	Reserve Bank of India
DPDP Act	Digital Personal Data Protection Act
IT Act	Information Technology Act, 2000
CERT-In	Indian Computer Emergency Response Team
SEBI	Securities and Exchange Board of India
TRAI	Telecom Regulatory Authority of India
IMEI	International Mobile Equipment Identity
CEIR	Central Equipment Identity Register
MSME	Micro, Small and Medium Enterprises
FAQ	Frequently Asked Questions
API	Application Programming Interface
OTP	One-Time Password
ISO	International Organisation for Standardisation

Executive Summary

A. Context and Key Concern

The Draft Telecommunication Cybersecurity (Amendment) Rules, 2025 (Draft Amendment Rules) mark a significant shift in India's regulatory landscape by expanding the scope of telecom cybersecurity obligations beyond licensed telecom service providers (TSPs) to include Telecommunication Identifier User Entities (TIUEs). TIUEs may include any digital platform that uses mobile numbers for customer identification or service delivery. While the intent to curb fraud and strengthen security is laudable, the draft raises legal, operational, and constitutional concerns that merit recalibration.

B. Key Challenges

1. Overbroad Scope and Legislative Overreach: The inclusion of TIUEs, such as OTT communication platforms, fintech apps, and e-commerce players, extends the Rules well beyond the Telecommunications Act's intended domain, creating concerns over legal validity and sectoral jurisdiction.

2. Privacy and Fundamental Rights Implications: Mandating identity validation for all users across digital platforms through a centralised Mobile Number Validation (MNV) platform poses risks to user privacy, undermines anonymity, and potentially infringes on freedom of expression.

3. Unrestricted Government Powers: The Rules allow the government to direct disconnection, data sharing, or identifier suspension without adequate procedural safeguards, raising concerns of unchecked executive authority and absence of due process.

4. Regulatory Convergence Without Coordination: The Draft Amendment Rules duplicate existing obligations under the Information Technology Act (IT Act), Indian Computer Emergency Response Team (CERT-In directions), Reserve Bank of India (RBI) KYC norms, and the Digital Personal Data Protection Act (DPDP Act), creating fragmented oversight, conflicting mandates, and increased compliance costs.

5. Ambiguity on Cost and Infrastructure Responsibility: The financial and technical burden of building, maintaining, and utilising the MNV system and associated integrations is unclear, risking unsustainable cost imposition on telecom operators and TIUEs.

6. Risks to Device Resale Ecosystem: IMEI-based checks on used devices, while aimed at curbing theft and tampering, may hinder informal markets if not implemented in a low-cost, accessible manner, especially for small resellers.

7. Lack of Operational Clarity: Several critical terms and processes remain undefined, including the definitions of 'validation' and 'KYC', the flow of consent, responsibility for due diligence, and the nature of government-TIUE contracts, which leads to uncertainty and scope for misapplication.

C. Key Recommendations

i. **Reconsider current approach:**

- **Withdraw the Draft Amendment Rules in their current form**
  - The provisions introducing TIUEs and mandating the MNV framework represent a significant regulatory expansion beyond the mandate of the Telecommunication Act, 2023. Given concerns around legislative competence, operational feasibility, and rights implications, we recommend withdrawing these provisions in their current form.
- **Phased, Voluntary Rollout via Sandbox**
  - Launch a voluntary regulatory sandbox inviting partners from high-risk sectors to test MNV integration, assess operational

- feasibility, and generate feedback to refine the framework.
- Maintain voluntary adoption of the MNV platform to avoid unintended disruptions, especially for smaller or low-risk entities.

ii. If retained, address the following key areas:

- **Strengthen Public Consultation Framework**
  - Enhance the stakeholder consultation timeline by at least 60 days to allow meaningful review and feedback, especially from small businesses, civil society, and sectoral experts.
  - Before finalising the rules, proactively consult diverse stakeholder groups as well as relevant sectoral regulators such as MeitY, MIB, and RBI, to ensure harmonisation and avoid regulatory overlaps.

- **Phased, Voluntary Rollout via Sandbox**
  - Launch a regulatory sandbox inviting partners from high-risk sectors to test MNV integration, assess operational feasibility, and generate feedback to refine the framework.
  - Maintain voluntary adoption of the MNV platform to avoid unintended disruptions, especially for smaller or low-risk entities.

- **Proportional Use of MNV:**
  - Restrict mandatory MNV only to transactions or platforms where fraud risk is demonstrably high.
  - Monitor and limit voluntary use of the MNV Platform, as its utilisation by malicious TIUEs could lead to exposure of personally identifiable information at scale.

