International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Cyber Crime in India

Divya S R

Reva University, Bangalore, Karnataka, India

Abstract: ***The dissertation concludes that the battle against cybercrime cannot be won without first understanding what cybercrime is. Developing a common understanding of cybercrime and related terminology, the implementation of the necessary Information and Communication Technology (ICT) strategies, policies, and regulatory frameworks, are thus recommended. Concluding international cooperation and mutual assistance agreements to assist with transnational cybercrime investigations and prosecutions is paramount.***

Keywords: Breach, broadband, board of directors, computer crime, conventions, cyber-attack, cybercri, cyber terrorism, cyber espionage, cybersecurity, cyber warfare, cyber crime management, cyber liability

1. Introduction

The United Nations Commission on Trade Law adopted the Model Law on Electronic Commerce in 1996 in order to bring uniformity in the law of different countries. The general assembly of the United Nations by Resolution No.51/162, dated 30th January, 1997, recommended that all the states should give favorable considerations to this Model Law when they enact or revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication, so does the IT Act. It is in consonance with the Model Law. It seeks to remedy most of the problems.

Cyber law is a part of the overall legal system that deals with the internet, cyberspace and their respective legal issues. Cyber law covers various subtopics such as access to internet, usage of the internet, online privacy, regulation cybercrimes, an issue of cyber space jurisdiction, freedom of expression etc.

Cybercrimes can involve traditional criminal activities such as theft, fraud, forgery, defamation, mischief etc. which are subject to the Indian Penal Code. Cyber laws regulate the Cybercrimes. Cybercrimes are those crimes which involve abuse of the computers. Cybercrimes include fraud and identity theft, malware, hacking, defamation, virus attacks, social networking crimes, net extortion and like that.

Cybercrimes have been classified on the basis of the nature and purpose of the offence and have been broadly grouped into three categories depending upon the target of the crimes. It may be against person, property or Government. The Cybercrimes against person include crimes like hate messages, stalking, defamation and transmission of pornographic material. The Cybercrimes involving property include unauthorized computer trespass, vandalism, and transmission of harmful programs and unauthorized computers possession of computerized information. The third category of Cybercrimes target the Governments.

This category of Cybercrime is more popularly called as Cyber terrorism. The comprehensive classification of computer crimes has been given by David L, Carter who classifies computer-related crimes into three broad categories.

a) Where computers is the target of the crimes;
b) Where computer facilitates the commission of crime;
c) Where computer is incidental to the crime.

Cyber Crimes and their Objectives

Objectives of cybercrimes should be formulated in such a way so that it would result into effective prevention and control of cybercrimes. They provide foundation for the cyber security.

These objectives can be summarized as –

- To develop awareness amongst the people about the prevention of cybercrimes.
- To make timely information sharing and action to respond, resolve and recover from cyber attacks.
- To establish a legal and regulatory framework to enable a safe and vibrant cyberspace.
- To develop a culture of cyber security that promotes safe and appropriate use of cyberspace.
- To develop and cultivate national cyber security capabilities.
- To consider and analyze the economic impact of cybercrime on non-ICT sectors.
- To analyze the criminal structures and economics behind cybercrimes.
- To develop solid measures and methods to deter cyber criminals.
- To limit and control the captivation of cyber crimes.

Need for cyber law

Few reasons for the need of cyber law are as –

- Cyber law is needed for regulation of cybercrimes.
- Cyber law is crucial and it is needed to exercise supervision and control on the transactions and behavior on transactions and behavior on and concerning the Internet, the worldwide web and cyberspace.
- Cyber law is vehemently needed as it exercise control over all categories of cybercrimes such as child pornography, cyber harassment, cyber stalking, cyber defamation, e-mail spoofing,
- cracking, SMS spoofing, pornography, frauds, online liable, online slander, cyber smearing, trafficking, financial frauds, identity theft, cyber squatting, cyber trespass, DDOS attacks, worm attacks, hacking,

intellectual property theft, cyber terrorism, cyber welfare, pirated software etc.

