International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 9, Number 1 (2017), pp. 1-11

http://www.irphouse.com

Cyber Security: A Legal Perspective

Dr. Sudhir Kumar Sharma

B.E., M.Tech.(CSE), Ph.D., Lecturer,
Department of Computer Science & Engineering,
Government Polytechnic College, Jodhpur(Rajasthan)

Abstract

Computer technology provides a boost to the human life and adds accuracy, speed and efficiency. Computer crime is a great hurdle in the development of a country. The rapid growth of cyber crime makes cyber security as an unavoidable part of our lives. Normally a person is concerned with the tools and technologies used to prevent cyber crime. This paper emphasises on legal response to cyber security and focuses on the importance of law against cyber crime for achieving the cyber security in an indirect manner.

Keywords: Cyber crime, cyber security, information and communication technologies, hacking etc.

1. INTRODUCTION

Nowadays, the term cyber crime is well known and needs no introduction. Crime is a great hurdle in the development of a country. It adversely affects the members of the society and lowers down the economic growth of the country. Computer technology provides a boost to the human life and makes it easier and comfortable. It adds accuracy, speed and efficiency to the life of human being. But a computer is exploited by the criminals and its illegal use leads to cyber crime. To combat cyber crime, India enacted the Information Technology Act,2000 which was drastically amended in the year 2008 providing more powerful and stringent law.

Cyber crime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc.. Cyber crime is an international crime as it has been affected by the global revolution in information and communication technologies (ICTs). It has affected the global community. It would be unlawful act where the

computer is either a tool or a target or both. Continuous attempts have been made to specify different types of cybercrime, their detection and preventive methods.

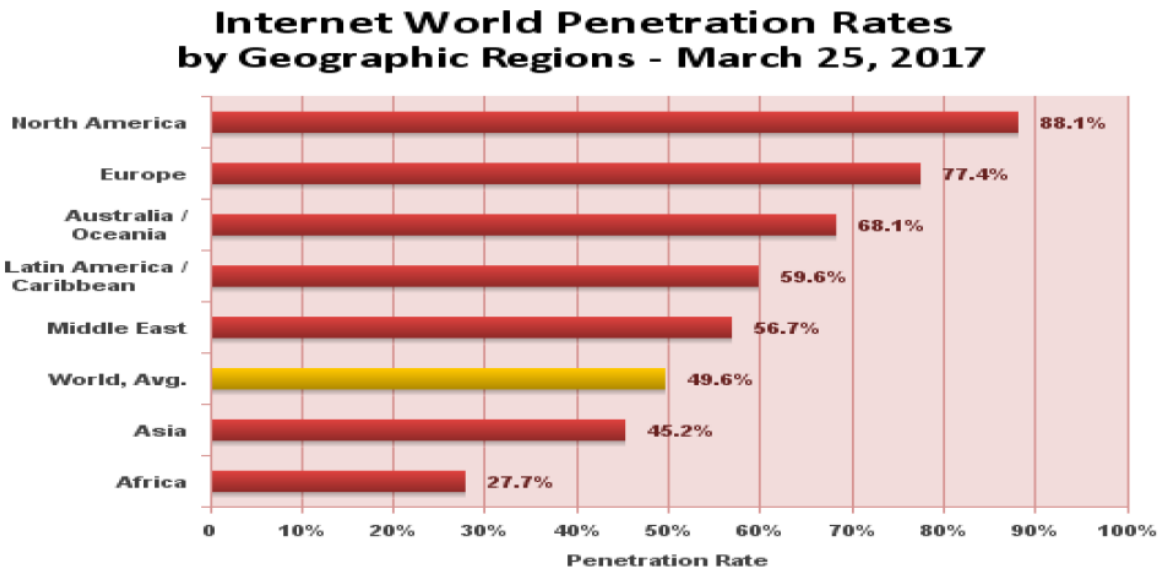
Cyber crimes have become the most potentially damaging threat to IT-related activities, transactions, and assets. Unfortunately, some organizations do not seem to be much alert to detect, address, or protect themselves from these threats.

2. WORLDWIDE CYBER SECURITY PROBLEM

The internet has become an integral part of everyone's life. It has also given new dimensions to our economic and social life. But at the same time we cannot be oblivious of the negative side of use of computers and internet. It is very unfortunate that computer crime is rampant and is increasing exponentially as the side effect of the excessive use of computers and internet.

The internet security problem is immensely growing and cyber crimes are continuously increasing even though we are using many countermeasures.

The following figures would reveal the worldwide penetration percentage of cyber crimes.



Source: Internet World Stats-www.internetworldstats.com/stats.htm

Penetration Rates are based on a world population of 7,519,028,970 and 3,731,973,423 estimated Internet Users on March 31,2017

Figure- Worldwide Penetration Percentage

From the above graph it is very evident that almost in the every region of the world the penetration rate is very high which warrants to take steps for cyber security. Many tools and techniques have been used regularly by the computer experts for achieving the cyber security. Cyber security plays an important role in age of information technology and internet services.