- **Privacy and Rights Protection:**
  - Incorporate privacy safeguards, including data minimisation, lawful purpose, storage limitation, and third-party oversight, in line with the DPDP Act.
  - Ensure due process in all user-affected decisions, such as identifier disconnection with mechanisms for notice, appeal, and review.

- **Tiered Compliance Approach:**
  - Calibrate obligations based on risk and entity size, e.g., phased implementation, exemption thresholds, or lighter compliance tracks for MSMEs.
  - Offer technical templates and capacity-building support to TIUEs new to telecom-grade cybersecurity.

- **Regulatory Harmonisation:**
  - Align the Rules with parallel frameworks under MeitY, CERT-In, RBI, and the DPDP Act to prevent duplicative or contradictory requirements.

- **Cost and Infrastructure Funding:**
  - Finance development and use of the MNV platform using the Digital Bharat Nidhi or similar funds.
  - Clarify commercial flows, who contacts whom and who pays whom, to ensure predictability and sustainability for TSPs and TIUEs alike.

- **Clarity on IMEI Compliance:**
  - Provide clear definitions and timelines for manufacturer and reseller obligations.
  - Develop low-cost, public IMEI lookup tools to facilitate compliance by small second-hand phone sellers.
  - Ensure the IMEI database returns only a binary “safe to sell” flag to protect user privacy.

- **Stakeholder Consultation:**
  - Before finalising, publish FAQs or detailed guidance to explain ambiguous terms and implementation pathways.
  - Engage with industry bodies, civil society, legal experts, and TSPs to co-develop proportionate and operationally feasible rules.

- **Impact Review Clause:**
  - Mandate a one-year competition impact assessment, with a commitment to course-correct if adverse effects on startups or market entry are observed.
  - Review after one year of implementation to assess the impact of the Rules on marginalised communities and adopt corrective measures where necessary.

1 Background

The Draft Amendment Rules[1] released in June 2025, propose significant changes to the Telecom Cyber Security Rules, 2024,[2] which were notified under the Telecommunication Act, 2023[3], in November last year. The Draft Amendment Rules signal a fundamental shift from a telecom-centric approach to a broader cybersecurity regime encompassing digital platforms and telecom-connected devices.

The amendments are purportedly driven by a rising incidence of telecom-enabled cyber fraud in India, including SIM swapping, fake OTPs, and stolen devices. The government seeks to strengthen telecom security by requiring consistent standards across all entities using telecom identifiers. Key systemic interventions include a centralised MNV platform and a national IMEI tracking system to improve identity verification and deter misuse.

The draft introduces new definitions that expand regulatory reach:

- **TIUEs:** Any non-licensee entity that uses telecom identifiers (like mobile numbers) for user verification or service delivery e.g., OTT apps, e-commerce platforms, or fintech services.[4]
- **MNV Platform:** A government-backed mechanism enabling verification of mobile number ownership by matching user data against telecom operator KYC records.

This expanded scope brings numerous digital platforms under the telecom regulatory umbrella, redefining traditional boundaries between telecom regulation and digital services governance.

Our aim is to support the Department of Telecommunications in shaping a robust, balanced, and legally sound cybersecurity framework, one that enhances security while safeguarding innovation, proportionality, and fundamental rights in the digital ecosystem.

[1] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules,* 2025.
[2] Ministry of Communications, *Telecommunications (Telecom Cyber Security) Rules,* 2024.
[3] The Telecommunications Act, No. 44 of 2023.
[4] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 2(1)(i).

2 Overarching Recommendations

2.1 Overreach Beyond the Telecom Act Mandate

The Draft Amendment Rules stray beyond the legal and constitutional mandate of the Telecommunication Act, 2023. Designed to govern licensed telecom networks and services, the Act does not extend its reach to digital platforms like e-commerce, fintech, or social media platforms. However, the Draft Amendment Rules seek to regulate all entities using mobile numbers for customer identification and service delivery by designating them as TIUEs, despite such platforms operating entirely outside the licensed telecom domain.

This expansion raises serious legal concerns. Section 22 of the Act empowers the government to make rules for telecom cyber security, clearly intended to secure telecom infrastructure from cyber threats.[5] Requiring digital platforms to validate user numbers against telecom KYC databases is not a telecom security function, but a broader digital identity measure. Such regulatory overreach risks being declared ultra vires, as it imposes obligations on entities not contemplated by the Parent Act.

