Compliance & Security Framework
(Chapter -2 : DISSA Course)

Arijit Chakraborty

Jan 23 , 2022

IT Act 2000

- Enacted on 17th May 2000-
- India is **12th nation** in the world to adopt cyber laws
- The original Act = 94 sections, divided into 13 chapters and 4 schedules.
- The laws apply to the whole of India. If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under the law
- Introduced by - Pramod Mahajan, Minister of Communications and Information Technology
- Amended by - IT (Amendment) Act 2008

Objectives of the IT Act

To provide legal recognition for transactions:-

- Carried out by means of electronic data interchange, and other means of electronic communication, commonly referred to as "electronic commerce"
- To facilitate electronic filing of documents with Government agencies and E-Payments
- To amend the Indian Penal Code, Indian Evidence Act,1872, the Banker's Books Evidence Act 1891,Reserve Bank of India Act ,1934
- Aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

IT Amendment Act (ITA2008)

- An Act to provide **legal recognition for transactions** carried by EDI
- Act is administered by **Indian Computer Emergency Response Team** (CERT-In).
- Amended by IT Amendment Bill passed in LS on Dec 22nd and in RS on Dec 23rd of 2008.

- Facilitate **e- filing of documents**
- Facilitate **electronic storage of data**
- Give **legal sanction & facilitate e- transfer of funds b**etween banks & FI
- **Amendment =**
- introduced Section 66A which penalized sending "offensive messages".
- Introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".
- introduced provisions addressing - pornography, child porn, cyber terrorism

Civil offences under IT Act

- **Chapter IX of IT Act, Section 43**
- Whoever without permission of owner of computer
  - Secures access
  - Downloads, copies, extracts any data
  - Introduces or causes to be introduced any viruses or contaminant
  - Damages or causes to be damaged any computer resource
    - Destroy, alter, delete, add, modify or rearrange
    - change the format of a file
    - Disrupts or causes disruption of any computer resource
    - Preventing normal continuance of computer

- Denies or causes denial of access by any means
- Denial of service attacks
- Assists any person to do any thing above
- Rogue Websites, Search Engines, Insiders providing vulnerabilities
- Charges the services availed by a person to the account of another person by tampering or manipulating any computer resource
- Credit card frauds, Internet time thefts
- **Liable to pay damages not exceeding Rs. One crore to the affected party**
- **Investigation by ADJUDICATING OFFICER**

Offences-
Cybercrime provisions

- Section 65 - Tampering with computer source documents
- Section 66 - Hacking with computer system
- Section 66 B – received stolen computer / communication device
- section 66 C- Using PW of another person
- Section 66 F – Acts of cyber-terrorism
- section 67 – publishing obscene information
- Section 67C - Failure to maintain records
- Section 68 - Failure/refusal to comply with orders
- Section 69 - Failure/refusal to decrypt data
- Section 70 - Securing access to a protected system
- Section 71 – Misrepresentation
- Section 72 – breach of confidentiality & privacy
- section 73 – publishing false DSC

Sec 69: Decryption of information

- **Ingredients**
- Controller issues order to Government agency **to intercept any information transmitted through any computer resource.**
- Order is issued in the interest of the:
- sovereignty or integrity of India,
- the security of the State,
    - friendly relations with foreign States,
    - public order or
    - preventing incitement for commission of a cognizable offence
    - Person in charge of the computer resource **fails to extend all facilities and technical assistance to decrypt information**- punishment up to 7 years.

Forgery

Andhra Pradesh Tax Case

In the explanation of **Rs. 22 Crore recovered** from house of owner of a plastic firm by vigilance department,

accused person submitted 6000 vouchers to legitimize the amount recovered,

but after **careful scrutiny of vouchers and contents of his computers** it revealed that

all of them were made **after the raids were conducted** .

All vouchers were **fake computerized vouchers.**

Essence

- Information Technology Act 2008 = **suitable case for analytical study of cyber crime issues.**
- **Comprehensive, clear framework.**
- Legal recognition to the Virtual electronic medium.

- *‘’ Information technology and cybercrime becoming inextricably interwoven. I don't think anybody can talk meaningfully about one without the talking about the other.”*
- - Bill Gates

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

- Social media intermediaries, with registered users in India above a notified threshold, have been classified as **significant social media intermediaries (SSMIs).**
- SSMIs required to observe certain additional due diligence

✓ appointing certain personnel for compliance,

✓ enabling identification of the first originator of the information on its platform under certain conditions,

✓ deploying tech-based tool on best-effort basis to identify certain types of content.

- The Rules prescribe a framework for the regulation of content by online publishers of news and current affairs content, and curated audio-visual content.

- All intermediaries are required to provide a grievance redressal mechanism for resolving complaints from users or victims.
- A 3-tier grievance redressal mechanism with varying levels of self-regulation has been prescribed for publishers.