In the early ages the people were trying to use new tools and technologies for cyber security. But they realized that law could also be helpful to achieve cyber security.

3. NEED FOR CYBER LAW

Today, it cannot be overemphasized that billions of users are using internet. The internet is used almost everywhere like in home, shop, office, railway station, college etc. by the users. The internet and our economies have also become interwoven. The internet generates both wealth and employment.

Unfortunately, the internet is misused by hackers and organised criminals. The growth of cyber crime is increasing proportionately to the internet explosion. Cyber crime is expanding parallel with the growing number of internet users. The internet is open to the public and the internet users are at risk and targeted for mental harassment, financial gain through malware and social evil purposes. Therefore, for detection and prevention of such cyber threat, the industries are developing a range of products for use in the home and the business, for example, intrusion detection systems, firewalls, antivirus software etc.. Despite all the preventive steps, we are not able to get rid of cyber crime. The internet security problem is immensely growing and cyber crime continues to thrive even though we are using many countermeasures.

Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world, it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers.

4. LEGISLATIVE MEASURES FOR PREVENTION OF CYBER CRIMES

4.1 Statutory Provisions Governing Cyber Defamation In India

4.1.1 The Indian Penal Code, 1860

The Indian Penal Code, 1860 contains provisions dealing with the menace of cyber defamation.

(1) 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 to defame that person. However, there are 10 exceptions viz., imputation of truth

required to be made or published in public good, expression of public conduct of public servants in good faith, expression of conduct of any person touching any public question in good faith, publication of reports of proceedings of Courts, expression of opinion respecting merits of case decided in Court or conduct of witness and others concerned in good faith, expression of opinion respecting merits of public performance in good faith, censure passed in good faith by person having lawful authority over another, accusation preferred in good faith against any person by authorized person, imputation on the character of another made in good faith by person for protection of the interest of the person making it or of any other person, or for the public good, caution intended for good of person to whom conveyed or for public good. The 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 expression 'harm' used in Section 499 means harm to the reputation of the aggrieved party. No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, 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 harm to reputation of the person is made with necessary *mens rea* (guilty mind). The offence of defamation is punishable under Section 500 of IPC with a simple imprisonment up to 2 years or fine or both.

(2) 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.

The phrase "intending that the document forged" under Section 469 was replaced by the phrase "intending that the document or electronic record forged" vide the Information and Technology Act, 2000. The offence is cognizable, bailable, non-compoundable. It is worthwhile to mention 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 Code of Criminals Procedure, 1973 or which is made bailable by any other law and non-bailable offence means any other offence.

(3) 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 Information Technology Act, 2000.

(4) Section 503 of IPC. **Criminal intimidation.** Whoever, threatens another with any injury to his person, reputation or property, or to the person or reputation of any one in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threats, commits criminal intimidation. Section 503 of IPC covers the offence of criminal intimidation by use of e-mails and other electronic means of communication for threatening or intimidating any person or his property or reputation. It is punishable with imprisonment for a term which may extend to 2 years, or fine, or both under section 504. The offence is non-cognizable, bailable and compundable.

4.1.2 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, arithmetic, 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' and 'computer system' have been so widely defined and therefore, any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

The Information Technology Act, 2000 (ITAct- 2000) was enacted by 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. The above Act was further amended by the Information Technology (Amendment) Act, 2008 (ITAAct-2008). The word '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. ITAct- 2000 defined 'digital signature', but 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.

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

(i) any information that is grossly offensive or has menacing character; or

(ii) 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

(iii) 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.

4.2 Jurisdiction and Procedure

4.2.1 Adjudication: Adjudication powers and procedures have also been dealt with in Section 46 and others. As embodied in the Act, the Central Government may appoint any officer not below the rank of a director to the Government of India or a State Government as the adjudicator. The I.T. Secretary in any State is normally the nominated adjudicator for all civil offences arising out of data thefts and resultant losses in the particular State. It has been observed that a very few applications were received during first 10 years of enactment of the ITAct, that too in the major metros cities only. However, the trend of receiving complaints under ITAct is rapidly growing. The first adjudication obtained under this provision was in Chennai in a case involving ICICI Bank in which the bank was told to compensate the applicant with the amount wrongfully debited in Internet Banking, along with cost and damages. There is also an appellate procedure under this process and the composition of Cyber Appellate Tribunal at the national level has also been described in the Act. Every

adjudicating officer has the powers of a civil court and the Cyber Appellate Tribunal has the powers vested in a civil court under the Code of Civil Procedure, 1973.