Creating new regulated categories like TIUEs through subordinate legislation, without clear legislative backing, undermines the doctrine of separation of powers.[6] It also opens the door to jurisdictional conflict with existing digital laws such as the IT Act, 2000, which already governs platform accountability and identity verification.[7] The Draft Amendment Rules, if legislated without revision, would invite legal challenge and weaken policy coherence across ministries.

Recommendations:

- **Reconsider the Current Approach:** The provisions introducing TIUEs and mandating the use of the MNV platform may benefit from being withdrawn in their present form and revisited through broader inter-ministerial consultation.
- **Ensure Statutory Alignment:** Future iterations should be anchored within the express scope of the Telecommunications Act, focusing rule-making powers strictly on licensed telecom networks and their cybersecurity.
- **Clarify the Nexus to Telecom Security:** Any new obligations should be clearly and narrowly defined to align with the objective of protecting telecom infrastructure, thereby avoiding potential jurisdictional conflicts with other legal regimes.

2.2 Regulatory Convergence

The Draft Amendment Rules introduce TIUEs (e.g., social media, fintech, e-commerce platforms) into a telecom cybersecurity framework, creating a de facto convergence between telecom and digital regulation. However, this convergence lacks coordination with existing legal regimes, notably the IT Act[8] and CERT-In Directions[9]. The result is duplicative compliance, regulatory confusion, and potential jurisdictional overreach.

[5] The Telecommunications Act, No. 44 of 2023, § 22.
[6] Naresh Chandra Agrawal v. ICAI, 2024 SCC OnLine SC 114.
[7] The Information Technology Act, No. 21 of 2000.
[8] Id.
[9] Indian Computer Emergency Response Team (CERT-In), Direction No. 20(3)/2022, § 70(b) IT Act, 2000.

Compliance overlaps would arise in data protection, KYC norms, and security audit, particularly where sectoral regulators like RBI[10], SEBI[11], or MeitY[12] already provide tailored obligations.

In 2022, the then Minister of Communications clarified that OTT services fall outside the scope of the Telecommunications Act, 2022, as they are governed by the IT Act 2000. This position is further reinforced by the conscious omission of OTT platforms from the Telecommunications Bill, 2022, reflecting clear legislative intent.

Recommendations:

- **Ensure Inter-Regulatory Coordination:** Collaborate with MeitY, CERT-In, TRAI, RBI, and others to harmonise incident reporting, audit timelines, and standards. Avoid siloed obligations.
- **Define Telecom-Facing Scope:** Clearly limit DoT's jurisdiction to misuse of telecom identifiers (e.g., spoofing, SIM-based fraud). Broader digital platform operations should remain under MeitY's purview.
- **Introduce Mutual Recognition Clauses:** Where TIUEs comply with equivalent sectoral norms (e.g., RBI KYC or ISO standards), allow deemed compliance under Telecom Rules to prevent duplication.

2.3 Balancing Security with Innovation and Competition

While the Draft Amendment Rules seek to bolster security, they may inadvertently stifle innovation and harm competition, especially for startups and SMEs. MNV integration and verification impose non-trivial financial and technical burdens, creating entry barriers that may disproportionately affect smaller players.

For instance, ₹3 per verification may seem nominal, but at scale, it's significant. For instance, it's ₹30 lakh for just 10 lakh verifications. Startups might avoid phone verification altogether and use more risky verification mechanisms like email or exit segments requiring it.

Moreover, if telecom operators handling MNV queries gain access to usage metadata, they could exploit this for anti-competitive purposes, a risk currently unaddressed.

Recommendations:

- **Utilise the Digital Bharat Nidhi:** The Government should finance validation costs via the Digital Bharat Nidhi instead of shifting the burden on TIUEs, who are anyway complying with sectoral guidelines.
- **Innovation Sandbox:** Launch a sandbox phase for voluntary implementation, testing usability, cost, and accuracy before mandating adoption.
- **Competition and Data Safeguards:** Prohibit TSPs or government agencies from using MNV data for analytics or business purposes. Mandate query anonymisation, audits, and strict penalties for misuse.
- **Impact Review Clause:** Mandate a one-year competition impact assessment, with a commitment to course-correct if adverse effects on startups or market entry are observed.
- **Graduated Compliance:** Introduce thresholds based on revenue or user base to ease compliance for smaller TIUEs.

