

Ad. Deepak M. Tiwari

Advocate, High Court & Subordinate Courts

PRACTICE NOTE — CYBER & INFORMATION TECHNOLOGY LAW

The Information Technology Act, 2000 — Key Points

Electronic records, cyber offences, data protection, intermediary liability, blocking & interception, and adjudication

Title note: There is no "Information Technology Act, 2005." India's cyber law is the **Information Technology Act, 2000**, substantially recast by the **IT (Amendment) Act, 2008** (which introduced S.66A–66F, S.67A/67B, S.69/69A, and data-protection provisions under S. 43A). This note covers the Act as it currently stands, including the IT Rules, 2021 and the October 2025 Amendment Rules.

STRUCTURE

13 Chapters, 94 Sections, 4 Schedules

MAJOR AMENDMENT

IT (Amendment) Act, 2008 — added cyber-offence provisions, data protection (S.43A), intermediary due diligence (S.79)

KEY RULES IN FORCE

IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021, as amended 2022 and 2025 (in force 15 Nov 2025)

DATA PROTECTION OVERLAP

S.43A/SPDI Rules 2011 remain in force alongside the DPDP Act, 2023 — repeal of S.43A tied to DPDP Act's final phase (expected ~13 May 2027)

DEAD LAW ALERT

Section 66A struck down (Shreya Singhal, 2015) — SC/PUCL proceedings confirm continuing (unlawful) use by some police stations; always check for wrongful S.66A invocation

LEGAL RECOGNITION OF ELECTRONIC RECORDS & SIGNATURES

SECTIONS 4–10A — VALIDITY

- Electronic records and electronic signatures are given legal recognition equivalent to paper records/signatures for most purposes (subject to exceptions in the First Schedule, e.g. certain negotiable instruments, wills, trusts, and real property conveyance documents); electronic contracts are enforceable (S.10A).

SECTIONS 3, 3A — ELECTRONIC/DIGITAL SIGNATURE

- S.3 recognises digital signatures via the asymmetric crypto-system/hash-function method; S.3A (2008 Amendment) technology-neutrally recognises **electronic signatures** more broadly via any reliable authentication technique notified by the Central Government (e.g. Aadhaar e-Sign).

DAMAGE TO COMPUTER SYSTEMS & DATA PROTECTION

SECTION 43 — CIVIL LIABILITY

- Unauthorised access, downloading/copying data, introducing a virus/contaminant, damaging a computer/database, denial of access, or assisting another to do so: liable to **pay compensation** to the affected person — a civil remedy, adjudicated by the Adjudicating Officer (S.46) or a competent court.

SECTION 43A — BODY CORPORATE DATA PROTECTION

- A body corporate possessing/handling **sensitive personal data** that is negligent in maintaining reasonable security practices, causing wrongful loss/gain, is liable to pay damages — read with the SPDI Rules, 2011. **Remains in force** alongside the DPDP Act, 2023 until the DPDP Act's final phase is notified.

CYBER OFFENCES — CHAPTER XI (ILLUSTRATIVE)

SECTION	OFFENCE	KEY POINT
S.66	Hacking / computer-related offences	Dishonest/fraudulent act referred to in S.43 — imprisonment up to 3 years and/or fine up to ₹5 lakh.

S.66A	Offensive messages	Struck down as unconstitutional (Shreya Singhal v. Union of India, 2015) — should never be invoked; continuing FIRs under this section are unlawful and challengeable.
S.66C	Identity theft	Fraudulent/dishonest use of another's password, electronic signature, or unique identification feature.
S.66D	Cheating by personation using computer resource	Common basis for online fraud/phishing prosecutions.
S.66E	Violation of privacy	Capturing, publishing, or transmitting the image of a person's private area without consent.
S.66F	Cyber terrorism	Acts intended to threaten unity/integrity/security of India via computer resource — punishable with imprisonment for life .
S.67 / 67A / 67B	Obscenity / sexually explicit material / child sexual abuse material	Graded penalties, escalating sharply for S.67B (material depicting children) — read with POCSO where applicable.

INTERCEPTION, MONITORING & BLOCKING

SECTION 69 — INTERCEPTION/MONITORING/ DECRYPTION

- Central/State Government may direct interception, monitoring, or decryption of information through a computer resource, on grounds of sovereignty/integrity of India, defence, security of the State, friendly relations with foreign States, public order, or preventing incitement to a cognizable offence — subject to procedural safeguards under the IT (Procedure for Interception) Rules.

SECTION 69A — WEBSITE/CONTENT BLOCKING

- Government may direct blocking of public access to information on the same specified grounds, by written, reasoned order, following the IT (Blocking) Rules, 2009 procedure — intermediaries must comply; non-compliance is punishable with imprisonment up to 7 years and fine.