Objective

- ‘’ *In order to ensure an Open, Safe & Trusted Internet and accountability of intermediaries including the social media intermediaries to users and in tune with the changing requirements, the Rules have been revised* ‘’
- **- MEITy**
- The Rules have come into effect from : date of their publication in the Gazette (i.e., 25th February, 2021).
- The threshold criteria [Ref. rule 2(1)(v)] for **significant social media intermediaries (SSMI)** was published on 26th February, 2021.
- Additional due diligence for SSMI have come into effect **from 26thMay, 2021**

Due diligence by intermediaries

- **Rule 3(1)(d) requires an intermediary to remove or disable access to certain information about which the intermediary is notified/ requested by Appropriate Government / its agency within 36 hours**
- **Intermediaries** :**entities store /transmit data on behalf of other persons.**
- Intermediaries : **internet or telecom service providers**, **online marketplaces, & social media platforms.**
- **DD includes:**
- (i) **informing users about rules and regulations, privacy policy**, and **terms and conditions** for usage of its services,
- (ii) **blocking access to unlawful information within 36 hours** upon **an order from the Court, or the government,**
- (iii) **retaining information collected for the registration of a user for 180 days** after **cancellation or withdrawal of registration**.
- (iv) Intermediaries **required to report cybersecurity incidents** and share related information with **Indian Computer Emergency Response Team**

Significant social media intermediaries:

- Social media intermediary with **registered users in India above a threshold** – say, 5 Million (to be notified) classified as **Significant Social Media Intermediaries**.
- Additional due diligence to be observed by them:
- (i) appointing a **chief compliance officer** to ensure compliance with IT Act & Rules,
- (ii) appointing a **grievance officer residing in India**, and
- (iii) publishing a **monthly compliance report.**

Grievance redressal

- The intermediaries required to designate a **grievance officer** to address complaints
- Complaints **must be acknowledged within 24 hours & disposed within 15 days.**
- **"Chief Compliance Officer"** – KMP / senior employee of a significant social media intermediary **who is resident in India**."

In case of digital media publishers (news and OTT), a **3-tier grievance redressal** mechanism will be in place for dealing with complaints regarding content:

- (i) **self-regulation** by the publishers,
- (ii) **self-regulation by the self-regulating bodies** of the publishers, and
- (iii) **oversight mechanism by the central government**.
- The publisher will appoint a **grievance redressal officer** **based in India** and address complaints within 15 days.
- **Oversight mechanism: Ministry of Information and Broadcasting** (MIB) will establish an **Inter-Departmental Committee** to hear grievances **not addressed by self-regulatory bodies** and also oversee **adherence to code of ethics.**

Non-compliance & consequence

- **Invoking of section 79 of the IT Act**
- Clearly mentioned in new IT Rules 2021.
- "When an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of Act shall not be applicable for such intermediary **and the intermediary shall be liable for punishment under any law including the provisions of the Act & Indian Penal Code"**.
- Section 79 specifically gives digital media platforms such as Facebook, Twitter, YouTube & WhatsApp **legal immunity in a way against liability for posts made on their networks**, **third party information or data**.
- That **legal immunity will be withdrawn** if non-compliance becomes an issue.

Timeframes for action by an intermediary

S.N.	Actions to be taken by the intermediaries	Timeframe	Reference in the Rules
1.	Grievance Acknowledgement	24 Hours	Rule 3(2)(a)
2.	Response to Grievance	15 days	Rule 3(2)(a)

S.N.	Actions to be taken by the intermediaries	Timeframe	Reference in the Rules
3.	Removal/ disabling of content which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual	Within 24 hrs	Rule 3(2)(b)

4.	Content removal on receipt of court order or notice from Appropriate Government or its agency	36 hours	Rule 3(1)(d)
5.	Provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities	Within 72 hours of the receipt of an order	Rule 3(1)(j)
6.	Preservation of information and associated records relating to removal/ disabling of access to such information	180 days or as may be required	Rule 3(1)(g)
7.	Retaining user's registration information after cancellation or withdrawal of his registration	180 days	Rule 3(1)(h)

OTT Platform, News Publishers & Digital Media = Code of Ethics for Digital Media Publishers:

- **Over-the-top (OTT) Platforms- (like Netflix and Amazon Prime Video)**
- The new rules call OTT platforms **'publishers of online curated content'.**
- They would have to **self-classify the content** into **5 categories** based on age.
  - U (Universal)
  - U/A 7+
  - U/A 13+
  - U/A 16+
  - A (Adult)
- OTT platforms **required to provide parental lock systems** for content classified U/A 13+ or higher, & **have age verification mechanism f**or content classified as 'Adult'.
- The **rating for content & content's description with viewer discretion message should be prominently displayed before programme starts** so that users can make informed decisions based on suitability.
- **News Publishers**
- **Publishers of news on digital media** should observe **Norms of Journalistic Conduct of the Press Council of India** & **Programme Code under the Cable Television Networks Regulation Act 1995** to provide a level playing field between the offline (Print, TV) and digital media.