- Cyber law is needed to help and protect the people and organizations on the internet from malicious people on Internet.
- Cyber law is needed as it raises specific issues of intellectual property law, contract law, privacy, freedom of expression and cyber jurisdiction.
- Cyber law is needed to protect and maintain the security in online transactions.

2. Components of Cyber Law

It is difficult to answer this question that what are various components of cyber law because it is a debatable concept. Many jurists believe that as cyber law is to create order in cyber space therefore every branch of law dealing with cyber space would be covered under the components of cyber law. After the advent of information and communication technologies we have various new concepts such as E-commerce, E-governance,

E-contract, E-transaction, Cybercrimes, IPRs in digital medium and so on. Therefore laws dealing with computer, internet and with these various new concepts would be covered under components of cyber law. Further, telecommunication is very important aspect of Information and Communication Technologies affecting cyber space, therefore, telecommunication regulations would also be covered under this net.

Apart from this, cyber space also has impact on various conventional areas of laws such as Criminal Law, Business Law, Taxation Law, Banking Law, Financial Law, Consumer protection Law, Contract Law, Tort Law, International Law, Health Care, Security Law and so on. At international level, we have two main laws dealing with these new concepts i. t. the Model Law on e-commerce and Model Law on Electronic signature.

Another aspect of cyber law that was examined was intellectual property in cyber world. The major traditional means of protecting intellectual property were explained and their relevance in cyber world was outlined.

In particular, the system of domain names protection and trademark protection were compared and the application of copyright to computer programs was examined. Therefore various issues discussed were:

1) The implementation of a public key infrastructure for secure transacting and identification;
2) Issues of national security vis-a-vis human rights, in particular the right to privacy;
3) The issue of deciding which jurisdiction's laws apply and country's courts are competent is cases of contestation arising from electronically concluded agreements or electronically supplied services;
4) The increased relevance of inter-country cooperation in general and extradition arrangements in particular in the context of increased trans-border infringements brought about through ICTs;
5) Electronic evidence (E-evidence);
6) Issues arising from ICTs applications to taxation, trademarks, copyright, and other digital rights;

Indian Position

In India, most of the new concepts like E-commerce, E-governance,
E-record, Digital Signature and Electronic Signature are covered under the Information Technology act, 2000 which is in tune with Model Law on

E-commerce, 1996. Further it was amended by the Information Technology Act, 2008 so as to make Indian Law in tune with the model law on Electronic signature (2001).

However, for proper implementation of the Information Technology act, 2000 either certain amendments were made in some conventional laws such as Indian Penal Code, 1860, Indian Evidence Act, 1891, Reserve Bank of India, 1934, Banker's Book Evidence act, 1891, Negotiable Instrument Act, 1881 or wider interpretation is given to others. Let's briefly analyze the need for amendment of various conventional laws or wider interpretation of others:

Amendment of some conventional laws –

1) Amendment of the Indian Evidence Act, 1872:

Before amendment, there were only two evidences legally recognized under the Indian Evidence Act, 1872 i. e. oral evidence and documentary evidence. Electronic record was not legally recognized and was not accepted as evidence. Therefore amendment was made in Indian Evidence Act, 1872 to grant legal recognition to electronic record so that it can be accepted as evidence.

2) Amendment of The Indian Penal Code, 1860:

Under conventional law, offences could be committed against the documents. However, electronic record was not within the purview of Indian Penal Code and hence no offence against electronic record was recognized. However, after the amendment when legal recognition was granted to electronic record, new offences against electronic record were also bought within the purview of Indian Penal Code.

3) Amendment of The Reserve Bank of India Act, 1934:

Before the amendment, electronic fund transfer between the financial institutions was not legally recognized. Therefore, the Reserve Bank of India act, 1934 was amended so as to grant legal recognition and to facilitate electronic fund transfer between the financial institutions; and

4) Amendment of The Bankers Books Evidence Act, 1891;

Under the conventional law E-books of accounts were not legally recognized, therefore, the Banker's Books Evidence act, 1891 was amended so to give legal sanctity for books of accounts maintained in the electronic form by the banks.