2.4 Disenfranchisement and Access Barriers

India's digital growth has been remarkable, but a significant share of users still access the internet through shared devices or SIM cards. This is especially true for women and low-income individuals, many of whom use phones and SIM cards registered in the names of male family members or share devices within households. The Draft Amendment Rules, however, appear to assume a one-to-one relationship between a user, device, and telecom identifier. This assumption does not reflect ground realities.

[10] Reserve Bank of India, Master Directions on Fraud Risk Management in Regulated Entities (15 July 2024); see also, Reserve Bank of India, Circular No. RBI/2024-25/105: Prevention of Financial Frauds Perpetrated Using Voice Calls and SMS – Regulatory Prescriptions and Institutional Safeguards (17 January 2025).
[11] Securities and Exchange Board of India (SEBI), Circular No. SEBI/HO/MIRSD/MIRSD-PoD-1/P/CIR/2024/96: Measures to instil confidence in securities market – Brokers' institutional mechanism for prevention and detection of fraud or market abuse (4 July 2024).
[12] The Information Technology Act, No. 21 of 2000.

If different TIUEs initiate verification requests for separate individuals using the same number or device, the system may either reject the validation or flag it as suspicious. This creates a risk of legitimate users being denied access, particularly affecting women and vulnerable populations who already face barriers to digital inclusion. The Draft Amendment Rules, in their current form, risk excluding such users from essential digital services and entrenching structural inequalities.

Recommendations:

- **Inclusive Design Principles:** The Draft Amendment Rules should incorporate clear provisions that account for multiple users linked to a single SIM or device, especially in shared-access contexts.
- **Guidance for TIUEs:** TIUEs must be issued guidance on managing validation in such cases to prevent wrongful denial of service.
- **Gender-Sensitive Frameworks:** The government should consult with gender rights organisations and civil society groups to incorporate gender-sensitive approaches to identity verification.
- **Impact Assessment:** Introduce a mandatory review after one year of implementation to assess the impact of the Draft Amendment Rules on marginalised communities and adopt corrective measures where necessary.
- **Awareness and Outreach:** Launch public information campaigns to build awareness around the Draft Amendment Rules and their implications for shared users, ensuring that digitally marginalised groups are not left behind.

3 Rule-by-Rule Recommendations

3.1 Definition of TIUE: Rule 2(1)(i)

The Draft introduces the category of TIUE to include any non-telecom organisation using mobile numbers (telecom identifiers) to identify customers or deliver services.[13] This casts a wide net from communication apps and e-commerce platforms to small websites and offline businesses using phone numbers for customer engagement or delivery tracking. TIUEs are treated as a new compliance category, distinct from licensed telecom operators.

Key Concerns

- **Overbreadth and Ambiguity:** The broad language risks sweeping in thousands of entities, many without clarity on their inclusion. Even ancillary uses of mobile numbers like delivery updates could trigger TIUE obligations, causing confusion and possible selective enforcement.
- **Regulatory Overlap:** Many affected services are already regulated under MeitY, MIB, RBI, SEBI, or other regulators. Bringing them under Draft Amendment Rules risks duplication, inconsistent standards, and compliance fatigue.
- **Compliance Capacity:** Startups and small entities may lack awareness or resources for telecom-grade compliance, unlike large telcos. Sudden inclusion could lead to inadvertent violations.
- **Jurisdictional Uncertainty:** TIUEs include global platforms. Without a local presence, enforcement is difficult, creating uneven burdens on domestic entities.
- **Innovation Deterrent:** The regulatory cost of using mobile identifiers may lead some services to abandon phone-based authentication and rely on email, potentially weakening security practices.
- **Legal Validity:** TIUE is not defined in the Parent Act. Imposing duties on them via delegated legislation risks a challenge for being ultra vires.

Recommendations:

- **Clarify Scope:** Restrict the definition to entities where mobile numbers are central to service delivery or identity management, not incidental.
- **Exempt Low-Risk Use:** Exclude cases where mobile numbers are used purely for outbound communication.
- **Phased Voluntary Implementation:** Introduce voluntary obligations gradually and develop guidance documents. Partner with industry bodies for outreach and support.
- **Enable Voluntary Registration:** Create a lightweight TIUE registry for awareness and engagement.

3.2 Mobile Number Validation Platform: Rule 2(1)(cb)

The Draft Amendment Rules introduce an MNV platform to be operated by the government or an authorised agency.[14] Telecom operators and TIUEs would use it to confirm whether a mobile number matches subscriber records. Through secure APIs, TIUEs submit requests; the platform routes them to the relevant TSP, which responds with a validation result. Government agencies may also access the system for identity validation. The service is priced at ₹3 per request (or ₹1.5 if government-directed).[15]

[13] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 2(1)(i).
[14] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 2(1)(cb).
[15] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 7A(2).

