DATA PROTECTION, INTERCEPTION AND NATIONAL SECURITY

The Telecom Sector's Compliance Tightrope

Navigating overlapping obligations under the DPDP Act 2023, the Telecommunications Act 2023, and India's cybersecurity and national-security framework

Telecom operators now walk a three-way tightrope

Every telecom service provider in India must simultaneously protect subscriber data, enable lawful interception on demand, and defend its networks from cyber and financial fraud — under three statutes that were not written with each other in mind.

The obligations don't just coexist they occasionally pull in opposite directions.

Protect

DPDP Act, 2023 — consent, purpose limitation, breach notification to citizens & the Board

Surrender on Order

Telecommunications Act, 2023 — interception, traceability, suspension on national-security grounds

Defend

Telecom Cyber Security Rules, 2024 — mandatory incident reporting & fraud-risk sharing

AGENDA

01 **Overlapping Regulatory Regimes**

DPDP Act, Telecommunications Act, Telegraph Rules

02 **National Security & Public Safety Powers**

Takeover, suspension, biometric ID, judicial scrutiny

03 **Cybersecurity & Fraud Prevention**

Telecom Cyber Security Rules, SIM-swap, FRI

04 **Compliance Burden & Litigation Risk**

Overlaps, adjudication, penalties, data localization

05 **The Path Forward**

An integrated compliance architecture

Three regimes govern one subscriber record

DPDP Act, 2023

- Applies to telcos as “Data Fiduciaries”
- Consent, notice & purpose limitation
- Breach notice to Data Protection Board
- Phased enforcement through May 2027

Telecommunications Act, 2023

- Interception, message traceability
- Equipment & network standards
- Supersedes Telegraph Act, 1885
- Phased commencement since June 2024

Telegraph Rules, 1951

- Rules 419 / 419A now superseded
- Existing interception orders continue
- Procedural DNA carried into 2024 Rules
- Review-committee model persists

The DPDP Act, 2023 meets the telecom operating model

Telecom service providers process India's largest and most sensitive pool of personal data identity documents, location trails, call and message metadata, and payment details. The DPDP Act, operationalised by the DPDP Rules 2025, now applies squarely to that data.

Consent & notice:
Verifiable, itemised consent for subscriber onboarding, VAS and marketing communication

Breach notification:
Reporting obligations to the Data Protection Board and affected subscribers

Cross-border transfer:
Blacklist-style model — transfers permitted unless the destination is restricted

Section 17 carve-outs:
Exemptions for processing in the interest of sovereignty, security & public order — the seam with the Telecom Act

₹250 Cr

maximum penalty per instance for failure to take reasonable security safeguards against a personal data breach

Telecommunications Act, 2023: interception, traceability & standards

Interception power (Sec. 20)

Central/State agencies may intercept, detain or disclose messages on occurrence of a public emergency or in the interest of public safety, national security, sovereignty, or public order.

2024 Interception Rules

The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 (notified 6 Dec 2024) now govern the process — competent authority sign-off, review committee oversight, and defined retention limits.

Message traceability

Telecom entities must be able to trace the origin of messages on their networks to curb spam, spoofing and fraudulent commercial communication.

Equipment & network standards

Mandatory standards for telecom equipment, testing and certification — tying network security directly to licensing conditions.

The Indian Telegraph Rules never fully disappear

1885

Indian Telegraph Act

Original source of government power to intercept & take over telecom services

1996–97

PUCL v. Union of India

Supreme Court reads procedural safeguards into Rule 419A after unregulated phone-tapping

2023

Telecommunications Act enacted

Repeals the Telegraph Act but keeps its rules in force pending replacement

Dec 2024

New Interception & Cyber Security Rules

Formally supersede Rules 419 & 419A — but retain their review-committee architecture

Today

Transitional overlap

Interception orders issued under the old Rules continue to run until they expire

Why it matters: legacy procedural safeguards — competent-authority sign-off, bi-monthly review committees — remain the backbone of "lawful" interception even under the new Act.

