INFORMATION TECHNOLOGY ACT, 2000

27th November, 2019

MCR HRD –

94th Foundation Course (FC)

A.Ram Kumar,
Advocate.

High Court of Hyderabad for the State of Telangana and State of Andhra Pradesh

Intellectual Property Rights & Information Technology

ashokramkumar@gmail.com **C: 9849674599**

Copyright disclaimer

- This presentation is the work of the author and owned by the author and is protected by worldwide copyright laws, all rights reserved. This presentation either in part or whole cannot be copied or transmitted in any form with out the express written permission permission of the author. Excerpts from this presentation can be used only for personal use and cannot be used for commercial purpose, giving a lecture or presentation before audience, or form part of any articles or research paper that could be published in a Journal.

Men are not hanged for stealing horses,

but that horses may not be stolen.

Criminal Offences under IT Act

Sec 65- Tampering with Computer Source Documents

Whoever knowingly or intentionally (this what prosecution needs to prove) - mens rea

conceals, destroys or alters / causes another to – Act

computer source code used for a computer, computer programme, computer system or computer network – object

computer source code is required to be kept or maintained by law - legal requirement

imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both - punishment

Destroying and altering includes deleting happened due to Hacking – word not specifically used in the Section nor in the definitions.

Eg: Hacking, Data Theft, credit card fraud, Forgery, web defacement and jacking

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 COMPUTER RELATED OFFENCES (SUBSTITUTED VIDE ITAA 2008)

The old provision specifically had the word “Hacking”. Removal of the word was done to include the acts even in other provisions like, 66, 66C etc.

Even under old act Hacking was not defined.

Whoever dishonestly, or fraudulently - mens rea

(meaning as in Sec 24 and 25 of IPC)

Does any Act referred in Sec 43 referred in (a) to (i) – Act

Computer, computer system or computer network – object

imprisonment up to three years, or with fine which may extend up to 5 lakh rupees, or with both - punishment

Eg Using WiFi services of other illegally

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 COMPUTER RELATED OFFENCES (SUBSTITUTED VIDE ITAA 2008)

Whoever dishonestly, or fraudulently - mens rea

(meaning as in Sec 24 and 25 of IPC)

Does any Act referred in Sec 43 referred in (a) to (i) – Act

Computer, computer system or computer network – object

imprisonment up to three years, or with fine which may extend up to 5 lakh rupees, or with both - punishment

Eg Using WiFi services of other illegally

Differences between 65 and 66:

1. Differences in ingredients of mens rea
2. To invoke 66, 43 ingredients have to be read into
3. While 65 may be a limted to Hacking 66 has very wide connotation

Where ingredients of Sec 43 are involved safe to include Sec 65 and 66 also in complaint along with sec 43.

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 A PUNISHMENT FOR SENDING OFFENSIVE MESSAGES THROUGH COMMUNICATION SERVICE, ETC.(INTRODUCED VIDE ITAA 2008)

it is framed in vague and sweeping language, which allows law enforcement authorities to interpret it in a subjective manner.

loosely worded and puts too much powers in the hands of the police.

For politicians, Section 66A is the big stick.

Main focus – loosely worded and possibility of abuse

What is lost : “there was a need for a mechanism to put checks and balances on this medium”

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 B PUNISHMENT FOR DISHONESTLY RECEIVING STOLEN COMPUTER RESOURCE OR COMMUNICATION DEVICE (INSERTED VIDE ITA 2008)

Dishonestly receives or retains – Act

any stolen computer resource or communication device –objects

Knows and dishonestly receives or having reason to believe the same to be stolen computer resource or communication device – Mens rea

three years or with fine which may extend to rupees one lakh or with both – punishment

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 C PUNISHMENT FOR IDENTITY THEFT. (INSERTED VIDE ITA 2008)

make use of – Act

electronic signature, password or any other unique identification feature of any other person–objects

fraudulently or dishonestly – Mens rea

three years or with fine which may extend to rupees one lakh or with both – punishment

Case of use of DS, Or using someone else's password

Identity theft and Email frauds, hacking

Responsibility caste on the DS owner Sec 48.

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 D PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER RESOURCE (INSERTED VIDE ITA 2008)

personation– Act

any communication device or computer resource –objects

Cheats – Mens rea

three years or with fine which may extend to rupees one lakh or with both – punishment

Email frauds, Email spoofing , facebook impersonation

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 E PUNISHMENT FOR VIOLATION OF PRIVACY. (INSERTED VIDE ITA 2008)

captures, publishes or transmits the image of a private area of any person without his or her consent, – Act

any communication device or computer resource (though not mentioned the explanation for word transmit, capture and publishing deems) –objects

intentionally or knowingly violating the privacy of that person – word (circumstances violating privacy to infer) Mens rea

three years or with fine which may extend to rupees two lakh or with both – punishment

Explanation to circumstances violating privacy

Eg Cameras in changing rooms, accessing laptop camera to take pics , taking pictures in public or private as mentioned in 66E(e)(ii)

What if consent is given? 67 and 67 B would come into play

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 F PUNISHMENT FOR CYBER TERRORISM)

Cyber terrorism is a controversial term . Crime affecting National security

The word first appeared in 1998

Broad and Narrow definitions. But agree that “Terrorism online should be considered cyberterrorism”

premeditated use, disruptive activities, against computers and/or networks

the politically motivated use of computers and information technology to cause severe disruption or widespread fear.

