IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER CRIMES AND LAW IN INDIA: A CRITICAL ANALYSIS

Nirav Prakashbhai Vithalani

Research Scholar

Department of Law, Saurashtra University

Abstract :

As is common knowledge, most activities in this day and age—from online business to online transactions—are conducted via the internet. the internet is seen as a global stage, and anyone can access online resources accessible from anywhere. On the web a small number of people have been exploiting technology for illegal actions such as fraud and illegal network access etc. These illicit behaviors or the corresponding infraction or crime Cybercrime is defined as occurring online. To put an end to or penalize online criminals the phrase "Cyber Law" introduced. We can characterize cyber law as a subset of the systems of law that address the Internet, cyberspace, and with the judicial matters.

1. INTRODUCTION

The development of computers has improved human lives. Consequently, it has been used for a variety of reasons by individuals and major businesses worldwide. In In simple terms, a computer is a device that information can be processed and stored, or instructions that the user provides. 99% of computers Users are misusing computers in their daily lives. either for their own personal gain or the welfare of others. advantage for many years [1]. As a result, "Cyber Crime" was born. This resulted in the participation in activities that are forbidden by society. Cybercrime is defined as the crimes conducted over a computer network or on a computer They are typically conducted online, particularly the World Wide Web.

2. Objectives: Our paper's main goal is to promote the familiarity with the laws that are enforced against those crimes and offenders, as well as understanding of the crimes or offenses that occur online or in cyberspace. We also want to emphasize the security in cyberspace.

3. CYBER CRIME AND CYBER LAW

We can define "Cyber Crime" as any criminal activity or other offenses involving electronic communications or information systems, including any equipment or the Internet, both or each of them, or both or more of them .

The legal concerns connected to the use of communications technology, specifically "cyberspace," or the Internet, are referred to as "cyber law." The goal is to harmonize existing legal frameworks for the physical world with the difficulties posed by human activity on the Internet.

3.1 Online Crime

In 1995, Sussman and Heuston initially suggested the phrase "cyber crime." Cybercrime is best understood as a group of acts or conducts; there is no single term that adequately captures it. These actions are based on the tangible offense item that has an impact on computer systems or data.

These are illicit activities when a digital device or information system is either a tool, a target, or both. Other names for cybercrime include electronic crime, crime involving computers, e-crime, high-tech crime, information age crime, etc.

Simply put, "Cyber Crime" refers to offenses or crimes committed via electronic communications or information networks. These offenses are essentially prohibited behaviors.

3.2 CYBER LAW

In order to take control of crimes committed online, in cyberspace, or via the use of computer resources, cyber law was created a description of the legal concerns relating to the uses a form of computer technology or communication like Cyber Law.

3.2.1 What is the importance of Cyber Law?

In this modern technological era, cyber law is extremely significant. It is significant since it affects practically all elements of activities and transactions that occur. on the internet or other platforms for communication. Whether Whether we realize it or not, every action and everywhere There are certain legal and cyber-legal responses in cyberspace.

3.2.2 Cyber Law awareness program

Once should have the following knowledge in order to stay aware about the cyber crime:

- One should read the cyber law thoroughly.
- Basic knowledge of Internet and Internet's security.
- Read cyber crime's cases. By reading those cases one can be aware from such crimes.
- Trusted application from trusted site can be used for protection of one's sensitive information or data.
- Technology's impact on crime.

3.2.3 The Information Technology Act of India, 2000

October 17, 2000. It is the most significant law in India that addresses cybercrimes or digital crimes. and online shopping. On the United Nations, it is based 1996 UNCITRAL Model Law on Electronic Commerce Model) suggested by the United Nations General Assembly a resolution dated 30 January 1997 among the nations.

Some key points of the Information Technology (IT) Act 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through egovernance.
- The communication between the companies or between the company and the

government can be done through internet.

 Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.

 In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company

3.2.4 Cyber Law in India

Following are the sections under IT Act, 2000

1. Section 65- Temping with the computers source documents Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

2. Section 66- Hacking with computer system, data alteration etc Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both.

3. Section 66A- Sending offensive messages through any communication services

 Any information or message sent through any communication services this is offensive or has threatening characters.

 Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.

 Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages.

Punishment: Any individual found to commit such crimes under this section could be sentenced upto 3years of imprisonment along with a fine

4. Section 66B- Receiving stolen computer's resources or communication devices dishonestly Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same.

Punishment: Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

5. Section 66C- Identify theft Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

Punishment: Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

4. CONCLUSIONS

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 withcybercrimes. The Act further revise the IPC, 1860, the IEA (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 international harmonizing efforts, coordination and co-operation among various nations are required to take action towards the cyber crimes. Our main purpose of writing this paper is to spread the content of cyber crime among the common people. At the end of this paper "A brief study on Cyber Crime and Cyber Law's of India"

we want to say cyber crimes can never be acknowledged. 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 never stop.