BREACH OF CONFIDENTIALITY & PRIVACY

SECTION 72 — BREACH OF CONFIDENTIALITY

- A person who, in exercising powers under the Act/Rules, discloses information obtained without the consent of the person concerned: imprisonment up to 2 years and/or fine up to ₹1 lakh — aimed primarily at officials/persons with statutory access (e.g. Certifying Authority personnel).

SECTION 72A — DISCLOSURE IN BREACH OF CONTRACT

- A person providing services under a lawful contract who discloses personal information without consent (or in breach of the contract), intending or knowing it is likely to cause wrongful loss/gain: imprisonment up to 3 years and/or fine up to ₹5 lakh — the key criminal-liability provision for data-breach-style misconduct by service providers.

SECTION 79 — SAFE HARBOUR FOR INTERMEDIARIES

CONDITIONAL IMMUNITY, NOW NARROWING

- An intermediary is **not liable** for third-party information/data/communication link hosted/transmitted, provided its function is limited to providing access, it does not initiate/select the receiver/modify the transmission, and it observes due diligence under the Act/Rules — immunity is lost if it fails to expeditiously remove/disable access to unlawful content on receiving actual knowledge (court order or appropriate government notification) under S.79(3)(b).
- The October 2025 IT Rules Amendment has **narrowed** this safe harbour further — see below.

IT RULES, 2021 & THE OCTOBER 2025 AMENDMENT

INTERMEDIARY DUE DILIGENCE — CURRENT POSITION

- **2021 Rules:** distinguish "social media intermediary" from "significant social media intermediary" (SSMI, above a user threshold) — SSIMs must appoint a Chief Compliance Officer, a Nodal Contact Person (24×7 law-enforcement liaison), and a Resident Grievance Officer, and enable traceability of the "first originator" of certain messages.
- **2025 Amendment (in force 15 Nov 2025):** targets deepfakes/synthetic content; unlawful-content takedown intimations may now only be issued by a senior officer (not below Joint Secretary rank, or DIG rank for police), must be reasoned with a stated legal basis, are subject to monthly secretary-level review, and the prior express protection for **voluntary** takedowns has been **removed** — intermediaries must now comply strictly with the 36-hour removal timeline on receiving a valid intimation and exercise their own care around voluntary moderation.

ADJUDICATION & APPEAL

SECTION 46 — ADJUDICATING OFFICER

- Central Government appoints an officer (not below the rank of Director to the Government of India, or State equivalent) as Adjudicating Officer to inquire into and decide contraventions/compensation claims under the Act. Adjudicating Officer's jurisdiction is generally for claims **up to ₹5 crore**; above that, jurisdiction lies with the competent civil court.

TDSAT — APPELLATE FORUM

- The erstwhile Cyber Appellate Tribunal (S.48) was merged into the **Telecom Disputes Settlement and Appellate Tribunal (TDSAT)** by the Finance Act, 2017. An appeal against an Adjudicating Officer's (or Controller's) order lies to TDSAT, ordinarily within **45 days**; further appeal on a question of law/fact lies to the High Court.

PRACTICE NOTES

Always Check for Wrongful Section 66A Invocation

If a client is charged/an FIR is registered citing S.66A, immediately flag this as unconstitutional and unlawful per *Shreya Singhal* (2015) and the subsequent PUCL proceedings — this remains a live, recurring issue despite the section's 2015 striking-down.

S.43 (Civil) vs S.66 (Criminal) — Choose the Right Track

For data/system damage without criminal intent, a S.43 compensation claim before the Adjudicating Officer can be faster and more proportionate than pursuing a S.66 criminal complaint — assess client objectives (compensation vs. deterrence/prosecution) before choosing the forum.

Track the DPDP Act Transition for Data-Breach Advice

S.43A and the SPDI Rules, 2011 remain the operative data-protection framework for now, but advise corporate clients to prepare for the DPDP Act, 2023's phased rollout (through ~May 2027) — data-handling policies should already be built around both regimes.

Intermediary/Platform Clients — Reassess Voluntary Moderation Risk

Given the October 2025 Amendment's removal of express protection for voluntary takedowns, advise platform clients to tighten internal moderation SOPs and ensure strict, timely compliance with valid removal intimations from authorised officers only.

For internal practice reference only — this note highlights select, frequently used provisions of the Information Technology Act, 2000 (as amended, 13 Chapters, 94 Sections) and the IT Rules, and does not cover the full Act/Rules. Cross-check exact section/rule text and the latest MeitY notifications before relying in advice or proceedings. Prepared 2 August 2026.

Primary sources: The Information Technology Act, 2000 (indiacode.nic.in, meity.gov.in); IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and Amendment Rules, 2025; *Shreya Singhal v. Union of India* (2015) and PUCL implementation proceedings via Supreme Court Observer/LiveLaw; Digital Personal Data Protection Act, 2023 and Rules, 2025; commentary via SCC Online, Lexology, ApniLaw, and CIS-India.