SECTION 2

National Security & Public Safety Powers

Where the State’s emergency powers meet the operator’s duty of care to subscribers

Government's power to take over or suspend services

Temporary possession / takeover

On the occurrence of any public emergency, or in the interest of public safety, the Central or State Government may take temporary possession of any telecommunication service or network or direct its management from the licensee.

Grounds: sovereignty & integrity of India · security of the State · friendly relations with foreign States · public order · preventing incitement to an offence

Suspension of telecom services

The same grounds empower authorities to suspend telecom services in a region. The statutory basis long used for internet shutdowns, now folded into the Telecommunications Act framework alongside the 2024 Rules.

Operator obligation: comply within tight windows while preserving evidentiary and audit trails — non-compliance risks licence action.

Biometric identification: the trust layer for every SIM

Fraudulent and impersonated SIM issuance has been a persistent vector for both crime and interception evasion. DoT policy now requires biometric, Aadhaar-based e-KYC as the standard for new subscriber acquisition and bulk/enterprise connections.

- **Point-of-sale accountability**

  Franchisees and retailers verified & graded; repeat violators delisted

- **Sanchar Saathi integration**

  Subscriber and device data linked to a national portal for fraud & theft reporting

- **Bulk connection scrutiny**

  Enhanced verification for enterprise and long-distance bulk SIM issuance

Biometric ID sits at the exact intersection of this deck's three regimes:

DPDP consent for biometric collection • Telecom Act identity assurance for lawful traceability • Cyber Security Rules' fraud-prevention mandate

Judicial scrutiny: proportionality is not optional

Since PUCL v. Union of India (1997) first read procedural safeguards into interception, and K.S. Puttaswamy v. Union of India (2017) recognised privacy as a fundamental right, courts have tested every surveillance and data measure against a four-part standard.

1 — Legitimate Aim

A goal the State may lawfully pursue — security, public order, crime prevention

2 — Suitability

The measure must be a rational means to that end

3 — Necessity

No less-intrusive, equally effective alternative is available

4 — Balancing

The measure's benefit must not be disproportionate to the rights it burdens

Practical effect for telcos: interception and data-sharing requests are increasingly expected to show reasoned, order-specific necessity — blanket compliance is a growing litigation exposure, not a safe harbour.

SECTION 3

Cybersecurity & Fraud Prevention

Defending the network is now a standalone statutory duty — with its own reporting clock

Telecom Cyber Security Rules, 2024: a standalone duty

Chief Telecom Security Officer

Every telecom entity must designate a senior officer accountable for cybersecurity governance

Mandatory incident reporting

Cybersecurity incidents must be reported to Government-designated authorities within prescribed short timelines

Traffic data collection powers

Government may direct entities to furnish traffic data and other specified data for cybersecurity purposes

Security testing & certification

Network equipment and telecom identifiers subject to testing, security assurance and disclosure requirements

The fraud landscape telcos must police in real time

SIM-Swap Fraud

Bad actors fraudulently reissue a victim's SIM to hijack OTPs and drain bank accounts — placing telcos at the center of financial-fraud liability disputes.

Caller-ID Spoofing

Manipulated caller identity is used for scam and impersonation calls; traceability mandates under the Telecom Act directly target this vector.

International Revenue-Share Fraud (IRSF)

Traffic is artificially pumped to premium international numbers, generating disputed inter-carrier settlement liabilities running into crores.

Financial Fraud Risk Indicator: turning telecom data into a shield

DoT's Financial Fraud Risk Indicator (FRI) flags mobile numbers as low, medium or high risk based on complaint patterns, and shares that signal with banks and financial institutions in near real time through inter-agency platforms.

