CYBER LAW – NEED AND SIGNIFICANCE OF CYBER LAW IN PRESENT INDIA

***Anmol Shrivastava**

****Prof.(Dr). Anil Kumar Dixit**

ABTRACT

This has created a nexus where people from almost all walks of life have started forming group to do Cyber Crime and being protected by professionals in law .Today situation Cyber crime taking place in very small scale and big scale . Talking about the prevalence of Cyber crimes in India, they are spreading like a fire in every part of the society. Though digital need of the society , has been the most talked about issue in all spheres-social, economic and political, what are the need of the law in this particular society . Therefore the concern of this paper is to define Cyber crime, think about improvement and define conditional answers for annihilating the issue.

Keywords – cyberspace , cybercrime , Digital , Education

INTRODUCTION

Cyber law is a term which consists of the legal issues related to use of the internet .It is very broad field which different from the intellectual property or contract law. As it is a very wide and cover many areas of law and regulation. Some of the topics it includes are internet access and usage, privacy, freedom of expression, and jurisdiction.

In other words, cyber law can be considered as the part of the overall legal system that deals with the internet, digital contracts, electronic evidence and cyber space. As the cyber law is a broad subject to cover which also includes freedom of expression, data protection, data security, digital transaction, electronic communication and online privacy.

The Indian Information Technology Act in 2000 ("IT Act "). On the other side most of the companies are still aware about the strict provision of the law. The rising usage of information and communication has given up to serious compile concerns, which state unnoticed may attract various and criminal side. All the companies who directly or indirectly connected with cyber business are needed to fulfill with the requirement of the law. There are few cyber law firms in present India that had been given growth and devilment in the field of cyber law.[1]

*Student of BALLB 10th semester, Law College Dehradun , Faculty of Uttaranchal University , Dehradun Uttarakhand
**Prof in Law College Dehradun , Uttaranchal University , Dehradun Uttarakhand

HISTORY OF CYBER CRIME

The first cybercrime was recorded in 1820. The first type of computer has been found in Japan, China and India since 3500 BC. C., but Charles Babbage's analytical engine is considered to be the time of today's computers. In 1820, in France, a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of continuous steps in the fabric of fabrics or special materials. This has caused great concern among Jacquard workers that their livelihoods and traditional employment are at risk, and they prefer to sabotage to discourage Jacquard so that the new technology cannot be used in the future.

IMPORTANCE OF CYBER LAW

Cyber law is very vital because it put it hands in almost all aspects of transaction and behavior on and concerning the internet, the World Wide Web and cyberspace. Firstly it may see that the cyber laws is a very technical filed and it does not have any consistency to most actives in Cyberspace .But the true fact is that nothing could be further than the truth. Every work and every reaction in cyber space has some legal and cyber legal point of view.

In the computer-generated world of internet is known as basically cyberspace and law that is prevailing this particular area of cyberspace are known as Cyber laws and all the people use this cyberspace are come under the provisions of cyber laws. The cyber laws can also be describe as the branch of law that deals with the legal issues related to use of inter-networked technology. In short cyber law is the law governing the computer and the internet.

With the growth of Electronic commerce basically known as E-commerce has propelled the need for vibrant and regulatory mechanism which further gives strength the legal structure. And all of those infrastructure and mechanisms are come under the provision of Cyber law. As per the Information Technology Act 2000 Cyber Crime are not defined under it or in the National Cyber security Policy 2013, or in any other regulation in India. For the define Cyber-crime there only one can say that it is just a combination of crime with the computers. In other words any offence or crime in which a computer is used is a cyber-crime. Even a petty offence like stealing or phishing can be brought under the ground of cyber law. As per the I.T Act it defines all other particular necessary ingredients that can help for held of Cybercrime.

[1] http://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html (visited on 5th march)

"The Cyber Laws in India has paved the way for electronic commerce and electronic governance in the country by ensuring maximum connectivity and minimum cyber security risks. Also, enhancing the scope and expanding the use of digital mediums," says Advocate Krishnamohan K Menon.[2]

NEED FOR CYBER LAWS

In today's dynamic world and in a technological environment, the world is becoming increasingly digitalized and so are crimes. Internet was developed for research and to share the information tool. Over time, the Internet has paved the way for electronic commerce and electronic transactions. And all legal problems related to Internet crime are treated through cyber laws. According to the number of Internet users it has increased in recent years. With increasing use, the application of cyber laws to rigid and effective regulatory changes must be made to save the use of the Internet in today's world.

