INTERNATIONAL JOURNAL OF PHARMACY AND ANALYTICAL RESEARCH

ISSN:2320-2831

IJPAR |Vol.7 | Issue 3 | July - Sep -2018
Journal Home page: www.ijpar.com

Research article *Open Access*

Cyber crime and related laws in India

Dr. Jyoti Pralhad Kasture[1]

Sumati Park, Shrinagar Housing Society, Garkheda Parisar, Aurangabad- 431005, Maharashtra, India.

***Corresponding Author: Dr. Jyoti Pralhad Kasture**
Email: drjyotipk@gmail.com

ABSTRACT

The internet in India is growing rapidly. It has given rise to new opportunities in every field, it is universally proved that every concept has advantages and disadvantages and one of the most disadvantage is cyber crime. Cyber crime is any illegal activity which is committed using internet. It violates privacy or damage to computer system such as files, website or software. In current scenario of increasing crimes, cyber crime has also geared up its ratio. India has largest internet users with comparatively less cyber crime awareness. The article attempts to describe every angle related to cyber crime and its laws.

Keywords: Cyber Crime, India, Cyber Law

INTRODUCTION

Internet has occupied human life with the speed of lightening. In present days, people access, store and share information through internet. The growing fastest world of the internet is known as cyber world. Cyber world is fastest moving and hi-technology world. Asian countries uses huge amount of internet and therefore internet has become backbone of social and economic world. Because of evolution of internet services and smart phones, users can access internet anytime, anywhere and thus it has become most efficient way of data communication.

Cybercrime is most complicated problem for cyber world. 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 [1]. The Indian law has not given any definition to the term cybercrime [2]. In fact, Indian penal code does not use term, cybercrime at any point, even after its amendment by the information technology (amendment act 2008). The cyber terrorism is the premeditated, politically motivated attack against information, computer system, computer programs and data which result in violence against property, government and people at large. The terms cyber forensics, digital forensics and computer forensics are almost synonymous to cyber crime. Cyber forensics deals with preservation, identification, extraction and documentation of computer evidences stored in the form of magnetically encoded information i.e. Data. In India, information technology act 2000 deals with the cybercrime issues.

TYPES OF CYBER CRIME

Now a day, personal computer has become less expensive and has become powerful tool, but can be used further for almost any criminal activity. Following are the types of cybercrime.

Hacking / webcam hacking-

Unauthorized access to computer system or networks (hacking) writing or using readymade programs to attach the target computer). Webcam hacking is done through software by spyware, Trojan or Google.

1. Theft of telecommunication services including theft of information contained in electronic form.
2. Fraud in electronic fund transfer
3. E-mail bombing- sending a many mails to the victim.
4. Software piracy, malicious software, spreading of spywares.
5. Denial of service attacks.
6. Trafficking, virus attack (i.e. Virus, worms, Trojan and spyware)
7. Web jacking- control over the website of another.
8. Child pornography, cyber stalking, phishing, organized crimes.

FACTORS RESPONSIBLE FOR CYBER CRIME

- Negligence is considered to be the single largest factor, responsible for cyber crime.
- Carelessness or negligence in the security of computer system provides easy access to a cyber thief to gain access and can take control the computer system.
- The computer operating system is a collection of billions of codes. Human mind can make mistakes or error –prone and therefore it is not possible that there might not be any loophole present at any stage. The cyber criminals get upper hand of these loopholes and make easier access in the computer system.
- The problem faced in protecting a computer system from an intruder access is that, there are increased chances of breach, not due to human error but due to complex technology. By secretly placed logic bomb, key logger can steal access code, advanced voice recorder, retina imager can fool biometric system and by pass firewalls can be utilized to get passed much security system.
- Personal computers have become an inexpensive and very powerful tool that can be used further for any criminal activity. Cyber security has become a critical concern of government, law enforcement agencies and industries.

PRESENT TRENDS OF CYBER CRIME IN INDIA

India is starving hard to execute the digital India project effectively. The success of digital India project would depend upon maximum connectivity with maximum cyber security. This is one of the major obstructions for India as India has many loopholes history in cyber security. According to home ministry statistics, as many as 71780 cyber frauds were reported in 2013, while 22060 such cases were reported in 2012. There have been 62189 incidents of cyber frauds till June 2014. In 2013, a total of 28481 Indian websites were hacked by various hacker groups spread across the globe. The numbers of hacking incidents were 27605 in 2012 and 21699 in 2011. As per the cyber crime data maintained by national cyber records bureau, a total of 1791, 2876, 4356 cases were registered under the IT act in 2011, 2012, 2013 respectively. A total of 422, 601 and 1337 cases were registered under cyber crime related sections of IPC in 2011, 2012, and 2013 resp. There has been an annual increase of more than 40% in cyber crime cases, registered in the country during the past years[2]. According to national crime records bureau, a total of 288, 420, 966, 1791 and 2876 cyber crime cases were registered under it act during 2008,2009,2010,2011 and 2012 resp. As per the information reported to and tracked by Indian computer response team a total no of 208, 371 and 78 government websites were hacked during the years 2011,2012 and 2013 respectively and 16035 incidents related to spam, malware infection and system break-in were reported in 2013 [3].