4.2.2 Where to lodge a complaint: A person aggrieved of the offence of of cyber defamation can make a complaint to the Cyber Crime Investigation Cell. The Cyber Crime Investigation Cell is a branch of the Criminal Investigation Department (CID). Cyber Crime Investigation Cells have been opened up in many cities like Delhi, Mumbai, Chandigarh, Hyderabad, Bangalore, Gurgaon, Pune, Lucknow, etc. The Cyber Crime Investigation Cells deal with offences related to the computer, computer network, computer resource, computer systems, computer devices and internet. CID has power to look into other high-tech crimes.

4.2.3 Punishment for damage to computer system and hacking: According to Section: 43 of '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. Section 43A which is inserted by '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, 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.

5. AMENDMENT OF MAJOR ACTS AFTER ITACT,2000

5.1 The Indian Penal Code, 1860. A number of sections of the Indian Penal Code were amended by inserting the word 'electronic record' thereby treating the electronic records and documents on a par with physical records and documents. The sections of IPC dealing with false entry in a record or false document etc (e.g. Section 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc.) have since been 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-sheets quoting the relevant sections from IPC under Section 463,464, 468 and 469 read with the ITAct/ITAAct 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.

5.2 The Indian Evidence Act, 1872. Prior to enactment of ITAct, all evidences in a court were in the physical form only. After enactment of ITAct, the electronic records

and documents were recognized. The definition part of 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 ITAct, 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 ITAct.

5.3 The Bankers' Books Evidence Act, 1891. Before passing of ITAct, a bank was supposed to produce the original ledger or other physical register or document during evidence before a court. After enactment of ITAct, 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 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.

6. JUDICIAL TRENDS ABOUT OFFENCE OF CYBER DEFAMATION

In the first case of cyber defamation in India, ***SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra***,[1] the reputation of a corporate was being defamed by an employee of the plaintiff company by sending derogatory, defamatory, obscene, e-mails obscene, vulgar, filthy and abusive e-mails to its employers and also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The Hon'ble Delhi High Court passed an ex-prate ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive e-mails either to the plaintiffs or to sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing Departments. Further, the Hon'ble Court also restrained the defendant from publishing, transmitting or causing to be published any

[1]. CS(OS) No. 1279/2001 (Delhi High Court, 2001)

information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiff.

In another case ***State of Tamil Nadu v. Suhas Katti,***[2] related to posting of obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on a complaint made by the victim in February 2004, the Police traced that the accused was in Mumbai and arrested him within the next few days. Relying on the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners, the Additional Chief Metropolitan Magistrate held the accused guilty of offences under Section 469, 509 of IPC and 67 of IT Act, 2000 and the accused was convicted and sentenced for the offence to undergo rigorous imprisonment (RI) for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence under section (u/s) 509 IPC sentenced to undergo 1 year simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment (RI) for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.

In the case of ***Tata Sons v. Turtle International,***[3] the Delhi High Court held that publication is a comprehensive term, embracing all forms and mediums including the internet. Though internet publication has wider viewership, or a degree of permanence, and greater accessibility, than other fixed (as opposed to intangible) mediums of expression, it does not alter the essential part, that it is a forum or medium.

It is submitted that there is much sense to have more defined criteria taking into account the nature of the internet content. Injunctions on internet content should not be readily granted (especially ex-parte) since, firstly the internet is an easy and self publishing platform providing a medium of expression for marginal individuals not having corporatist outlets. Secondly, the internet facilitates the distribution of content for a minor cost to a vast audience. Both the alleged injury and the free speech concern are greater due to the wider dissemination of the content.

7. ISSUES NOT COVERED UNDER ITACT

7.1 Existing Law Insufficient. It is submitted that ITAct and ITAAct 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 ITAct or ITAAct. Jurisdiction has been mentioned in Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected therewith. Section 80 deals with the police officers' powers to

---

[2]. **4680 of 2004 Criminal Complaint**
[3]. **I.A. No. 9089/2010 in CS(OS) 1407/2004**

enter, search a public place for a cyber crime etc.. Since 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 ITAct or the ITAAct which enable the investigating agencies that even if the ITAct part of the case is lost, the accused cannot escape from the IPC part.

7.2 Punishment For Teens and First Time Cyber Crime Offenders: Usually teens involve in cyber crime unknowingly or which according to them is fun. So, it was proposed by Home Ministry and IT department that first time offenders will be handled with leniency and with remedies like warning, counseling and parental guidance. It is submitted that the Government may consider the desirability of enacting a suitable law on such offenders.

8. 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 savior 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. 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. Endeavor 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

[1] Gaur, K.D., Text book on Indian Penal Code, Fifth edition, 2014, Universal Law Publishing Company Pvt. Limited, New Delhi

[2] The Constitution of India

[3] The Information Technology Act, 2000

[4] The Information Technology (Amendment) Act, 2008

[5] Code of Criminal Procedure, 1973

[6] The Indian Evidence Act, 1872

[7] The Bankers' Books Evidence Act, 1891