Advocate Tanuj Aggarwal says, "With the exponential growth in the digital space, the establishment of certain reforms was highly needed for the security of the citizen's privacy and data protection."3

CYBER LAWS IN INDIA

In India, Cyber laws are govern by the Information Technology Act 2000 also known as I.T act 2000, which particular came into force on the 17TH October, 2000. The core purpose of this Act is to provide legal recognition to E-commerce.

The existing laws of India, are very compassionate and liberal interpretation could not be interpreted in the light of the emergency of Cyberspace, to consists all the aspects relating to different activates in cyberspace, it the other hand the practical expression and the wisdom of judgment found that not be with savior treats , The exciting laws were to be interpreted in the situation of emerging of the Cyberspace , with not enhancing of new Cyber laws , therefore the need for enactment of the relevant Cyber laws . The laws relating to Cyber does been provided by the legal validity and sanction to the Cyber space. As per the example of basic thing that is E mail as in the India till today, email id not "legal". There is no particular which give the light to the validity to the email. The Courts and judiciary in our country have been reluctant to grant judicial recognition to the legality of email and in the not presence of any specific law having been enacted by the Parliament Accordance to need of the Cyber law in present India.

As IT Act is cyber security law introduced to secure the cyber space, the information Technology Law was amended under these other Acts:

[2] https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/ (visited on 5th march)
[3] https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/ (visited on 5th march)

- The Indian Penal Code
- The Indian Evidence Act
- The Banker's Book Evidence Act
- The Reserve Bank of India

But the core focus of this Act in India is to prevent:

- Computer Crime
- Forgery of electronic data & record in e-commerce
- Electronic transaction

THE INFORMATION TECHNOLOGY ACT OF INDIA, 2000

According to Wikipedia "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), it was notified on 17th October, 2000. It is the most important law in India that deals with the digital crimes or cyber-crimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997" [14].
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 e-governance.
- 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.

CYBER LAWS 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.[4]

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 personal computer. Diminish its utility, values or affects it injuriously by any means, commits hacking[5].

Punishment: Any person who involves in such crimes could be sentenced up to 3 years imprisonment, or with a fine that may extend up to 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 up to 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.[6]

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

[4] The Information Technology Act 2000 Chapter XI (Offences) Page no 29 .

[5] The Information Technology Act 2000 Chapter XI (Offences) Pageno.29

[6] The Information Technology Act 2000 Chapter XI (Offences) Page no. 30

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.[7]

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

6. **Section 66D**- Cheating by personation by the use of computer's resources Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend up to 3 years of imprisonment along with a fine that may extend up to rupee 1 lakh.[8]

7. **Section 66E**- Privacy or violation Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.[9][10]

OVERVIEW OF CRITICAL INFRASTRUCTURE (IT, PHYSICAL, SOCIAL) IN INDIA

More recently, service providers have resorted to the administration and hosting of email, websites and corporate physical and IT infrastructure, increasing the scope of cyber-attacks. The current scenario highlights that online crimes as a whole are committed through critical infrastructure rather than individuals that force researchers to learn to use computers,

Physical and social infrastructures are important for a better understanding of electronic crimes or cyber-crimes. The worst possible outcome of the risks created by information and communication technologies has been revealed in the possible failure of the so-called critical infrastructure, these are systems and assets whose incapacity would have an unbearable impact on national security and economic well-being and Social of a State. Motivated by a growing fear of the potential weakness of connected companies composed of amplified distractions in the cyber domain, several countries have taken the initiative to better understand vulnerabilities and threats to their infrastructure, and have implemented measures for the security of these assets

IT & PHYSICAL INFRASTRUCTURE

[7] The Information Technology Act 2000 Chapter XI (Offences) Page no. 30

[8] The Information Technology Act 2000 Chapter XI (Offences) Pageno .30

[9] The Information Technology Act 2000 Chapter XI (Offences)
https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf (visited on 6th March)

