



IMEI Tampering

Threat to Digital Sovereignty

23 September 2026

India's Growing Digital Ecosystem and the Need for Secure Devices

India's rapid digital transformation has made **telecommunications integral to everyday life, commerce and governance**. The country's active wireless mobile subscriber base reached **1,204.01 million in July 2026**. This vast subscriber base reflects the scale of India's connected digital ecosystem. Mobile networks and devices increasingly support **digital payments, online services and citizen-centric governance**. As dependence on these technologies grows, ensuring the **security and integrity of telecom networks and devices** becomes increasingly important.

This expanding digital ecosystem also brings new security challenges. One such concern is the misuse of the **International Mobile Equipment Identity (IMEI) number**. Tampering with or misusing IMEI numbers can facilitate the operation of devices with altered identities and complicate the identification of devices on telecom networks. Such practices can create challenges for law enforcement, consumer protection and network security. Strengthening the integrity of device identifiers is therefore essential for maintaining a secure, trusted and resilient telecommunications ecosystem.

What is Unlawful Tampering of an IMEI

It shall be unlawful if a person:

- Intentionally removes, obliterates, changes or alters unique Mobile Device Equipment Identification number; or
- Intentionally uses, produces, traffics in, has control or custody of, or possesses hardware or software knowing it has been configured as above.

Understanding IMEI

- **What is an IMEI?** The IMEI is a unique **15-digit number** that identifies a mobile device on a telecom network.
- **What does TAC mean?** The first eight digits of an IMEI form the **Type Allocation Code (TAC)**, which identifies the device model or type.
- **Who allocates IMEI numbers?** The Global System for Mobile Communications Association (GSMA) oversees the global allocation of TAC.



- **How are IMEIs assigned?** GSMA allocate TACs to manufacturers and brand owners. Manufacturers then assign unique IMEIs to individual devices.
- **How many IMEIs does a dual-SIM phone have?** A dual-SIM phone generally has two IMEI numbers, one for each SIM slot.
- **How can users find their IMEI?** Users can dial ***#06#** on their mobile device to display its IMEI number.
- **How can users verify an IMEI?** Users can visit Sanchar Saathi portal or mobile App or send **KYM <15-digit IMEI number>** by **SMS to 14422** to verify device details.

Everyone's Accountability Towards Safety

A secure telecom ecosystem requires responsibility across the entire device lifecycle, from manufacturing to everyday use. Manufacturers, importers, sellers and citizens each have a role in preventing misuse of IMEI.

- **Manufacturers** must register the IMEI numbers of all applicable telecom devices manufactured in India with the Government before their first sale, testing, research or other use. Registration is carried out through the Device Setu–Indian Counterfeited Device Restriction (ICDR) portal. Manufacturers must also ensure that devices are assigned valid, unique and untampered IMEI numbers.

- **Importers** must register IMEI numbers with the Central Government before importing applicable telecom equipment into India. The registration must be completed through the Device Setu–ICDR portal for devices intended for sale, testing, R&D or other purposes. Importers must ensure that imported devices carry valid and authorised IMEI numbers.
- **Resellers and retailers** must ensure that telecom devices offered for sale have valid and untampered IMEI numbers. Those dealing in used devices should verify the IMEI against the Government’s central database of tampered and blacklisted devices before completing transactions, by paying certain fees per IMEI verification. Selling or dealing in devices with tampered or configurable IMEIs can attract stringent legal action.
- **Brand owners** must ensure that devices sold under their brands comply with applicable IMEI registration and cybersecurity requirements. Their brands must be appropriately registered through the Device Setu–ICDR portal, linked to the relevant GSMA Type Allocation Code (TAC). They should ensure that devices placed on the market carry authentic and authorised IMEIs.

