Chapter XI-A - Cyber Offences

Separate civil contraventions and criminal offences; preserve forensic and authorisation evidence.

Chapter in 2 Minutes

- Identify the legal trigger, responsible actor and evidence relevant to cyber offences.
- Read the Act with all effective Rules, regulations, notifications, directions, guidelines and forum procedure as at the event date.
- Separate substantive obligation, operational workflow, filing or reporting, enforcement consequence, remedy, appeal and limitation.
- Maintain a reproducible source pack, decision memo, approval trail and transaction-level evidence.
- Apply connected company, contract, tax, accounting, data, competition, consumer, insolvency and sector-law overlays independently.

Provision / instrument map

Provision	Subject / control
S. 65	Tampering with computer source documents
S. 66	Computer-related offences
S. 67	Publishing or transmitting obscene material
S. 68	Cyber offences and enforcement - official section title to be read from the current Act
S. 69	Interception, monitoring or decryption
S. 70	Protected system
S. 71	Cyber offences and enforcement - official section title to be read from the current Act
S. 72	Breach of confidentiality and privacy
S. 73	Cyber offences and enforcement - official section title to be read from the current Act
S. 74	Cyber offences and enforcement - official section title to be read from the current Act
S. 75	Act applies outside India
S. 76	Cyber offences and enforcement - official section title to be read from the current Act
S. 77	Cyber offences and enforcement - official section title to be read from the current Act
S. 78	Cyber offences and enforcement - official section title to be read from the current Act
S. 66A	Cyber offences and enforcement - official section title to be read from the current Act
S. 66B	Cyber offences and enforcement - official section title to be read from the current Act
S. 66C	Identity theft
S. 66D	Cheating by personation using computer resource
S. 66E	Violation of privacy
S. 66F	Cyber terrorism
S. 67A	Sexually explicit material
S. 67B	Child sexual material
S. 67C	Cyber offences and enforcement - official section title to be read from the current Act
S. 69A	Blocking public access
S. 69B	Traffic data monitoring
S. 70A	National nodal agency for critical information infrastructure
S. 70B	CERT-In
S. 72A	Disclosure in breach of lawful contract
S. 77A	Compounding of offences
S. 77B	Offences with three-year imprisonment to be bailable

Implementation and practical application

A business decision raises cyber offences. The team should freeze the relevant chronology, identify every actor and legal relationship, map the current provision and delegated instrument, preserve system and communication evidence, quantify exposure, and choose cure, filing, response, settlement or litigation only after checking jurisdiction and limitation.

Control checklist

Classify facts and role; capture current source; map approvals and evidence; calculate threshold/time/exposure; implement system gate; preserve filing and delivery proof; verify forum and limitation.

Cross-law overlays

Contract, company/LLP, tax/accounting, data/cyber, consumer, competition, MSMED, RERA, FEMA, IBC, sector law and evidence rules must be applied separately.

Legal-use note

This publication is not a verbatim statutory reproduction. Official source and signed Gazette prevail.