International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

Cyber Laws in India

Ms. Anjali Jolly
Computer Science Deptt.
DAV College
Hoshiarpur, India

***Abstract*-In the present sophisticated era of communication and digital technology, the frauds are also tend to be the most hi-tech. technology is moving forward leaving behind the space for players from all walks of technocrats where few of them uses it effectively while other may hamper it unethically. Cyber laws are Act providing legal recognition for carried out transaction by means of electronic communications generally referred to as electronic commerce and storage of information, to facilitate electronic filing of documents with the government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act 1934 and for matters pertaining to them or incidental thereto. Most of the business and legal provisions anticipates the paper based progression holding physical signatures and law of evidence is also traditionally based upon paper records and oral testimony, hence to facilitate electronic commerce records and transaction the need for legal changes have become an urgent necessity. Cyber law in India desires provisions such that people can perform transactions through credit cards without fear of misuse over the internet. This paper illustrates Information Technology Act 2008 and its provisions, its need and necessity in India and the momentum at which cybercrimes are reached.**

Keywords:- Access, data, Information, digital signature, addressee, communication devices, certified authorities, security procedures, cyber law, cyber space, cyber crime, information and communication technology, Hackers, Fraud, and Privacy.

I. INTRODUCTION

There is a privacy concern about the problems of any data or confidential information hijack or damage, mat it be illegally consummated. In many countries, cyber crimes cells are primarily operated and used to deal with such offenses and to punish criminals who commit cyber crimes.

- It basically varies from theft of the entire identity of an individual, disrupting the internet and network connection of a specific country because of huge assaults across its networking resources.
- In this digital area, online communication is now becoming a standard; web users and government are in increase danger of becoming the eye of the cyber assaults. Cyber crimes can also damage anyone's ATM password. Hacking organizations transfer cash by hacking victim's account information to steal personal data. Also, some pornography problems are managed knowledgably.
- To tackle and cope-up with these crimes, there is an urgent need to enforce certain laws and regulations which are particular known as cyber law cyber safety, needs worldwide co-operation.
- It will protect against unauthorized accessed disclosure of computer equipment, system resources, information and data.
- Various types of attacks are strongly defined and the hacks category is also extracted.

Cyber crimes are detailed in its two types of crime classification in section II. In section III various kinds of assaults are summarized briefly. In the next section, the hacker category is acknowledged. Then in section V, the affect of cyber crimes is detailed. In the last section, there is a brief summary of cyber society.

II. II. BACKGROUND OF CYBER LAWS IN INDIA

In India IT Act has been introduced in year 2000 and was enforced successfully on 17th Oct 2000. The primary purpose of the said Act was to provide the legal recognition of electronic communication and to filing of electronic records with government. Information Technology Act 2000 was comprises of 94 sections segregated into 13 chapters. But as the trends in technology are changing with the flick of an eye and hence the commitment of offences. Ultimately, there was a need to amend the law according to the time and the Act has been amended in year 2008 known as IT Amendment Act 2008 which was passed by the parliament on 23rd Dec 2008. It receives the assent of the president of India on 5th Feb, 2009 and IT Act 2008 has been notified on October 27th,2009.

IT Act 2008 is a new version of IT Act 2000 which provides additional focus on information security. It also added several new sections on offences related to cyber terrorism and data protection. Schedule I and II have been replaced and schedule III and IV were deleted.

III. OBJECTIVES OF INFORMATION TECHNOLOGY ACT 2000

The main objectives of Act are to provide:

- Legal recognition of transactions.
- To facilitate electronic filing of documents with the government agencies.
- To amend the Indian Penal Code, the Indian Evidence Act 1872, the Banker's Book Evidence Act 1891 and Reserve Bank of India Act 1934.
- Aims to provide the legal framework to all electronics records.

IV. CYBER LAW: ITS NEED AND IMPORTANCE IN INDIA

As per the National Research Council, United States of America, "Computers at Risk", 1991, Publication quotes that the "the modern thief can steal much more with a computer

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

than with gun. Tomorrow's terrorist may be more efficient and to do more damages in a sophisticated way with a keyboard than with a bomb."

Cyber Law is a law of land governing cyber space and there are plethora of reasons why there was utmost need of cyber law:

- As the internet has become an integral part of every individual's life directly or indirectly.
- There is a huge transformation of transactions from black and white to paperless world.
- Real world existing laws are not sufficient and cannot be interpreted in the light of emerging cyber space.
- Internet services do require enabling and supportive legal infrastructures to tune with the present challenges and circumstance.

Cyber crime precisely deals with any crime committed with intervention of computer and telecommunication technology and any crime where either the computer is used as an object or subject to reach, amount or leveled at breach of trust and the cyber law deals with latest trends in crime such as cyber crimes, electronic and digital signature, intellectual properties and data protection and privacy where the scope is not limited to this.

Cyber law includes cyber space which comprises of computers, networks, software, data storage devices such as hard disk, USB disks etc. the internet online web portals, electronic mails and even electronic devices such smart phones, ATM machines and online transaction business systems.

A. Statistics of Cyber Crimes: National Crime Record Bureau (NCRB)

As per the statistical data provided by the National Crime Record Bureau the number of incidents of cyber crime was increasing drastically and it was the demand of scenario of the moment to turn up with the specific laws dealing with such hi-tech crimes.