Cybercrime cases in India, registered under the IT Act, increased at a rate of 300 percent between 2011 and 2014[4]. In 2015, there were 11,592 cases of cyber crime registered in India[5].

CYBER LAWS IN INDIA

The Indian parliament considered it necessary to give effect of the resolution of adopted model law on electronic commerce accepted by the United Nations commission on trade law in the general assembly of United Nations on 30th January 1997. As a consequence of which, the IT Act 2008 was passed and enacted on May 2000 based on uncial model.

The preamble of this act states its objectives to legalize E-commerce and to amend the IPC 1807, Indian evidence act 1872, the banker's book evidence at 1891 and the RBI act 1934. The important sections are sec43, sec65 and sec67.

SR. NO.	ACT/SECTIONS	OFFENSES	PENALTY
1	SEC 43	Deals with the unauthorized access, unauthorized downloading, virus attack or any contaminant causing damage to computer.	Fine up to Rs.1crore by the way of remedy.
2	SEC 65	Deals with tampering with computer sourced documents	Imprisonment up to 3 years or fine
3	SEC 66	Deals with hacking with computer system Sec 66-1: deals with loss or damage to computer resource Sec 66-2 : hacking	Imprisonment up to 3 years or fine
4	SEC 67	Deals with publication of obscene material	Imprisonment up to 10 years and also with the fine of 2 lakhs.
5	SEC 69	Deals with the failure to assist to decoy	
6	SEC 70	Unauthorized access or attempted access of protected computer system	
7	SEC 71	Obtaining lie or digital signature by misinterpretation or suppression of fact	
8	SEC 72	Breach of confidentiality	
9	SEC 73	Publishing false digital signature	
10	SEC 74	Fraud digital signature	
11	IPC SEC 167,172,173, 175	Offenses by or against public servant	
12	IPC SEC 193	False electronic evidence	
13	IPC SEC 204, 470	Destruction of electronic evidences	
14	IPC SEC 463, 465, 466, 469, 471, 474, 476 AND 477-A	Forgery	
15	IPC SEC 405, 406, 408, 409	Criminal breach of trust or fraud	
16	IPC SEC 183, 482, 483, 484, 485	Counterfeiting or marks	
17	IPC SEC 489	Tampering	
18	IPC SEC 489-A, 489-E	Counterfeiting currency or stamps	

Cyber crime cells have been set up in major cities, but still most cases remain unreported due to a lack of awareness [6]

List of Cyber Crime Cells [7, 8]

- Cyber Crime Investigation Cell (New Delhi)
- Cyber Crime Investigation Cell (Mumbai)

- Cyber Crime Police Station, Hyderabad City Police
- Cyber Crime Police Station, CID, Hyderabad
- Cyber Crime Investigation Unit (CCIU)
- Cyber Crime Cell Rajasthan
- Cyber Crime Cell Punjab

CONCLUSION

It is cleared from the previous studies and records that with the increment in technology, cyber crime increases. Qualified people commit crime more s, there is a need to know about principles and computer ethics for their use in proper manner. Cyber crime a hacking is not going away, if anything, it is getting stronger.

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 an integral part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891 and the Reserve Bank of India Act, 1934. Any part of the world cyber crime could be originated passing national boundaries over the internet creating both technical and legal complexities of investigating and prosecuting these crimes. The main purpose of writing this paper is to spread the content of cyber crime among the common people. If anyone falls in the prey of cyber attack, please come forward and register a case in your nearest police station. If the criminals won't get punishment for their deed, they will continue to harass people whenever they can.

REFERENCES

[1]. https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf

[2]. http:://deity.gov.in/sites/upload_files/dit/files/downloads/itacts2000/itbill2000.pdf

[3]. http:://ncrb.nic.in

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

[5]. Cybercrime in India up 300% in 3 years: Study". Economic times. Bennett, Coleman & Co. Ltd. Retrieved 8, 2017.

[6]. "11,592 cases of cyber crime registered in India in 2015: NCRB". LineMint. HT Media Ltd. Retrieved 8, 2017.

[7]. "Cyber crime scene in India".

[8]. "Cyber Crime Units in India". CSR India. Csr India. Retrieved 8, 2017.

[9]. "Cyber Crime Investigation Cell". Cyber Cell Mumbai. Cyber Crime Investigation Cell, Mumbai. Retrieved 16, 2017.