Key Concerns

- **Privacy Risks:** While designed for fraud prevention, the MNV system involves sensitive identity verification. It could enable metadata trails linking phone numbers to online services, posing privacy concerns. Retention policies, user awareness, and transparency remain unclear. DPDP Act principles of necessity and proportionality must be respected.[16]
- **Reliability and User Impact:** False positives/negatives may arise due to data mismatches (e.g., spelling variations). This can block legitimate users or let impersonators slip through. The risk of onboarding friction, like delays, rejections, or demand for additional KYC, may degrade user experience.
- **Cost and Burden on TIUEs:** Beyond the ₹3 fee, integration and operational costs may be significant, especially for startups and other platforms with high volumes of traffic. Without phased implementation or exemptions, compliance could be onerous.
- **Scope and Ambiguity:** The draft lacks clarity on the precise scope of validation against the telecom database. It is unclear whether the response from the MNV platform will be a simple binary of 'yes' or 'no', or whether it will extend beyond static KYC to include dynamic KYC markers such as location data or SIM/device swapping, which are typically available with TSPs and can be used for fraud detection. The format in which a request will be submitted and the nature of the response are also not specified.
- **Government Access and Oversight:** While public interest use is legitimate, open-ended access by agencies risks overreach. Guardrails are needed to prevent misuse.

Recommendations:

- **Define Key Terms and Processes:** Update the Draft Amendment Rules with the definition of 'Validation' to define its precise scope. Also, define the process for Validation along with the format for making requests and receiving responses from the MNV platform. It's equally important to define the nature of KYC data points that will be validated. Is it just name(s) associated with a phone number or does it also include dynamic data points like location data.
- **Targeted Rollout:** Begin with high-importance sectors like public services before wider expansion by private entities.
- **Privacy Protections:** Ensure data minimisation, encryption, minimal logging, and strong oversight. Clarify that MNV responses reveal no personal data beyond match status.
- **Fallback Mechanisms:** Allow manual KYC or secondary verification when MNV fails.
- **Cost Review:** Reassess pricing after 12 months and consider caps or discounts for high-volume TIUEs.
- **Grace Period:** Offer a sandbox before full implementation for testing and integration.

3.3 Need for Guardrails on Data Demands and Identifier Suspension: Rule 7A(5) and Rule 5 (6)

The Draft Amendment Rules empower the Central Government to access telecom identifier-related data from TIUEs (such as phone numbers linked to user accounts), excluding content.[17] They also enable directions to suspend the use of specific identifiers for authentication or service delivery, which may result in users being unable to access digital platforms.[18] Further, telecom operators or TIUEs may be directed to suspend or deactivate identifiers without prior notice, if considered necessary in the public interest.[19] While these provisions are intended to strengthen measures against cyber fraud, they merit further deliberation to ensure safeguards on proportionality and due process[20].

[16] *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023),* Chapter II Obligations of Data Fiduciary.
[17] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 7A(5).
[18] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 5 (6)(b).
[19] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 5(6).
[20] Maneka Gandhi v. Union of India, AIR 1978 SC 597.

Key Concerns

- **Absence of Procedural Safeguards:** The Draft Amendment Rules do not specify who can issue such directions or under what process. Unlike Section 69A of the IT Act, there are no institutional checks or review mechanisms.
- **No Notice or Remedy:** Sudden disconnection of telecom services without user notification or recourse can cause severe disruption, especially where numbers are used for banking, emergency services, or identity verification.
- **Operational Burden on TIUEs:** Platforms must establish systems to respond to government directions swiftly, adding compliance costs and complexity.
- **Single Point of Failure:** Mandating identifier suspension across all TIUEs risks creating a single point of failure, where one erroneous flag can block user access to multiple digital services. Such suspension must be limited to high-risk cases, restricted to high-risk TIUEs, and subject to prior notice, an opportunity to be heard, and adherence to the principles of natural justice.

Recommendations:

- **Codify Procedure:** Establish who may issue directions, on what basis, and with oversight, mirroring protocols like Section 69A of the IT Act.
- **Proportional Suspension:** Differentiate between temporary emergency suspension and permanent disconnection; require post-facto review and appeal. Even emergency suspension must be limited to high-risk cases, wherein the user services of only high-risk TIUEs are suspended.
- **Ensure User Notification:** Notify users after action is taken and establish a clear redressal pathway.
- **Legal Consistency:** Ensure data requests align with lawful access norms and are authorised by a senior officer.
- **Minimise Data Requests:** Limit demands to essential metadata; prohibit mass or fishing expeditions.
- **Stakeholder Input:** In non-urgent cases, seek TIUEs' contextual input before ordering disconnection to avoid erroneous actions.