Use of information technology and means by terrorist groups and agents.

Mode is cyber attack

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 F PUNISHMENT FOR CYBER TERRORISM)

Specific provision dealing with cyber terrorism

Acts of terrorism cover the following:

- Denial of access
- Unauthorized access
- Introduction of virus or contaminants leading to harming persons, property and critical infrastructure
- Leading to disruption of supplies
- Sensitive data thefts
- Leading to causing injury to sovereignty and integrity of India
- Leading to causing injury to security of state
- Leading to causing friendly relations with foreign state
- Causing injury to decency and morality of a person or a state
- Defamation and incitement of offence.

CRIMINAL OFFENCES UNDER IT ACT

SEC 66 F PUNISHMENT FOR CYBER TERRORISM)

Threatens, knowingly disrupts –66(1)(A) penetrates or accesses, exceeding authorized access66 (1)(B) Commits or conspires 66(2) - mens rea

Previous slide defines all the acts

Such acts should result in

- Death or injuries to persons
- Damage or destruction to property
- Sensitive national installations
- Disruption to essential supply and services
- Affects critical information, infrastructure – Acts

Imprisonment which may extend to life

CRIMINAL OFFENCES UNDER IT ACT

SEC 67 PUNISHMENT FOR PUBLISHING OR TRANSMITTING OBSCENE MATERIAL IN ELECTRONIC FORM (AMENDED VIDE ITAA 2008)

publishes or transmits or causes to be published lascivious and obscene material – Act

"Lascivious feeling or revealing an overt sexual interest or desire" Obscene: offensive or disgusting by accepted standards of morality and decency. Filth, vulgar, X-rated, lewd etc

electronic form – object

appeals to the prurient interest, or effects to deprave and corrupt persons who read, see or hear the matter contained or embodied in it – resulting

1st conviction - three years and with fine five lakh rupees
2nd and every subsequent conviction five years and ten lakh rupees.

CRIMINAL OFFENCES UNDER IT ACT

SEC 67A PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT, ETC. IN ELECTRONIC FORM (INSERTED VIDE ITAA 2008)

publishes or transmits or causes to be published any material which contains sexually explicit act or conduct – Act
or transmitted in the electronic form – object

offline world is concerned, the law only prohibits obscenity.
online publication and transmission singled out

Sexually explicit: **sexual** content without deliberately obscuring or censoring it. Synonym for pornography

67 and 67A - does not extend in any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form – this exception is subjective

CRIMINAL OFFENCES UNDER IT ACT

SEC 67B PUNISHMENT FOR PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT, ETC. IN ELECTRONIC FORM

Its an exhaustive provision : sexually explicit

What are the various acts : publishes or transmits or causes to be published or transmitted ; creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes, cultivates, entices or induces children to online relationship, facilitates abusing children online, records own abuse or that of others pertaining to sexually explicit act with children

in the electronic form – object . Exception prescribed but still subjective

1st conviction - 5 years and with fine five lakh rupees

2nd and every subsequent conviction 7 years and ten lakh rupees.

CRIMINAL OFFENCES UNDER IT ACT

[SECTION 75] ACT TO APPLY FOR OFFENCE OR CONTRAVENTIONS COMMITTED OUTSIDE INDIA:

This provision was brought in to cover universal jurisdiction without signing relevant international treaty.

This provision is based more on the Budapest convention recognizing international best practices.

The logic behind such an implementation is that the activity of those computers outside India impacted the computers physically located in India

This provision is in consonance with the provisions of sec 3 and 4 of Indian Penal Code which deal with punishment of offences committed beyond but which by law maybe tried in India. Procedure under Sec 188 CRPC

Supreme Court judgement: A.V Mohan Rao and another Vs Kishan Rao and another (2002) 6 SCC 174

CRIMINAL OFFENCES UNDER IT ACT

[SECTION 76] CONFISCATION :

What can be confiscated?
Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto

Who can confiscate?
Under the old act it was the DSP
Under the new act it is the IP
Or any officer of Central or State Gov authorized by Central Gov

What can be done?
Search and arrest without warrant and seizure of material

CRIMINAL OFFENCES UNDER IT ACT

[SECTION 77A] COMPOUNDING OF OFFENCES :

Who can compound?
Court of competent jurisdiction

What can be compounded?
Offences for which punishment for life or imprisonment for term exceeding 3yrs has been provided

What can't be compounded?
Second conviction which is liable for enhanced punishment

Compounding provision
As in 265B and 265C of CRPC

INTERMEDIARIES

Under Information Technology Act, 2000 and Information Technology (Intermediaries guidelines) Rules, 2011.