Wider interpretation of other Conventional Laws –

1) The Consumer Protection Act, 1896.
2) The Indian Contract Act, 1872.
3) Law of Torts.
4) E-commerce and Taxation Las.
5) Copyright and Patent Law.
6) Trademarks and Domain Names and Law.
7) Law and Cyber Jurisdiction.
8) Privacy issue and Law.

Cyber laws in India

India has laws against cybercrime, which is any crime committed using technology and a computer as a tool. Citizens are prevented from sharing private information with strangers online by cybercrimes laws. The It Act, 2000 which was passed and revised in 2008 to cover many types of offences under Indian cyber law, has been in effect since the establishment of cyber laws in India.

- Internet law and regulation are collectively referred to as "cyber law" in this context. Cyber laws cover anything that has to do with, is connected to, or results from legal matters or any citizen activity in cyberspace.
- Legal issues relating to the usage of network information technology and devices, distributive, transactional, and communicative features are covered by cyber law. It covers all of the laws, regulations, and constitutional clauses that apply to networks and computers. The Act defines the various types of cybercrime and the penalties associated with them.

Advantages of Cyber Laws

- Utilizing the legal framework, the Act, provides, businesses can now conduct E-commerce.
- In the Act, digital signatures have been legitimacy and authorization.
- It has made it possible for corporate organizations to issue digital signature certificates and operate as certifying authorities.
- It paves the way for e-government by enabling the government to publish alerts online.
- It allows business or organizations to electronically submit any forms, applications, or other documents to any offices, authorities, bodies, or agencies that are owned or managed by the appropriate government using any e-forms that may be specified by that government.
- The IT Act also addresses the crucial security concerns that are essential to the success of electronic transaction.

Classification of Cybercrimes

Cybercrimes can be categorized into two categories

1) Crimes that target computer networks or devices. These types of crimes include viruses and denial of services attacks.
2) Crimes that use computer networks to advance other criminal activities.

These types of crimes include cyber stalking, phishing and fraud or identity theft.

Alternate Classification

Major types of cybercrimes can be classified as-

- Hacking
- Cyber stalking
- Online identity theft and credit card fraud
- Online child abuse
- Ransom ware attack
- Internet fraud (online scam)
- Virus Dissemination
- Logic Bombs
- Denial of Service attack
- Phishing
- E-mail bombing and spamming
- Data diddling
- Web Jacking
- Salami skiing attack
- Software Piracy etc.

Causes of Cyber Crimes / reasons for cybercrimes are as discussed below –

- Computer systems are easy to access. It makes unauthorized access to the computer system very easy. Hackers can steal information easily and bypass firewalls. Easy access to the computer systems and the internet is one of the major causes of cybercrimes.
- The computer has a capacity to store data in comparatively in a very small place which makes the people very easy to steal data and to use it for own benefit. It is another reason for the cybercrimes.
- Errors in programming and security systems of the computer lead to the commission of cybercrimes with ease.
- Negligence in protecting the computer system provides a cyber criminal the access and control over the computer system.
- Loss of evidence has become very common and obvious problem which encourages for the commission of cybercrimes.
- One of the causes of cybercrimes is that in a case pf reported cybercrimes, arrest rates are very low.
- Low rate of conviction is one of the reasons for cybercrimes as there is a very low risk of prosecution.
- Cybercrimes are very easy to commit. Hence these crimes are committed frequently.

Measures to combat cybercrimes

Measures to combat cybercrimes can be categorized into following categories.

- Technological measures/ technological prevention

- Soft prevention
- Personal measures
- Legal measures
- Measures to be taken by the corporate

Problems of investigating agency –

a) Hiding, spoofing, re-mailers and remote storage.
b) Lack of skilled investigators.
c) On-line investigations.
d) Liaisons with the Internet industry.
e) Forensic computing.
f) Co-operation.

3. Conclusion

People are becoming more and more dependent on the Internet which means that criminal activities will also keep on increasing. The laws making bodies of the nation should always keep in mind the rate to development of the cybercrimes and the laws should be able to minimize them to best possible extent. Thus, it is responsibility of the government and the law makers to make sure that every perspective and issues of cybercrime have been included in the cyber laws which enable the consistent and lively growth of the laws.