On 24 June 2025, the Ministry of Communications published draft amendments (Draft Amendment) to the Telecommunications (Telecom Cyber Security) Rules, 2024 (Cybersecurity Rules) issued under the Telecommunications Act, 2023 (Telecom Act), inviting stakeholder comments until 24 July 2025. The Draft Amendment seek to further strengthen the telecom cybersecurity framework by extending its applicability to users of telecom identifiers (such IMEI / MSISN / SIM numbers), enhancing the surveillance powers of the government and imposing additional obligations on telecom device importers and manufacturers.

Key highlights of the draft amendment

1. Scope and Applicability: While the original Cybersecurity Rules applied mainly to telecom licensees / authorized telecom entities (TEs), the Draft Amendment seeks to specifically include in its scope non-licensed entities that use telecom identifiers for user authentication and validation, known as telecommunication identifier user entities (TIUEs). Such entities may include digital platforms, OTTs and e-commerce platforms that allow OTP-based authentication and login for users.

2. Establishment of MNV Platform: The Draft Amendment also introduces the concept of 'mobile number validation platform' (MNV Platform). This is proposed as an online platform created by the government that helps telecom companies and other authorised service providers to check if a phone number (or other telecom identifier) actually belongs to the person claiming to use it. The MNV Platform will enable matching of these user-provided details with the corresponding user records in the database of the TE. A TIUE, either on its own, or in case of a government direction, can request a validation from the MNV portal, by submitting the request on the MNV Platform in the specified format and payment. TIUEs will have to pay a fee of INR 1.5 (per request) if TIUE makes the request pursuant to a government direction, or INR 3 (per request) if TIUE makes a suo moto request. The MNV Platform will route these requests to telecom operators for verification, and responses will be shared back through the MNV Platform. The validation can only be made for confirming user identity for service purposes, and all parties involved (TIUEs and TEs) must comply with data protection laws while handling customer data.

3. Additional obligations on telecom equipment manufacturers and importers: Government may direct telecom equipment manufacturers to assist in cases of tampered IMEIs and ensure they do not reuse IMEIs already active on Indian networks for new devices. The government will maintain a central database of tampered or restricted IMEIs, and entities buying or selling used mobile devices in India must check this database (by paying INR 10 per IMEI) before completing the transaction to avoid dealing in equipment bearing IMEI specified in the database.

4. Powers of the government: The Draft Amendment authorises the government to seek data related to telecom identifiers used by a TIUE and issue directions to TIUEs to suspend the use of the telecom identifiers for identifying customers or delivery of services. Additionally, TIUEs are also required to ensure compliance with directions and standards (including timelines) issued by the government for prevention of misuse of telecom identifiers.

Conclusion

While the proposed framework appears to be a promising effort to curb cybercrime and identity theft, it has triggered various concerns related to excessive on-going surveillance from the government as a default measure as opposed to an event-based surveillance, threat to user privacy, lack of regulatory basis for seeking data from TIUEs and absence of appropriate procedural safeguards, duplicity of regulations on TIUEs who are already regulated under the Information Technology Act, 2000 and its rules, etc. Additionally, it also results in increased compliance costs, especially for startups and MSMEs, both in terms of technological and infrastructure investment as well as the per-request fees for IMEI verification and TIUE validation.

Stakeholders have been requested to submit their comments and feedback on the Draft Amendment by 24 July 2025. The final rules are expected to be notified after the conclusion of the public consultation and will likely play a crucial role in shaping the cybersecurity and resilience of the telecom industry for the years ahead.

- Harsh Walia (Partner) and Sanjuktha A. Yermal (Senior Associate)

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1200 legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit www.khaitanco.com