TABLE 1: STATISTICS OF CYBER CRIME SHOWING INCREASED TREND OF OFFENCES.

Year	2008	2009	2010	2011
Cyber Crimes Reported	267	411	1322	2213

Cybercrime cases in India, registered under the Information Act, increased at a rate of 300 percent between 2011 and 2014.[6] In 2015, there were 11,592 cases of cyber crime registered in India.[7]

Number of cybercrime cases registered in Bengaluru was the highest in 2018. The country's technology capital saw a whopping 5,035 FIRs registered at the solely cybercrime police station in the city.[8]

B. Importance of Cyber Laws:

- The current is highly digitized and every think is based upon information and telecommunication technology.
- All the companies / corporate houses depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic formats.
- Online financial transactions using credit/debit cards are increased drastically in the recent past including operations in large business enterprises.
- Emails and SMS services have become an integral part of almost every individual's life and people are effectively habitual of using these services.
- Even in case of non-cyber crime cases, important evidence is found in computers / smart gadgets like cell phones and tablets, e.g. in case of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.
- Since it touches all the aspects of online transactions and operations on and concerning internet, the World Wide Web and cyber space therefore cyber laws are extremely important.

V. CATEGORIES OF CYBER CRIME

Cyber crimes are categories under three different categories (and further to business class):

C. Crimes against People:

Such crimes involves crimes like cyber aggravation and stalking, distribution or circulation of child pornography, fraud related to credit card, human trafficking, spoofing, identity/ credential theft, and online libel or slander offences.

D. Crimes against Property:

Online crimes are also vulnerable to be occurred against property, such as a computer or server. These crimes comprises of DDOS attacks, virus transmission, hacking, cyber and typo squatting, computer wreckage, copyright encroachment.

E. Crimes against Government:

Cybercrimes committed against the government are referred to as offence committed against the authorities, and it is considered an attack on that nation's sovereignty. Cybercrimes against the government also include hacking, fetching confidential information, cyber warfare, terrorism in cyber space, and pirated software or copy right violations.

F. Crime against business:

In these crimes, the criminals essentially hack any business organization's system or machine. They store and steal the system's private information on the server. They obtain unauthorized access to the company's secured and confidential information, transferring the company funds to their bankrupt organization.

VI. LIMITATIONS OF IT ACT 2000/ IT AMENDMENT ACT 2008

Even after the amendment of Act 2008, there are many weakness and gaps in the IT Act 2000 which are furnished explicitly below:

A. IT Act 2000 Is net concerned with proper protection of intellectual property for electronic data and information .controversial , but very major problem relating to the interest copyrights , trademarks and patents have been left in noticed by the law , leaving many gaps.

B. It does not pay any attention to problem linked to domain name. It does not cope with domain name holder right and liabilities (responsibilities).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

C. It does not cover different types of cyber crimes and its manifestation such as:
- Cyber theft
- Cyber stalking
- Cyber harassment
- Cyber deformation
- Cyber fraud
- Chat room abuses
- Misuse of credit card number

D. It does not address the problem of antitrust.
E. The electronic payment rules are not explicit.

VII. CONCLUSION

It can be said that each individual is at risk of cyber crimes, but they all are not victims. Cyber crime is not always related to computer only, but is operated through computer networks over the electronic communication channels. It is quite difficult to assess that someone is hacked, whereas, hacking can easily be performed across borders. With the advancement of technology, cyber criminals easily commit crime from their homes. Terrestrial laws may not be sufficient to reduce cyber crimes. Several countries depend upon these laws to conduct legal proceedings. Sometimes, cyber crime may have huge adverse impact on economic scale. Hence, there is an utmost need to execute huge penalties to reduce rate of such crimes. Further, in this era of advanced technology, users must be made aware about several methods of information security. At the same time, adequate technologies must be developed to address these concerns efficiently. Otherwise, weak technical solutions may worsen the situation. On a global scale, coordinated efforts must be taken to eliminate the gaps between terrestrial laws. This can significantly help to combat cybercrime more easily as similar jurisdictions may streamline the process of fighting against such incidents. It is important to understand the severity and promoting a secure environment while utilizing the technology. Legal and technical resources together may eliminate the complexity. With these approaches, cyber crimes can be decreased to a greater extent, which may further help in building the progressive economies, offering positive growth environment to business organizations.

REFERENCES:

[1]. //economictimes.indiatimes.com/articleshow/67769776.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
[2]. "Bengaluru is India's cybercrime capital ", Economics Times, Tushar Kaushik, Retrieved 01 feb 2017
[3]. ET Bureau|Updated: Feb 01, 2019, 07.15 PM IST
[4]. https://www.scribd.com/document/232861510/Conclusions-cyber-law
[5]. UGC-SWAYAM-MOOC on Cyber security. By Dr Padmavathi Ganapathi Professor in Computer Science Avinashilingam Institute for home science and higher education, course from July 2019 –Nov 2019
[6]. "Cybercrime in India up 300% in 3 years: Study". Economic Times. Bennett, Coleman & Co. Ltd. Retrieved 8 May 2017.
[7]. "11,592 cases of cyber crime registered in India in 2015: NCRB". LineMint. HT Media Ltd. Retrieved 8 May 2017.