Subscriber reports fraud

via Chakshu / operator channels

Risk signal generated

aggregated across operator complaint data

Shared with banks & FIs

through the Digital Intelligence Platform

Transaction flagged or blocked

before the fraud completes

Why compliance teams should care

Inter-operator and inter-sector data sharing for fraud prevention must itself satisfy DPDP consent/exemption logic — turning a fraud-control tool into a fresh data-protection compliance question.

SECTION 4

Compliance Burden & Litigation Risk

Three regulators, three timelines, one incident — the operational reality of overlap

One breach, three overlapping obligations

Trigger Event	DPDP Act, 2023	Telecom Cyber Security Rules, 2024	IT Rules, 2021 (where applicable)
Personal data breach	Notify Data Protection Board & affected principals	Report as a cybersecurity incident to designated authority	Report to CERT-In for covered intermediaries/VAS
Regulator	Data Protection Board of India	Department of Telecommunications	CERT-In / MeitY
Reporting clock	"Without delay", per DPDP Rules timelines	Short, prescribed window from detection	Within 6 hours of notice (CERT-In directions)
Appeal route	Telecom Disputes Settlement & Appellate Tribunal	Designated Adjudicating Officer → TDSAT	Appellate mechanisms under IT Act

Same underlying incident — three notification duties, three regulators, three clocks. Compliance calendars built around a single statute miss this.

Adjudication and penalties: where enforcement bites

Both the DPDP Act and the Telecommunications Act create dedicated adjudicatory tracks. For “authorized entities” under the Telecom Act, telecom licensees and their vendors. A Designated Adjudicating Officer can penalise contraventions, with appeal to the TDSAT.

Show-cause first:

Adjudicating Officer must issue notice and hear the entity before penalty

Graded penalties:

Calibrated to the nature and gravity of the contravention, not a flat fine

Board vs. Officer:

DPDP breaches go to the Data Protection Board; Telecom Act contraventions go to the Adjudicating Officer — different forums, different procedures

One appellate home:

Both routes ultimately converge at the TDSAT — a rare point of procedural unity

Litigation-risk signal

With enforcement of the DPDP Act phasing in through 2027 and the Telecom Act’s rules still maturing, telcos face parallel, evolving exposure the safest posture is to document proportionality and necessity for every disclosure decision now.

Data localization: one Act, several sectoral answers

DPDP Act, 2023

Default position is transfer permitted, subject to a Government "restricted list" of countries — a blacklist, not a whitelist, model.

Sectoral overlays

RBI payment-data localization norms and telecom licensing conditions can be stricter than the DPDP default for the same dataset (e.g., mobile wallet, UPI-linked data).

Practical friction

Global cloud, analytics and customer-support vendors used by telcos must be mapped against every applicable regime — not just the DPDP Act's list.

Emerging dispute pattern

Enforcement actions and vendor disputes are increasingly turning on where a subsidiary's technical support or backup infrastructure actually sits — not just where the telco's primary systems are hosted. Contractual data-flow maps are becoming as important as the policy itself.

Building one compliance architecture, not three

Unify the governance model

Bring DPDP, Telecom Act and cybersecurity obligations under one accountable owner, not three siloed teams filing separately.

Build a single incident playbook

One breach-response process that triggers all applicable notifications the Data Protection Board, DoT, CERT-In is on their respective clocks.

Document proportionality by default

Treat every interception/disclosure request as a recorded, reasoned decision — not a rubber stamp — anticipating judicial review.

Map data flows end-to-end

Maintain a live map of where subscriber data sits and moves, tested against DPDP, RBI and licence conditions simultaneously.

Train the front line

Point-of-sale, call-center and network-ops staff are where biometric KYC, fraud flags and lawful-order execution actually happen.

KEY TAKEAWAY

The tightrope isn’t going away — but it can be walked with a plan.

Data protection, national security and cybersecurity obligations will keep evolving in parallel. Telecom operators that govern them as one integrated program — not three compliance silos — will move faster and litigate less.