3.4 Obligations on Device Manufacturers Must Stay Focused and Proportionate: Rule 8 (4)

The Draft Amendment Rules empower the government to direct telecom equipment manufacturers and importers to ensure all devices sold in India have unique, valid IMEIs that are not already active on Indian networks.[21] It also allows the government to seek assistance from manufacturers in cases of IMEI tampering, such as providing production data, verifying original IMEI allocations, or helping investigate cloned or modified devices.[22] This aims to plug technical loopholes exploited in phone theft and fraud, and aligns with India's Central Equipment Identity Register (CEIR) framework.[23] However, certain aspects require greater deliberation and clarity to ensure regulatory clarity and seamless operationalisation.

Key Concerns

- **Ambiguity in Scope:** "Any support" is undefined, potentially allowing broad and intrusive demands beyond IMEI assistance.
- **Lack of Timelines and Safeguards:** No clarity on response deadlines or confidentiality of proprietary data shared.

Recommendations:

- **Limit Scope:** Define that manufacturer obligations are restricted to IMEI verification, production records, and anti-tampering support.
- **CEIR Integration:** Provide CEIR access or APIs to verify IMEIs pre-sale and prevent duplicate use.
- **Stakeholder Consultation:** Work with handset industry bodies and civil society to develop realistic implementation protocols.

[21] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 8 (4).
[22] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 8 (4)(a).
[23] Central Equipment Identity Register (CEIR), 2025. https://ceir.gov.in/Home/index.jsp.

3.5 IMEI Verification by Second-Hand Device Resellers Must Be Practical and Privacy-Preserving: Rule 8

The draft introduces a mandatory IMEI verification process for all entities involved in the resale of used mobile phones.[24] Before completing any transaction, resellers must check the device's IMEI against a government-provided database of tampered or blacklisted identifiers, likely integrated with the CEIR system. Each verification will cost ₹10 per IMEI.[25] If the device is flagged, the sale is to be halted, and further guidance may be prescribed.

Key Concerns

- **Informal Market Challenges:** Much of India's second-hand device ecosystem is unregistered or informal. Without targeted enforcement, only law-abiding resellers may comply, while black market sellers continue unchecked.
- **Usability and Access:** Smaller vendors without digital literacy or infrastructure may struggle unless the interface is mobile-friendly, multilingual, and quick.
- **Online Platforms:** Platforms like OLX or Cashify may also fall under "involved in sale/purchase", but their obligations are unspecified.
- **Data Privacy:** IMEI checks must not disclose personal or sensitive information; only a binary clean/blocked status should be shown.
- **Error Handling:** False positive listings can trap legitimate phones and users without a clear redressal mechanism.

Recommendations:

- **Simple, Mobile-First Interface:** Ensure the check system is accessible via apps, WhatsApp bots, and multilingual web portals with fast turnaround.
- **Public and Consumer Awareness:** Run campaigns encouraging buyers to demand verified devices, creating market-driven compliance.
- **Marketplace Compliance:** Mandate online resale platforms to integrate IMEI checks and block flagged devices automatically.
- **Privacy Protection:** Limit query results to IMEI status only, and no user identity or case specifics.
- **Balanced Enforcement:** Focus enforcement on large volume traders first, with warnings for early-stage non-compliance.

[24] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 8.
[25] Ministry of Communications, *Draft Telecommunication Cybersecurity (Amendment) Rules, 2025,* r 8 (7).

Author

Pranav Bhaskar Tiwari

Senior Programme Manager - Platform Regulation, Gender and Tech, The Dialogue | Secretariat, Alliance for Cyber Trust and Safety (ACTS)

Pranav Bhaskar Tiwari, a Gold Medallist from the Indian Society of International Law, leads The Dialogue's work on Platform Regulation and Gender and Technology. A lawyer with expertise in IP and Technology Law, he focuses on technology's impact on society. Certified as an Information Privacy Professional/Europe, Pranav engages with global tech policy leaders and has worked with institutions like the Centre for AI and Digital Policy. He previously advised the Internet Society on IP, cybersecurity, online safety, and data protection.

thedialogue.co

@_DialogueIndia

@TheDialogue_Official

@The-Dialogue-India

@TheDialogue