VOLUME-6, ISSUE-5, MAY-2017 • ISSN No 2277 - 8160 IF : 4.547 | IC Value 80.26

Original Research Paper Law

Cybercrime in India: A study of legal response with special reference to Information Technology Act, 2000

Reetika Rana Assistant Professor, Himachal Pradesh University Institute of Legal Studies, Shimla (H.P)

ABSTRACT The advent of computer has been boon to students, lawyers, business, doctors, teachers....and criminals. The Internet is fast becoming a way of life for millions of people. However, it is also being transformed into a haven for criminals. In fact, the growth of crime on Internet is directly proportional to the growth of Internet itself, and so is the variety of crimes being committed or attempted. Evil minded persons are taking benefit out of this technological progress by committing crimes, which are popularly known as Cybercrimes. Considering the nature of cyber criminality the deterrence is not only answer to cybercrime. It is being realised that a multipronged strategy has to be adopted to defend the internet community against cybercrime.

KEYWORDS : Cyber Crime, Internet, Information Technology Act, 2000.

Introduction

"The Modern thief can steal more with computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

- National Research Council, "Computer at risk" 1991

While Computer technology has opened doors to enhanced conveniences for many, this same technology has also opened new doors for criminals. Businesses that have grown to reply upon computerisation to collect and assemble sensitive information on their critical resources now face the daunting, and costly, task of protecting this information from those who would seek illegal access to it. Due to extraordinary impact of the internet, a computer crime scene can now span from geographical point of victimisation (e.g. the victim's personal computer) to any other point on the planet, further complicating criminal investigative efforts.[1]

Meaning of Cybercrime

Cybercrime can be defined as any crime with the help of computer and internet with the purpose of influencing the functioning of computer or computer system. It is an umbrella term and may have different meaning attached to it. But even after all these definitions and arguments, it can be stated that these terms are not amenable to a precise definition.[2]

Cyber Crimes in India: Information Technology Act, 2000

The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. The Information Technology Act, 2000 does not define Cybercrime but specifies many acts as an offence and make them punishable in certain circumstances. But, it would be unsuitable to restrict to all crimes described under IT Act as the IPC, Copyrights Act and Patent Act also cover many form of cybercrimes.[3]

For the sake of convenience, the computer crimes enlisted have been classified into following categories:

(i) Conventional Crimes through Computer

(a) Cyber Defamation

Cyber defamation would imply defamation by anything which can be read, seen or heard with help of computers. Cyber defamation is covered under Sec 499 of IPC read with Sec 4 of the IT Act, 2000.[4]

(b) Digital forgery

Digital forgery implies making use of digital technology to forge a document. Sec 91 of IT Act, 2000 (read with second schedule) amen ded the provisions of IPC in relation to forgery to include digital forgery and offences relating to it under IPC.

(c) Cyber Pornography

Cyber pornography refers to stimulating sexual or other erotic activity over the internet. The issue of cyber pornography has been dealt with in Sec 67 of IT Act, 2000 where the publishing of information which is obscene in electronic form has been made an offence.

(d) Cyber Stalking/ Harassment

Cyber Stalking is just an extension of physical form of stalking, the only difference being that in cyber stalking electronic mediums like internet are used to pursue, harass or contact another in an unsolicited fashion. Cyber stalking is merely criminal intimidation under Sec 503 of IPC. 2008 amendment to IT Act tries to sort out these problems by inserting Sec 66A(a) of IT (Amendment) Act, 2008.[5]

(e) Internet Fraud and Financial Crimes

The IT Act, 2000 deals with the crimes relating to Internet fraud and online investment fraud in Sec 43(d), 66B and 66D. Sec 43(d) penalizes a person who damages or causes damage to data. Internet fraud would also come within the scope of Sec 66B, 66D of IT (Amendment) Act, 2008.

(ii) Crimes Committed on a Computer Network

(a) Hacking/ Unauthorised Access

Hacking means unauthorised access to a computer system. Sec 66 of the IT Act, 2000 deals with hacking which provides that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. If someone only access a computer system without authorization, he cannot be booked under Sec 66 of IT Act. However, that does not mean that any person accessing without any right would go scot-free. The IT Act has dealt with unauthorized access in Sec 43(a).[6] Hacking is punishable under Sec66 and hacking of protected system is punishable under Sec 70 of IT Act.[7]

(b) Denial of Service

A 'denial of service' attack is characterized by an explicit attempts by attackers to prevent legitimate users of service from using that service. Sec 43(f) of IT Act deals with denial of service.[8]

(iii) Crimes relating to Data Alteration/Destruction

(a) Viruses, Worms, Trojan Horses and Logic Bombs

This set of attacks onto the computer/ computer data is by way of transmitting programs designed to destroy, alter, damage or even send across data residing in the computer. Section 43© of IT Act, 2000 covers area of introduction of virus etc.[9]

(b) Theft of Internet hours

Theft of internet hours refers to using up or utilizing of somebody else's internet services. This is one of the most common computer crimes today. Sec 43(h) of the IT Act, 2000 address the issue of theft of internet hours.[10]

(c) Data Diddling

Data diddling involves changing data prior or during input into a computer. Sec 43(d) of IT Act, 2000 and Sec 66 of IT Act, 2000 would cover such kind of computer crime.