The Indian economy is highly dependent on IT infrastructure. India is putting more stress on the IT infrastructure in recent years. Indian IT industry is growing at a tremendous pace. Output of India's software industry has reached $16 billion. In connection to this scenario, millions jobs for professionals mainly at the support level have been produced with the rise of software industry[9]. Core proficiencies and strengths of IT services in India have exerted valued investments from key countries. IT infrastructure is not only essential in businesses and organizations straight associated to economic movement but also playing an increasingly significant role in households as well as in government crucial sectors [11]like healthcare and education. The IT industry has also formed considerable demand in the Indian education segment, specifically for engineering and computer science. The Indian IT and IT enabled services industry is divided into four major sectors - Software products and engineering services, business process management, IT services and hardware

CYBERCRIME CLASSIFICATION

Cybercrimes on the basis of nature and divergent types of attacks are classified into following main categories. Knowingly or unknowingly internet users becoming the victims of different types cyber-attacks. These attacks may vary in nature and their impact moreover it difficult to understand these attacks.

Crimes against individual - These are the crimes against person, against property of an individual are included. Against persons include harassment through e-mail, cyber stalking, and dissemination of obscene material on the Internet, defamation, hacking / cracking and by indecent exposure. Cybercrimes against property of an individual include computer vandalism, transmitting virus, Internet intrusion, unauthorized control over computer system and hacking / cracking etc.

Crimes against organizations - Includes crimes against government, private firm, company, group of individual etc. These crimes can be made by hacking and cracking, by possession of unauthorized information and through cyber terrorism against the government organization. Distribution of pirated software also covered under these attacks

Crimes against property - Involve credit card frauds, crimes related to intellectual property and internet time theft etc17,

Crimes against society - These crimes not only affect individual or any organization but the society at large. They include Pornography (especially child pornography), polluting the youth through indecent exposure and trafficking etc.

[11] https://blog.ipleaders.in/need-know-cyber-laws-india/ (Visited 0n 6th march)

Cybercrimes emanating from UseNet newsgroups - These attacks may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases posting have been mislabeled or are deceptive in another way[12]

CYBER CRIME'S SCENARIO IN INDIA (A FEW CASE STUDY)

A) The Bank NSP Case[13]

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

B) Bazee.com case[14]

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi. The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.

C) Parliament Attack Case[15]

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftily created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.

D) Andhra Pradesh Tax Case[16]

[12] https://expertcyberlawyer.com/meaning-of-cyber-law-and-importance-of-cyber-law/(Visited On 6th March)
[13] https://www.cyberralegalservices.com/detail-casestudies.php (Visited on 7th March)

[14] CRL.REV.P.127/2015 & CRL.M.A.No.3194/2015
[15] AIR MANU/SC/0465/2005

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.[17]

CONCLUSION

The tremendous growth in the use of the Internet worldwide and especially in India, accompanied by a sharp increase in cybercrime, has made India vulnerable to such crimes. Cyber-crimes are global in nature and criminals are not linked to a particular geographic area. Cyberspace is a free space, without borders and not protected by local geographical restrictions. These crimes cannot be deterred by local laws. India in such a scenario is like sitting ducks. India to combat cybercrime has concluded several bilateral agreements, such as a cyber-agreement with Russia and a framework agreement with the United States.

Israel's cyber framework is another effort by India to rationalize its cyberspace. These bilateral agreements have limited scope and are inadequate and ineffective in addressing cybercrime. India needs a multilateral treaty that harmonizes its laws through a common criminal policy and deals with international cooperation to combat cybercrime worldwide. The treaty should help to formulate effective legislation and solid investigative techniques that can foster international cooperation to combat cybercrime. The Budapest Convention on Cybercrime of the Council of Europe is one of those international multilateral treaties that deals with international cooperation to combat cybercrime worldwide. India is expected to sign the convention to combat cybercrime, including the United States and Israel with which India has concluded bilateral agreements to combat cybercrime have joined the Budapest Convention on cybercrime.

FUTURE WORK

We can arrange workshops, free advertisements, public interest with the help of government & NGO'S. The process of acknowledgment about cyber world crimes and cyber illiteracy should be start from grassroots level; institutes, computer centers, schools & individuals.

[16] AIR 1486, 1964 SCR (7) 17
[17] https://www.itlaw.in/judgements/