Introduction

- Intermediaries under the old act was a network service provider.

- They facilitated data on Internet by Means of Infrastructure for means of communication.

- They are one of the three pillars being originator, addressee and Intermediary.

- The existence of the Internet would be impossible without a Intermediary.

Definition

According to section 2(1)(w) of the IT Act, "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes

Definition

a platform which facilities interaction between buyers and sellers.

Jitendra Singh Yadav vs Union Of India

Intermediaries are also persons and entities that collect sensitive personal data and information and for the purpose of storing and disseminating such information they become intermediaries.

DATA

- Defined as “data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer”

Liability of Intermediary

Liability of the Intermediary for content transmission and posting through its service was first questioned in the US courts.

The debate was they should be treated as newspapers or magazines which publish contents therefore liable for copyright infringement, defamation and other civil criminal liabilities.

OR

Be treated as telephone company which cannot be held liable for content and communication that is transmitted.

US district court of northern California first set up precedent in 1995 in the Netcom case when it held that ISP is a passive service and like telephone company cannot be held liable for content transmitted through its server.

WHY INTERMEDIARIES THAT HANDLE SENSITIVE DATA SHOULD NOT QUALIFY FOR NON LIABILITY UNDER SECTION 79 OF IT ACT

Liability of Intermediary

This exemption is not absolute and ISP has to make certain conditions like

a. ISP should not have actual knowledge that the material is illegal or infringing
b. Is not aware of the fact and circumstances of apparent posting upon actual knowledge removes or disables access to such material.
c. Must not receive a financial benefit directly that can be attributed to the usage of such illegal or Infringing country

Section 79 (2) of IT Act 2000:

Non-liability shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

SECTION 79 OF THE IT ACT

- The intent behind inserting section 79 is for providing safe harbor for intermediaries who should not held liable unreasonably.

SECTION 79(2)(a)

"the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or"

- To avail the defence of non-liability under Section 79(2)(a), the intermediary should restrict its functions to- transmitting, hosting and temporarily storing.
- But, when it comes to matrimonial sites, it is observed to be otherwise.

SECTION 79(2)(b)

"(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;"

- If the above conditions are complied with, then the intermediaries could potentially qualify for non-liability.
- Many "web-hosting services", those discussed, do implicate a sense of initiation, selection of receivers and selection or modification of the intended transmission.

SECTION 79(2)(c)

- *"the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf."*
- The intermediaries are required to observe due diligence as prescribed in the IT(intermediaries guidelines), 2011.
- The comprehensive privacy policies and terms & conditions result in notification fatigue and click-wrap agreements, which defeats the purpose of user warnings.

INTERMEDIARY GUIDELINES

- These rules may be called the Information Technology (Intermediaries guidelines) Rules, 2011.
- In exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules,

RULE 3: DUE DILIGENCE

- **Due diligence means taking reasonable measures to avoid committing an offence**
- According to rule 3: The intermediary shall observe following due diligence while discharging his duties:
- RULE 3(1): the intermediary shall publish rules and regulations, privacy policy and user agreement.
- 3(2): such regulations shall inform the users of the service to not host:

a) Belongs to another person
b) Harmful, harassing, defamatory, obscene, etc…
c) Harms minors in any manner
d) Infringes any proprietary rights such as patent, trademark, copyright.
e) violates any law for the time being in force
f) deceives or misleads the addressee about the origin of such messages
g) impersonate another person
h) contains software viruses
i) threatens the unity, integrity, defence, security or sovereignty of India

- 3(3): The intermediary shall not knowingly host or publish any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission .
- 3(4): the intermediary shall preserve information and associated records of a said crime for at least ninety days for investigation purposes.
- 3(5):The Intermediary shall inform its users that in case of non-compliance with rules and regulations, user agreement and privacy policy the intermediary has the right to immediately terminate the access
- 3(6) :The intermediary shall strictly follow the provisions of the Act or any other laws for the time being in force.
- 3(7): When required by lawful order, the intermediary shall provide information or any such assistance to Government Agencies who are lawfully authorised
- 3(8): The intermediary shall take all reasonable measures to secure its computer resource
- 3(9): The intermediary shall report cyber security incidents
- 3(10):The intermediary shall not knowingly deploy or install or modify the technical configuration of computer resource or become party to any such act
- 3(11): The intermediary shall publish on its website the name of the Grievance Officer and his contact details.

PROVISIONS UNDER IT ACT

- Sec 67C – retention of information as per prescription of Central Govt.