(iv) Crimes relating to Electronic Mail

(a) E-Mail Spamming/Bombing

Spam means to crash a program by overrunning a fixed-size buffer with excessively large input data. In relation to email accounts, it means bombing an email account with a large number of messages may be same or different messages. In case an Internet service provider is receiving a voluminous, regular supply of spam messages that is disrupting its entire network and consuming its disk space, Sec 43(e) of act can be a good refuge.[11] After 2008 amendment to IT Act, Sec 66A(b) of IT Amendment Act, 2008 entitled as ' punishment for sending offensive messages through communication service etc' would cover Spam.

(b) E-Mail Snoofing/Phishing

A snooped email is one that appears to originate from one source but actually has been sent from another source.[12] This kind of computer crime is also covered by provisions under Section 463 of IPC relating to forgery. Sec 66A(c) of IT (Amendment) Act, 2008 deals with E-mail spoofing.[13]

Conclusion

To curb computer crimes, one is required to understand them in the perspective of technological advancements and case with which they can be committed. The old adage of 'an eye for an eye' would be equally applicable to reduce computer crimes. It should be 'technology for technology'. The Information Technology Act is an evolving law. New varieties of cyber crimes are being committed day-by-day and existing law is not sufficient to deal with all such crimes. The IT Act, 2000 provides for the most prevalent and convenient method used in our country to deal with crime i.e. deterrence. Considering the nature of cyber criminality as discussed above even common sense would tell us that deterrence is not only answer to cyber crime. It is being realised that a multi pronged strategy has to be adopted to defend the internet community against cyber crime. Deterrent laws are only one of the several strategies of tackling criminality. Each of the aforesaid characteristics of cyber crime ought to considered while devising effective measures of checking, preventing and punishing cyber crimes which threaten the global community.

1. Shashank Manish,"Regulation of Cyber Crime in India", 114 CrLJ 305 (2008).
2. Dr Sunil Desta and Shweta Thakur, "Cyber Jurisprudence and IT Act, 2000", 47 CMLJ 204 (2011)
3. Dr Chandra Pal Sheoran, "Cyber Crimes: Meaning, Nature and Scope", XIV MDULJ 166 (2009).
4. The Information Technology Act, 2000 (Act 21of 2000), s. 4 provides that if the law requires any information or any other matter in writing or typewritten or printed form, such requirement would be deemed to have been satisfied if such information is rendered or made available in electronic form and accessible so as to be usable for a subsequent reference.
5. The Information Technology(Amendment)Act, 2008 (Act 21of 2000), s. 66A(a) provides 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 shall be punishable with imprisonment up to 3 yrs and fine.
6. The Information Technology Act, 2000 (Act 21of 2000), s. 43(a) provides that if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network (a) access or secure access to such computer, computer system or network, shall be liable to pay damages by way of compensation not exceeding 1 crore to person affected.
7. The Information Technology Act, 2000 (Act 21of 2000), s. 70 provides that if protected system is accessed unauthorisedly, it would be an offence punishable with imprisonment up to 10 years and fine.
8. The Information Technology Act, 2000 (Act 21of 2000), s. 43(f) provides that if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network denies or causes denial of access to any person authorised to access any computer, computer system or network by any means shall be liable to pay damages by way of compensation not exceeding 1 crore to person affected.
9. The Information Technology Act, 2000 (Act 21of 2000), s. 43(c) provides that if any person without permission of the owner or person in charge introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, shall be liable to pay damages by way of penalty not exceeding 1 Crore to person so affected.
10. The Information Technology Act, 2000 (Act 21of 2000), s. 43(h) provides that if any person without authorization of owner or the person in charge, charge the service availed of by a person to the account of another person by tampering with or manipulating any computer, computer system shall be liable to pay damages by way of penalty not exceeding 1 Crore to the person or office
11. The Information Technology Act, 2000 (Act 21of 2000), s. 43(e) provides that if any person has dishonestly or fraudulently disrupts or causes disruption of any computer, computer system or network shall be liable for damages to tune of 1 crore to person affected.
12. Dr. Krishna Pal Malik, Computer and Information technology law 187 (Allahabad Law Agency, Faridabad, 1st edn., 2010).
13. The Information Technology(Amendment) Act, 2008 (Act 21of 2000), s. 66A (c) provides that any person who sends.....any electronic mail for purpose of causing annoyance or to deceive or to mislead addressee or recipient about origin of such messages shall be liable.