RESEARCH REVIEW JOURNALS
Volume-03
Issue-01
January-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Cyber Crime and Cyber Law under Information Technology Act 2000

Jadeja Prithviraj Manubha

B.Com, LL.B & LL.M

ARTICLE DETAILS

Article History

Published Online: 28 January 2018

Keywords

Cybercrimes, Cyber law, Cyberspace, Information Technology Act 2000, Internet

***Corresponding Author**

Email: pmjadvocate@gmail.com

ABSTRACT

"Cybercrime" combines the term "crime" with the root "cyber" from the word "cybernetic", from the Greek, "kubernân", which means to lead or govern. Cybercrime, or computer oriented crime, is crime that involves a computer and a network. Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones. This research paper aims to discuss following aspects of Cybercrimes: the definition, why they occur, laws governing them, methods of committing cybercrimes, who they affect, and cybercrime prevention procedures. The report will show the usage and progression of technology has amplified different types of crimes such as theft crimes and terrorism. Also, this report will display statistical data which will give an idea of how far cybercrimes has increase over the period of ten years or more.

INTRODUCTION

In our modern technology-driven age, keeping our personal information private is becoming more difficult. Due to exponential growth of Internet and thereby online mobile banking and such other related technologies, present world is being benefited by the use of these technologies. In each segment like banking, airport, space, railway, telecommunication and social media today's world is fully dependent on the technology and all these technologies are interlinked with one another through Internet. Each innovation or new technology facilitates a lot of advantages but same time it may produces the side effects. In the present day world is fully dependent on Internet via social media, banking transaction, mobile transactions etc[1]. The truth is, highly classified details are becoming more available to public databases, because we are more interconnected than ever. Our data is available for almost anyone to sift through due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promise to ease our daily lives; however, there are dangers of using technology. One of the main dangers of using technology is the threat of cybercrimes. This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet. Now comes the term "Cyber Law". It doesn't have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law[2]. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model[3].

HISTORY OF CYBER CRIME

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future.[4]

TYPES OF CYBER CRIMES

It is important to note that a computer, Internet or computer technology has to be involved, and when the use of any of the following techniques or activities is made to carry out a crime or illegal activity only then can it be classified as a Cybercrime. There are many types of cyber crimes and the most common ones are explained below:[5]

3.1 Hacking

Hacking is the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data (leaving a trace) without the intention of destroying data or maliciously harming the computer. Hacker Person who gains authorized/unauthorized access to a computer without the intention of causing damage[6].

3.2 Cyber-Stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to Web site or a discussion group. A cyber stalker relies upon the anonymity

afforded by the Internet to allow them to stalk their victim without being detected[7].

3.3 Cyber Defamation

Cyber defamation is not a specific criminal offence, misdemeanor or tort, but rather defamation or slander conducted via digital media, usually through the Internet. Penalties for 'Cyber defamation' vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights[8].

3.4 Cracking

It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer systems without your knowledge and consent and has tampered with precious confidential data and information[9].

3.4 Cyber Squatting

Cyber squatting (also known as domain squatting), according to the United States federal law known as the anti-cyber squatting Consumer Protection Act, is registering, trafficking in, or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cyber squatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price[10].

3.5 E-Mail Spoofing

Email spoofing is the creation of email messages with a forged sender address. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations[11].

3.6 SMS Spoofing

SMS spoofing is a relatively new technology which uses the short message service (SMS), available on most mobile phones and personal digital assistants, to set who the message appears to come from by replacing the originating mobile number (Sender ID) with alphanumeric text. Spoofing has both legitimate uses (setting the company name from which the message is being sent, setting your own mobile number, or a product name) and illegitimate uses (such as impersonating another person, company, and product)[12].

3.7 Intellectual Property Crimes

Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. A copyright is the legal right of an author, publisher, composer, or other person who creates a work[13].

3.8 Cyber Vandalism

Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer[14].

3.9 Cyber Trespass

The word ―trespass‖ in general means to enter into the other's property without seeking consent. It is considered a civil wrong ordinarily. If the trespass is committed with criminal intention it is called criminal trespass. The concept of trespass is applicable in cases of the cyber world and may be termed as Cyber Trespass[15].

3.10 Online Gambling

Internet gambling business means ―the business of placing, receiving or otherwise knowingly transmitting a bet or wager by any means which involves the use, at least in part, of the Internet, but does not include the performance of the customary activities of a financial transaction provider, or any interactive computer service or telecommunications service.

3.11 Fraud and financial crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:[16]

- Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes.
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect.
- Altering or deleting stored data.

3.12 Cyber extortion

Cyber extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyber extortionists are increasingly attacking corporate websites and networks, crippling their - bility to operate and demanding payments to restore their service[17].

3.13 Transmitting Virus

Computer viruses usually spread in one of three ways: from removable media; from downloads off the Internet; and from e-mail attachments.

3.14 Phishing

Phishing schemes are one of the chief ways in which people end up with their identity stolen and a computer fill of viruses. A phishing scheme starts when you receive an email from a website claiming to be your bank or Credit Card Company.

Many times, when you visit these sites, spyware, adware and viruses are automatically installed on your[18].

3.15 Credit/Debit Card Fraud

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

3.16 Spam

Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc[19].

3.17 Cyber terrorism

Cyber terrorism is the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

3.18 Identity theft

This is when someone seizes another's individual information without his or her awareness to commit theft or fraudulency. Typically, the victim is led to believe they are revealing sensitive private data to a genuine business, occasionally as a response to an e-mail to modernize billing or membership information etc.

