International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 01-06-2019; Accepted: 04-07-2019
www.lawjournals.org
Volume 5; Issue 5; September 2019; Page No. 25-28

A study on Cyber crimes in India (With reference to information technology act 2000)

Satish Kumar Ganta
Research Scholar, KLU College of Law, KL University, Andhra Pradesh, India

Abstract
The aim of this paper is to present the Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities.

Keywords: phenomenon, diffusion, digitization, ordinary

Introduction

Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Kautilya's Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it. Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile.

Snatching some one's mobile will tantamount to dumping one in solitary confinement!

Cyber Crime is not defined in Information Technology Act 2000 [6] nor in the I.T. Amendment Act 2008 nor in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber-crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber-crime'. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber-crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber-crime.

Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet the Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

Criminal Liabilities under Information Technology Act, 2000

- Sec.65: Tampering with Computer source document
- Sec.66: Hacking with Computer systems, Data alteration and other computer related Offences
- Sec. 66A: Punishment for sending offensive messages through communication service etc.
- Sec. 66B: Punishment f or dishonestly receiving stolen computer resource or communication device
- Sec. 66C: Punishment for identity theft
- Sec. 66D: Punishment for Cheating by personating by using computer resource
- Sec. 66E: Punishment for Violation of Privacy
- Sec. 66F: Punishment for Cyber Terrorism
- Sec.67: Publishing obscene information
- Sec. 67A: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form
- Sec. 67B: Punishment for Child Pornography
- Sec. 67C: Preservation and Retention of Information by Intermediaries
- Sec.70: Un-authorized access to protected system
- Sec. 70A: National Nodal Agency
- Sec. 70B: CERT-in
- Sec. 71: Penalty for Misrepresentation
- Sec.72: Breach of Conf identiality and Privacy
- Sec.73: Publishing false digital signature certificates
- Sec. 74: Publication for fraudulent purposes

Sect ion 65
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.

Sect ion 66
If any person, dishonestly or fraudulently, does any act referred to in sect ion 43, he shall be punishable with imprisonment for a term which may extend to three years or with f ine which may extend to five lakh rupees or with both.

66A: Punishment f or sending offensive messages through communication service, etc.— Any person who sends, by mean s of a computer resource or a communication device,— (a) any information that is grossly offensive or has meaning character, or (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, persistent ly by making use of such computer resource or a communication device; or (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 message, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Sect ion 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 convict ion 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 convict ion with imprisonment of either descript ion for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B
Punishment for publishing or transmitting of material depict ing children in sexually explicit act, etc. in electronic form:
Whoever,-

a. Publishes or transmits or causes to be published or transmit ted 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 of fend 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, shall be punished on first convict ion with imprisonment of either descript ion for a term which may extend to five years and with a f ine which may extend to ten lakh rupees and in the event of second or subsequent convict ion with imprisonment of either description for a term which may extend to seven years and also with fine
f. which may extend to ten lakh rupees: Provided that the provisions of sect ion 67, sect ion 67A and this sect ion does not extend to any book, pamphlet, paper, writing, drawing, paint ing, representation or igure in electronic form-
g. 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
h. Which is kept or used for bonafide heritage or religious purposes

Section 69: Powers to issue direct ions for intercept ion or monitoring or decrypt ion of any information through any computer resource:

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or
expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable of fence relating to above or for investigation of any offence, it may, subject to the provisions of subsection (2), for reasons to be recorded in writ ing, by
Order, direct any agency of the appropriate Government to intercept, moni t or or decrypt or cause to be intercepted or monitored or decrypted any information transmit ted received or stored through any computer resource.
(2) The Procedure and safeguards subject to which such intercept ion or monitoring or decrypt ion may be carried out, shall be such as may be prescribed

Sect ion 71: Penalty for misrepresentation
Whoever makes any misrepresentation to, or suppresses any material fact from, the Cont roller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.
Penalties:
Punishment: imprisonment which may extend to two years
Fine: may extend to one lakh rupees or with both.

Section 72
Penalty for breach of confidentiality and privacy Save as

otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conf erred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

Penalties

Punishment: term which may extend to two years.

Fine: one lakh rupees or with both.

Section 72A

Punishment for Disclosure of information in breach of lawful contract. Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Sect ion 73

Penalty for publishing electronic Signature Certificate false in certain particulars:

No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that

- the Certifying Authority listed in the certificate has not issued it ; or
- the subscriber listed in the certificate has not accepted it; or
- The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

Section 74

Publication for fraudulent purpose: Whoever knowingly creates, publishes or otherwise makes available a Electronic Signature Certiticate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or With fine which may extend to one lakh rupees, or with both.

Section 75

Act to apply for offence or contraventions commit ted outside India Subject to the provisions of sub-sect ion (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Cyber crimes under IPC and special laws

The Indian Penal Code, 1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many a times since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied

Upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well.

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sect ions dealing with false entry in a record or false document etc. (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc.) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and elect ronic documents has been treated just like physical records and documents during commission of acts of forgery or falsificat ion of physical records in a crime. After the above amendment, the investigating agencies f ile the cases/ charge-sheet quoting the relevant sect ions from IPC under sect ion 463, 464, 468 and 469 read with the ITA/ITAA under Sect ions 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.

Sending threatening messages by email - Sec 503 IPC

- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

Conclusion

India must ensure techno legal measures to regulate Indian cyberspace. Similarly, regulations and guidelines for effective investigation of cyber-crimes in India is also need of the hour. The Indian Government has assured in the year 2014 that the IT Act, 2000 could be amended to accommodate e-commerce concerns. The technological development has given rise to a cyber-world constituting cyber space. Cyber space is witnessing considerable advancement with the rapid increase in the information technology. It is always hard to determine or predict something in the future in an accurate manner. There is a possibility to consolidate the technological advancements in the past. The internet users are increasing tremendously every year and at the same time there is also rise in the number of people using mobiles and smart phones.

References

1. Audit of Fraud, Fraud Detect ion Technique& Forensic Audit, Case Study on Cyber Crimes. Indian Audit & Accounts Departments; (unpublished).
2. Barkha U. Ram Mohan, Cyber Laws and Crimes, 3rd Edit ion, Delhi Law House.
3. Basha KN. Seminar. Workshop on Detect ion of Cyber Crime and Invest igat ion," (unpublished).
4. Boateng, Amanor. Phishing, Smishing & Vishing: An Assessment of Threats against Mobile Devices. 2014; 5:297-307.
5. Bramhe Manoj. SMS Based Secure Mobile Banking. 2011; 3:472-479.
6. Common Cyber Crimes and Government Laws and Rules in Information Security" Unit 3, Information Technology Act, 2000.

7. Crime in India: 2011-Compendium National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India CSIS Securing Cyberspace for the 44th Presidency, CSIS Commission on Cyber security, US Center for Strategic and, 2012.