

CYBER CRIMES

Understanding the Landscape

DR. NAGARATHNA. A

CO-DIRECTOR

ADVANCED CENTRE ON CYBER LAW & FORENSICS,

ASSOCIATE PROFESSOR OF LAW

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY, BANGALORE

INTRODUCTION

- Increasing reliance on technology - especially computer, Internet - in day to day life
- **Developing law and legal principles.**

- Today, crime is no longer limited to space, time or a group of people.
- New technology – has given a new way to express criminal tendencies.

CYBER CRIMES

VARIOUS FORMS OF CYBER CRIMES

- NOVEL WAYS
 - NOVEL NAMES
-
- HENCE – LAW IS A COMBINATION OF BOTH NEW ONES AS WELL AS TRADITIONAL ONES.....

Traditional crimes on Computers

- Fraud – Forgery
- Counterfeiting
- new mischief's – like – computer hacking and deliberate erasure of programs / data.

•Defamation

—

•Harassment & Intimidation.

- Cyber Stalking.
- Criminal Intimidation u/s. 503 IPC
- S. 354D IPC

INDIAN CYBER CRIME LAW

INFORMATION TECHNOLOGY ACT, 2000

Seeks to provide legal framework for

- recognition of **electronic contracts**,
- promotion of **electronic governance** and
- also provides for the legalization of **digital signature**.
- +
- prevention of **computer crimes**.

Impact of I T Act, 2000

Amendments to –

- Indian Evidence Act
- Indian Penal Code
- Bankers Books Evidence Act
- RBI Act

LAWS:

CYBER CRIMES
UNDER

INFORMATION TECHNOLOGY ACT, 2000

WITH 2008 AMENDMENT

Chapter XI of the IT ACT deals
with cyber crimes

- **65. Tampering with Computer Source Documents**

- Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
- Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

Sec 66. Computer Related Offences

- ***If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.***

Explanation:

- For the purpose of this section,-
- a) the word "**dishonestly**" shall have the meaning assigned to it in section 24 of the Indian Penal Code;
- b) the word "**fraudulently**" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

- Act u/s. 43 + dishonest/fraudulent = 66

- **43. Penalty for damage to computer, computer system, etc.-**
- If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network –
 - a) accesses or secures access to such computer, computer system or computer network or computer resource
 - b) downloads, copies or extracts any data, computer data base information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.

c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) damages or causes to be damaged and computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

e) disrupts or causes disruption of any computer, computer system or computer network;

f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

.....CONTINUED....

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or compute network

- i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.**

- j) steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.**

HE SHALL BE LIABLE TO PAY DAMAGES BY WAY OF COMPENSATION TO THE PERSON SO AFFECTED.

66 A Punishment for sending offensive messages through communication service, etc –

Any person who sends, by means of a computer resource or a communication device,-

a)any information that is grossly offensive or has menacing character; /

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

- **Shreya Singhal v. UOI**
- **S. 66A – violation of fundamental right to freedom of speech and expression.
[19(1)(a)]**

- **66 B. Punishment for dishonestly receiving stolen computer resource or communication device**

- **Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.**

- **66-C Punishment for identity theft**

- Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

- **66D Punishment for cheating by personation by using computer resource**
- Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

66E Punishment for violation of privacy –

- Whoever, intentionally or knowingly
 - captures, publishes or transmits
 - the image of a private area of any person
 - without his or her consent,
 - under circumstances violating the privacy of that person,
- = shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Explanation.- For the purposes of this section--

(a) “transmit” means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) “capture”, with respect to an image, means to videotape, photograph, film or record by any means;

(c) “private area” means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) “publishes” means reproduction in the printed or electronic form and making it available for public;

(e) “under circumstances violating privacy” means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

66F. Punishment for cyber terrorism:

1) Whoever,-

(A) with intent to threaten the unity, integrity, security/sovereignty of India/to strike terror in the people or any section of the people by –

(i) denying /cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate/access a computer resource without authorization/exceeding authorized access; or

(iii) introducing/causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to/destruction of property or disrupts or knowing that it is likely to cause damage/disruption of supplies/services essential to the life of the community or adversely affect the critical information infrastructure specified u/s. 70, or

(B) knowingly/intentionally - penetrates or accesses a computer resource without authorisation or exceeding authorized access,

- and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations;
- or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to
 - the interests of the sovereignty and integrity of India,
 - the security of the State,
 - friendly relations with foreign States,
 - public order, decency or morality, or
 - in relation to contempt of court, defamation or
 - incitement to an offence, or
 - to the advantage of any foreign nation, group of individuals or otherwise,
- commits the offence of cyber terrorism.

- 2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Sec 70 Protected system

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation: For the purposes of this section, "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which , shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1)

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

- **67. Punishment for publishing or transmitting obscene material in electronic form**

- Whoever publishes or transmits or causes to be published
- in the electronic form,
- any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it,

.....CONTINUED...

= shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and

= in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

[earlier punishment = term not exceeding 3 years and fine not exceeding 2 lakh rupees or both]

- **67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form**
- Whoever publishes or transmits or causes to be published or transmitted
- in the electronic form
- any material which contains sexually explicit act or conduct

= shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and

= in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception:

- This section [67A] and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
- (i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or
- (ii) which is kept or used bona fide for religious purposes.

67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever,-

- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or
- (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or
- (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or
- (d) facilitates abusing children online or
- (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

....continued.....

= shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and

= in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

- Provided that the provisions of section 67, section 67A and this section [67B] does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-
- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or
- (ii) which is kept or used for bonafide heritage or religious purposes

Explanation:

For the purposes of this section, "children" means a person who has not completed the age of 18 years.

- **THE PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT, 2012**

Offences By Companies

Sec 85 Offences by Companies.

(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

- continued.....

.....continued.....

(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation – For the purposes of this section

(i)"Company" means any Body Corporate and includes a Firm or other Association of individuals; and

(ii)"Director", in relation to a firm, means a partner in the firm

- **Sec 84 B Punishment for abetment of offences**

- Whoever abets any offence shall,
- if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.
- **Explanation:** An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

Sec 84 C Punishment for attempt to commit offences:

- Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed,

and in such an attempt does any act towards the commission of the offence, shall,

= where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

Sec 79 Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) 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

(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

.....CONTINUED.....

- (3) The provisions of sub-section (1) shall not apply if-
- (a) the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act.
 - (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

- Most of the offences under the Act are –

-COGNIZABLE

-BAILABLE

-COMPOUNDABLE

.... Any
Questions ?..

Thank you.