What Citizens Should Avoid

The Department of Telecommunications (DoT) advises citizens to refrain from activities that involve the tampering or misuse of telecommunication identifiers and resources:

- Using, procuring or assembling devices such as modems, modules, SIM Boxes or other equipment with configurable or tampered IMEIs.
- Procuring SIM cards through fake documents, fraud, cheating or impersonation.
- Transferring, selling or handing over SIM cards obtained in their name to others who may misuse them.
- Using mobile applications, websites or any other means to modify Calling Line Identity (CLI) or other telecommunication identifiers.

Sanchar Saathi Platform

Citizens can leverage the Sanchar Saathi platform to verify and secure their mobile handsets. The platform enables users to validate a device’s **IMEI details**, including the **brand, model, and manufacturer**, helping strengthen device authenticity and security. *Read more about the [Sanchar Saathi app](#).*



What Citizens Should Do

Consumers should take precautions to protect their devices and ensure that their IMEI numbers remain genuine and secure.

- Purchase mobile devices only from authorised sellers and verify the IMEI details.
- Use strong passwords, PINs or biometric authentication to secure the handset.

- Get devices repaired only at authorised service centres to reduce the risk of IMEI tampering or other malicious activity.
- In the event of device loss or theft, follow the official step-by-step blocking procedure:
 - i) File an immediate report with the local police and secure a copy of the complaint.
 - ii) Obtain a duplicate SIM card for the lost mobile number from your telecom operator. (Under TRAI regulations, SMS services are restricted for the first 24 hours of a re-issued SIM's activation. Since Sanchar Saathi requires a mobile OTP verification, you must wait 24 hours after activation to submit your request).
 - iii) Register the blocking request on the Sanchar Saathi (CEIR) portal or mobile app, uploading the police report and a valid ID proof to receive a unique Request ID.
 - iv) If your device is subsequently recovered, report it to the local police first, and then use your Request ID on the portal to safely unblock the handset.

Maintaining device security is a shared responsibility across the telecom ecosystem. Awareness, compliance and responsible use can further help prevent fraud, protect citizens and strengthen the security of India's digital infrastructure.

Legal Safeguards Against IMEI Tampering^{1&2}

India has established a strong legal framework to protect the integrity of the telecommunication ecosystem.

- The **Telecommunications Act, 2023** provides for stringent action against tampering with telecommunication identifiers, including the IMEI number of mobile handsets and other telecommunication devices.
- **Section 42(3)(c)** prohibits tampering with telecommunication identifiers. **Section 42(3)(e)** prohibits obtaining Subscriber Identity Modules (SIMs) or telecommunication identifiers through fraud, cheating or impersonation.
- Violations may attract imprisonment for up to **three years**, a fine of up to **₹50 lakh**, or both. Such offences are **cognizable and non-bailable** under **Section 42(7)** of the Act.
- Under **Section 42(6)**, persons who abet or promote the commission of such offences are also liable to the same punishment.

These provisions create a strong deterrent against IMEI tampering and misuse of telecom resources.

Safeguarding India's Digital Future

¹<https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2305203®=3&lang=1>
² <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763®=48&lang=2>

India's telecom journey reflects both remarkable progress and shared responsibility. Strong laws, verification tools and citizen awareness together keep this network secure and trustworthy. Every stakeholder – including the government, industry, and individual users- has a role in preserving this trust. A vigilant, informed citizenry remains the strongest defence against misuse. Sustained cooperation will keep India's digital connectivity safe for generations to come.

References:

Ministry of Communications

- <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2305203®=3&lang=1>
- <https://www.ceir.gov.in/Home/index.jsp>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763®=48&lang=2>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763®=48&lang=2>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763®=48&lang=2>
- <https://www.eservices.dot.gov.in/sites/default/files/circular-notifications/cybersecurity-rules-2024.pdf>
- <https://www.eservices.dot.gov.in/sites/default/files/circular-notifications/telecom-cyber-security-amendment-rules-2025.pdf>
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2193461&lang=2®=3&utm_source
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=1598008&lang=2®=3&utm_source

Telecom Regulatory Authority of India

- www.trai.gov.in/sites/default/files/2026-08/PR_No116of2026_0.pdf

PIB Research