3.19 Bot Networks

A botnet is a collection of compromised computers often referred to as ―zombies‖ infected with malware that allows an attacker to control them[20].

3.20 Distribution of pirated software

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries.

CATEGORIES OF CYBER CRIME

Cyber crimes are broadly categorized into three categories, namely crime against[21].

1. Individual
2. Property
3. Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

4.1 Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

4.2 Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

4.3 Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

CYBER LAW IN INDIA

Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy. Generically, cyber law has been referred to as the Law of the Internet.

5.1 The Origin of IT legislation in India

Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records i.e. the data what is stored in a computer or an external storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record[22].

5.2. Information Technology Act 2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce[23].

5.2.1 Objectives of I.T. legislation in India

- It's objective of I.T Act 2000 to give legal recognition to any transaction which is done by electronic way or use of internet.

- To give legal recognition to digital signature for accepting any agreement via computer.
- To Provide facility of filling documents online relating to school admission or registration in employment exchange.
- According to I.T. Act 2000, any company can store their data in electronic storage.
- To stop computer crime and protect privacy of internet users.
- To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
- To make more power to IPO, RBI and Indian Evidence act for restricting electronic crime.

5.3 Amendments

A major amendment was made in 2008. It introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009[24].

5.4 Penalties, Compensation and Adjudication under IT Act 2000

Sec.43:- If any person without permission of the owner damages to computer, computer system, etc. he/she shall be liable to pay compensation to the person so affected.

Sec.43A:- Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, in negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Sec.45:- Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Sec.66:- 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.

Sec.66B:- Punishment for dishonestly receiving stolen computer resource or communication device is Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Sec.66C:- Punishment for identity theft— Whoever, fraudulently make use of electronic signature or password, shall be liable for imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Sec.66E:- Punishment for violation of privacy- Whosoever, 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.

Sec.66F:- Cyber terrorism Imprisonment which may extend to imprisonment for life.

Sec.67:- Punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published or transmitted 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, 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.

Sec.67A:- 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.

Sec.67B:- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form- Abusing children online, imprisonment 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.

Sec.67C:- Preservation and retention of information by intermediaries.—(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribed. (2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Sec.72:- Penalty for breach of confidentiality and privacy.— Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations 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 electronic record, book, register, correspondence, information, document or other 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.

Sec.75:- Act to apply for offences or contravention committed outside India.—(Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

{ Section 43, 43A, 45, 66, 66B, 66C, 66E, 66F, 67, 67A, 67B, 67C, 72, 75 *}[25]*

5.5 Indian Computer Emergency Response Team (CERT-IN)

CERT In is the national nodal agency for responding to computer security incidents as and when they occur. As per the Information Technology Amendment Act 2008 and Section 70B of IT Act 2000, CERTIn has been designated to serve as the national agency to perform the following functions in the area of cyber security: Collection, analysis and dissemination of information on cyber incidents, Forecast and alerts of cyber security incidents, Emergency measures for handling cyber security incidents, Coordination of cyber incident response activities. Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents. Such other functions relating to cyber security as may be prescribed[26].

CONCLUSION

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cybercrimes. The Information Technology Act is the sole savior to combat cyber crime in nature. Though offences where computer is either tool or target also falls under the Indian Penal Code and other legislation of the Nation, but this Act is a special act to tackle the problem of Cyber Crime. The Act was sharpened by the Amendment Act of 2008, yet the Act is still in its budding stage. There is grave underreporting of cyber crimes in the nation. Cyber Crime is committed every now and then, but is hardly reported. The cases of cyber crime that reaches to the Court of Law are therefore very few. There are practical difficulties in collecting, storing and appreciating Digital Evidence. Thus the Act has miles to go and promises to keep of the victim of cyber crimes.

References

[1] http://ijrest.net/downloads/volume-2/issue-4/pid-ijrest-24201503.pdf

[2] https://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india

[3] http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW

[4] https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

[5] http://www.thewindowsclub.com/types-cybercrime

[6] https://economictimes.indiatimes.com/definition/hacking

[7] https://www.techopedia.com/definition/14326/cyberstalking

[8] http://www.helplinelaw.com/family-law/CDII/cyber-defamation-in-india.html

[9] https://www.legalindia.com/cyber-crimes-and-the-law/

[10] https://www.nolo.com/legal-encyclopedia/cybersquatting-what-what-can-be-29778.html

[11] https://searchsecurity.techtarget.com/definition/email-spoofing

[12] https://hackernoon.com/sms-spoofing-used-to-swindle-retailers-merchants-c4023c7d8dbd

[13] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/intellectual-property-crime

[14] http://www.waronidtheft.org/cyber-vandalism-an-artwork-of-cyber-threat/

[15] https://definitions.uslegal.com/c/computer-trespass/

[16] http://www.spk.gov.tr/Sayfa/Dosya/849

[17] https://www.cisecurity.org/cyber-extortion-an-industry-hot-topic/

[18] https://www.incapsula.com/web-application-security/phishing-attack-scam.html

[19] https://www.computerhope.com/jargon/s/spam.htm

[20] https://www.lifewire.com/what-is-a-bot-net-2487267

[21] http://ijarcsse.com/Before_August_2017/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

[22] http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

[23] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

[24] http://www.eprocurement.gov.in/news/Act2008.pdf

[25] http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf

[26] http://www.cert-in.org.in/