P: ISSN NO.: 2394-0344 RNI No.UPBIL/2016/67980 VOL-4* ISSUE-2* (Part-1) May- 2019
E: ISSN NO.: 2455-0817 *Remarking An Analisation*

Legislative Measures for Protection from Cyber Crimes: An Overview

Priyanka Goswami
Guest Faculty,
Faculty of Law,
J. N. V. University,
Jodhpur, Rajasthan, India

Abstract

Illegal use of computer leads to cyber crime. Cyber crime has become the most potential damaging threat to IT related activities. To overcome cyber crime, India enacted the Information Technology Act, 2000, which was amended in 2008 providing more powerful Law. Consequently many other Acts like the Indian Penal Code, 1860, the Indian Evidence Act, 1872, Banker's Books Evidence Act, 1851 were amended. The amended Indian Evidence Act, 1872 recognizes admissibility of Electronic Records. The Banker's Books Evidence Act, 1851 as amended, treats the printout data as a valid document. The Law making machinery should keep in view the magnitude of crimes done by fraudsters.

Keywords: Cyber, Legislative, Information Technology, Evidence.

Introduction

Computer technology makes the human life easier and comfortable. It enhances accuracy, speed and efficiencies of the life of the human beings. Crime adversely affects the members of the society and hampers the development of a country. Illegal use of the computer leads to cyber crime. To overcome cyber crime, India enacted the Information Technology Act, 2000 which was amended vide the Information Technology (Amendment Act),2008 providing more powerful law. Cyber crime is caused from the misuse of the information technology for unauthorized or illegal access, electronic fraud; like alteration, interception, concealment, deletion of data, forgery etc..Cyber crime has become an international crime as it has affected the global community. Cyber crime has become the most potential damaging threat to IT- related activities and transactions. Nowadays, internet is used almost everywhere like in home, shop, office, railway station, college, etc..The internet is misused by hackers and organised criminals. The growth of cyber crime is increasing proportionately to the internet explosion.

Review of Literature

There is no literature available in a consolidated form of legislative measures provided under various enactments to prevent cyber crimes.

Necessity of Measures against Cyber Crimes

In order to detect and prevent cyber threat, the industries are developing a range of products for use in the home and the business. for e.g., intrusion detection systems, antivirus software etc..Despite all the preventive steps, we are not able to get rid of cyber crime. The internet has become an integral part of everyone's life. Unfortunately, computer crime in rampant as the side effect of the excessive use computers and internet despite taking many counter measures. In the modern cyber technology world, it is very necessary to regulate cyber crimes and for it cyber law should be made stricter in the case of cyber hackers.

Enactment of the Information Technology Act

The Information Technology Act, 2000

The ITAct-2000 defines 'Computer' as any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. The word 'computer' has been widely defined that it includes any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities..

The technology, used by the computer experts to prevent the hackers, has often been misused by the hackers necessitating enactment

of strict statutory laws to regulate the criminal activities in the cyber world. Therefore, the Information Technology Act, 2000 (ITAct- 2000) was enacted by the Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as to provide for penalties and punishments in the field of cyber crimes

Aim of the Study

This paper focuses on the legislative measures for the protection from cyber crime in India

The Information Technology (Amendment) Act, 2008

The Information Technology Act, 2000 was further amended by the Information Technology (Amendment) Act, 2008 (ITAAct-2008). The scope and applicability of ITAct-2000 was increased by its amendment in 2008. The term 'communication devices' was inserted in the definition, to include into its coverage cell phones, personal digital assistance or such other devices used to transmit any text, video etc. like those which were later being marketed as iPad or other similar devices on Wi-fi and cellular models. Though the ITAct- 2000 defined 'digital signature', the said definition was incapable to cater to needs of the hour and therefore, the term 'Electronic signature' was introduced and defined in the ITAAct - 2008 as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures not confining the recognition to digital signature process alone.

Punishment for damage to computer system and hacking

According to Section: 43 of ' the Information Technology Act, 2000' whoever does any act or destroys, deletes, alters and disrupts or causes disruption of any computer with the intention of damaging of the whole data of the computer system without the permission of the owner of the computer, shall be liable to pay fine upto 1crore to the person so affected by way of remedy. According to Section 43A which is inserted by 'the Information Technology (Amendment) Act, 2008' provides that where a body corporate is maintaining and protecting the data of the persons as provided by the Central Government, if there is any negligent act or failure in protecting the data/ information, then a body corporate shall be liable to pay compensation to the person so affected. Section 66 deals with 'hacking with computer system' and provides for imprisonment up to 3 years or with fine, which may extend up to 2 lakh rupees or with both.

