

Digital Firms Raise Alarm Over Mobile Number Validation Rules in India

August 2, 2025 • vajiramandravi.com



Digital Firms Latest News

- Digital firms have raised concerns over India's draft Telecom Cyber Security Rules, 2025, citing jurisdictional overreach and high compliance costs due to proposed mobile number validation requirements.

Introduction

- India's digital economy may soon face new compliance burdens due to a draft rule under the **Telecommunications (Telecom Cyber Security) Amendment Rules, 2025**.
- Proposed by the Department of Telecommunications (DoT), the new framework mandates **mobile number validation** to ensure subscribers are legitimate users.
- While intended to strengthen cyber security, the rule has sparked serious concerns among tech companies about its **legal scope, cost implications, and regulatory overreach**.

Scope of the Draft Telecom Cyber Security Rules, 2025

- The draft rule introduces the concept of a **Telecommunication Identifier User Entity (TIUE)**, defined broadly as any person or entity (excluding licensed telecom operators) that uses telecom identifiers like mobile numbers for delivering services or identifying users.
- This wide definition has triggered alarm among digital firms, as it could include virtually every online platform, from fintech and social media to e-commerce and ride-hailing services.
- The proposed framework enables telecom operators to **charge up to Rs 3 per validation request**, providing confirmation of the subscriber's legal identity linked to a mobile number.

Industry Concerns on Jurisdiction and Regulatory Overreach

- The **Internet and Mobile Association of India (IAMAI)**, representing global players like Google, Apple, and Amazon, has called the move a case of **legislative overreach**.
- In its submission to the DoT, IMAI argued that the draft rules extend telecom-style regulation to entities that neither provide telecom services nor control telecom infrastructure.
- The association warned that this expansion of regulatory authority could have **widespread consequences for digital service providers**, especially in sectors such as:
 - Fintech and digital payments
 - Mobility and e-commerce platforms
 - OTT content providers and social media
 - Micro, Small and Medium Enterprises (MSMEs)
- IMAI emphasised that such rules were **not envisioned under the Telecommunications Act, 2023**, making their extension to unrelated sectors legally questionable.

Financial Burden and Operational Disruption

- Although Rs 3 per mobile verification may seem nominal, IMAI warned that it would add up quickly for platforms handling **millions of users**.
- For startups and MSMEs, these recurring costs could **reshape business models** or compel platforms to pass the burden onto consumers via price hikes or service restrictions.
- CUTS International, a policy think tank, echoed these concerns.
- It noted in its regulatory impact assessment that the **net benefit of the draft rules could be negative**, especially when alternative cybersecurity initiatives are already underway.
- CUTS advised the government to **focus on streamlining existing cyber safety frameworks** rather than introducing fragmented and potentially burdensome mechanisms.

Potential for Mandatory Enforcement in Specific Sectors

- While the DoT has hinted that the validation framework may **remain optional for private entities**, the **draft language leaves room for later mandatory adoption**.
- Experts pointed out that the vagueness around implementation adds to business uncertainty.

- Legal analysts questioned whether the DoT even had the authority to mandate such rules across non-telecom sectors, suggesting that the proposal may **violate the separation of regulatory domains**.

The Broader Debate on Digital Regulation in India

- This controversy comes amid a larger push by the Indian government to tighten digital security through legislation. Recent moves like:
 - The **Digital Personal Data Protection Act, 2023**
 - The **Digital India Act (in draft stage)**
 - Expanded roles for **CERT-In and the MeitY**
- reflect an assertive approach to securing India's growing digital landscape.
- However, concerns about **regulatory overlap, business costs, and innovation slowdowns** are increasingly surfacing.
- As India aims to be a global digital innovation hub, the challenge lies in **balancing national security objectives with ease of doing business**, especially for small tech enterprises and startups.

Source : **TH**

Source: <https://vajiramandravi.com/current-affairs/digital-firms-raise-alarm-over-mobile-number-validation-rules-in-india/>

© Vajiram & Ravi. For personal use only.