The new amendment has replaced Section 43 by Section 66. The word "hacking" used in Section 66 of earlier Act of 2000 was removed and named as "data theft" and consequently widened in the form of Sections 66A to 66F. The section covers the offences such as the sending of offensive messages through communication service, misleading the recipient of the origin of such messages, dishonestly receiving stolen computers or other communication device, stealing electronic signature or identity such as using another person's password or electronic signature, cheating by personation through computer resource or a communication device, publicly publishing the information about any person's location without prior permission or consent, cyber terrorism, the acts of access to a commuter resource without authorization, such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. The offences covered under Section 66 are cognizable and non-bailable. It may be pointed here that the consequence of Section 43 of earlier Act was civil in nature having its remedy in the form of damages and compensation only. Under Section 66 of the Amendment Act, 2008 if an act is done with mens rea i.e. criminal intention, it will attract criminal liability resulting in imprisonment or fine or both.

The law of defamation under Section 499 got extended to "Speech" and "Documents" in electronic form with the enactment of the Information Technology Act, 2000.

Section 66A of the Information Technology Act, 2000: Section 66A of the IT Act says that any person who sends, by means of a computer resource or a communication device any information that is grossly offensive or has menacing character; or any content 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 makes by making use of such computer resource or a communication device, or 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.

Section 66A of the Information Act, 2000 does not specifically deal with the offence of cyber defamation but it makes punishable the act of sending grossly offensive material for causing insult, injury or criminal intimidation.

Effect of Information Technology Act on Other acts

The Indian Penal Code, 1860: A number of sections of the Indian Penal Code were amended by the Information Technology Act, 2000 and its amendment in 2008 by inserting the word 'electronic record' thereby treating the electronic records and documents at par with physical records and documents. The word digital signature was substituted by electronic signature. The sections of IPC dealing with false entry in a record or false document etc (e.g. Section 192, 204, 463, 464, 468 to 470, 471, 474 etc.) were amended as 'electronic record and electronic document'. Now, electronic record and electronic documents have been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC read with the IT Act/ITA Act under Sections 43 and 66 in like offences to

ensure that the evidence and/or punishment can be covered and proved under either of these or under both legislations. Mainly Sections 463 to 471 of the Indian Penal Code,1860 deal with the offences relating to forgery and forged documents. The Indian Penal Code contains following important provisions to combat the menace of cyber crime.

Section 463 of IPC: Forgery

Whoever makes any false documents or false electronic record or part of a document or electronic record, with the intent to cause damage or injury, to the public or to any person or to support claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery. In Section 463, for the words " whoever makes any false document or part of a document with intent to cause damage or injury", the words "whoever makes any false document or false electronic record with intent to cause damage or injury" were substituted vide the Information Technology Act, 2000. Thus, whoever dishonestly or fraudulently makes a false document or false electronic record in order it may be used as genuine commits forgery. Section 465 prescribes punishment for forgery which may extend to 2 years of imprisonment of either description, or fine, or both.

Section 469 of IPC: Forgery for purpose of Harming Reputation

Whoever commits forgery, intending that the document or electronic document forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine. This section deals with forgery of a document or electronic record for the purpose of harming the reputation of a man. The word 'harm' means hurt, injury, damage etc..The phrase "intending that the document or electronic record forged" was substituted for the existing phrase "intending that the document forged " vide the Information and Technology Act, 2000. The offence is cognizable, bailable, non-compoundable and triable by a Magistrate of First class. It may be observed here that cognizable offence means an offence for which a police officer may arrest without warrant. A warrant case means a case relating to an offence which is punishable with death, imprisonment for life or imprisonment for a term exceeding 2 years . A bailable offence means an offence which is shown as bailable in the First Schedule appended to the Code of Criminal Procedure, 1973 or which is shown bailable under any other law and non-bailable offence means any other offence.

Section 470 of IPC: Forged document or Electronic Record

A false document or electronic record made wholly or in part by forgery is designated a forged document or electronic record. The word 'document or electronic record' was substituted for the word document vide the Information Technology Act, 2000.

Section 499 of IPC: Defamation

Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases excepted, to defame that person. There are 4 explanations to cyber defamation to the effect that it may amount to defamation if the imputation (i) is hurtful to the feelings of family or other near relatives, (ii) concerns a company, or an association of persons as such, (iii) ironically made , and (iv) in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person.

The expression 'harm' used in Section 499 means harm to the reputation of the aggrieved party. The meaning of the word 'harm' is not in the ordinary sense in which it is used. By harm is meant imputation on a man's character made and expressed to others so as to lower him in their estimation. Anything which lowers him merely in his own estimation does not constitute defamation. Character is what a person actually is while reputation is what others say that he is. A man's opinion of himself cannot be called his reputation. A man has no reputation in himself and therefore, communication of defamatory matter to the person defamed is not publication.

There are, however, 10 exceptions to the above law of defamation as stated infra:

1. Imputation of truth required to be made or published in public good.
1. 2. Expression of opinion in good faith respecting the conduct of public servants.
2. Expression of opinion in good faith respecting the conduct of any person touching any public question and respecting his character.
3. Publication of reports of proceedings of court.
4. Expression of opinion in good faith respecting merits of any case, civil or criminal decided in court or conduct of witness and others concerned.
5. Expression of opinion in good faith respecting merits of public performance.
6. Censure passed in good faith by person having lawful authority over another.
7. Accusation against any person in good faith to authorised person
8. Imputation in good faith by person for protection of his or other's interest.
9. Caution intended for good of person to whom conveyed or for public good.

These 10 exceptions are based on the ground of truth, good faith or public interest, and strike a balance between freedom of speech and expression guaranteed under Article 19(1) (a) of the Constitution of India and the individual's rights to reputation. The burden of proof of the Exception is on the accused.

The Indian Evidence Act, 1872

Prior to enactment of IT Act, all evidences in a court were in the physical form only. After existence of IT Act, the electronic records and documents were

recognized. The definition part of the Indian Evidence Act, 1872 was amended as "all documents including electronic records". Other words e.g., 'digital signature', 'electronic form', 'secure electronic record' 'information' as used in the IT Act, were also inserted to make them part of the evidentiary importance under the Indian Evidence Act. The important amendment was seen by recognition of admissibility of electronic records as evidence as enshrined in Section 65B of the IT Act.

The Bankers' Books Evidence Act, 1891

Before passing of IT Act, a bank was supposed to produce the original ledger or other physical register or document during evidence before a court. After enactment of IT Act, the definition part of the Bankers' Books Evidence Act stood amended as: "bankers' books" include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device. When the books consist of printouts of data stored in a floppy, disc, tape etc., a printout of such entry is a valid document if it is certified in accordance with the provisions of Section 2A to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure that data are entered or any other operation performed only by authorized persons; the safeguards adopted to prevent and detect unauthorized change of data and the safeguards available to retrieve data that are lost due to systemic failure or any other reasons.

The above amendment in the provisions in Bankers' Books Evidence Act recognized the printout from a computer system and other electronic document as a valid document during course of evidence, provided such printout or electronic document is accompanied by a certificate in terms as mentioned above.

Matters Not Addressed Under Information and Technology Act

It is submitted that IT Act and ITA Act are though landmark first steps and became mile-stone in the technological growth of the nation; however the existing law is not sufficient. Many issues in cyber crime and many crimes are still left uncovered. Territorial Jurisdiction is a major issue which is not satisfactorily addressed in the IT Act or ITA Act. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cyber crime etc.. Cyber crimes are basically computer based crimes and therefore, if the mail of someone is hacked in one place by accused sitting far in another State, determination of concerned police station, who will take cognizance is difficult. It is seen that the investigators generally try to avoid accepting such complaints on the ground of jurisdiction. Since the cyber crime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdiction; it is necessary that proper training should be given to all persons concerned.

However, most of the cyber crimes in the nation are still brought under the relevant sections of IPC read with the comparative sections of IT Act or the ITA Act which enable the investigating agencies that even if the IT Act part of the case is lost, the accused cannot escape from the IPC part.

Conclusion

Society is happening more and more dependent upon technology and crimes based on electronic offences are bound to increase. Cyber crime is rampant and is increasing exponentially as the side effect of the excessive use and misuse of computers and internet. Crime is a great hurdle in the development of a country and adversely affects the members of the society and lowers down the economic growth of the country. The Information Technology Act is a great savoir to combat cyber crime. This Act is a special Act to tackle the problem of cyber crime though offences relating to computer also fall under the Indian Penal Code and other legislation in India. The Information Technology Act amended the Indian Evidence Act, 1872 recognising admissibility of electronic records as evidence. The Act also amended the Bankers' Books Evidence Act, 1891 by treating the printout of data as a valid document if it is accompanied by the prescribed certificate under the Act. There is under reporting of cyber crimes in the country. Cyber crime is committed almost every day but only some of them get reported. The cyber crime cases reaching the court of law are, therefore, very few. There are difficulties in collecting, storing and appreciating digital evidence. The Act has a long way to go and promise to keep off the victims of cyber crimes. Endeavour of law making machinery of the nation should be made keeping in view the magnitude of crimes done by the fraudsters, to keep the crimes lowest. Hence, it should be the persistent efforts of rulers and law makers to ensure that governing laws of technology contain every aspect and issues of cyber crime and further grow in continuous and healthy manner to keep constant vigil and check over the related crimes.

References

Gaur,K. D.,Text book on Indian Penal Code, Universal Law Publishing Company Pvt. Limited, New Delhi,
Fifth edition, 2014.
The Information Technology Act, 2000
The Information Technology (Amendment) Act, 2008
The Code of Criminal Procedure, 1973
The Constitution of India
The Indian Evidence Act, 1872
The Bankers' Books Evidence Act, 1891