ISSN: 2456–5474 RNI No.UPBIL/2016/68367 Vol.-5* Issue-12* January- 2021
Innovation The Research Concept

Cyber Crime Prevention and Control in India

Paper Submission: 15/01/2021, Date of Acceptance: 26/01/2021, Date of Publication: 27/01/2021

Neha
Research Scholar,
Dept. of Laws,
BPS Women University,
Khanpur, Kalan, Sonipat,
Haryana, India

Abstract

Cyber crime occurs in India as a social problem, as a real threat. The generation of today is an inescapable penetration in PC innovation and communication that is on the road for generations to rise. As the product creates an affix to it, cyber-misrepresentation increases in demand to get the greatest benefit from it. Although the Information Technology Act was passed in 2000, it was later revised to reduce and add regulation over cyber-misconduct in 2008. In any case, the challenges to innovation are growing considerably after 17 years due to huge growth. To deter cyber criminals from committing a wrongdoing, it is crucial for warriors that individuals who condemn the cyber wrongdoing have to predict the qualitative and quantitative improvements such that no attempt at wrongdoing can occur.

Keywords: Cyber Crime, Communication, Technology, innovation

Introduction

Social orders are gradually being transformed into Knowledge Societies in the 21st century, and their occupants into Knowledge Networkers who are increasingly educated about neighborhood and worldwide occasions. Their activities depend on the strong establishment of all-inclusive, objective, auspicious information, and from various sources. Individuals are becoming ever more aware of their privileges and their openings. But computer, internet, and information technology bring this revolutionary shift. In reality, the way individuals communicate and connect around the globe has changed drastically in the information society of the 21st Century due to globalization and e-revolution the paper-based communication of earlier times is quickly replaced by electronic communication. That has prompted the legislature and business to work in new ways. (Justice T. Ch. Surya Rao, 2004)

The rapid growth on information technology is encompassing all walks of life in present generation. Such technological advancements enabled the possible transition from report to paperless contact. Whereas PC is intended to store special political, social, economic data which brings gigantic benefits to the general public. Globally, the broad expansion of an Internet and Computer invention has caused Internet-related wrongdoings to intensify. India has recently become a big spot for cybercriminals, who perpetrate misdeeds on the internet through most hackers and numerous malicious clients. As there are different types of cyber violations these misdeeds are rising at an alarming pace. India ranks fifth among various nations in cyber wrongdoing.

Objective of the Study

1. To understand cyber world basic concepts.
1. To trace the cyber crimes origin and evolution.
2. To find out about the international efforts to curb cyber threats.
3. To point out possible flaws and loopholes in existing cyber-crime laws.

Review of Litreture

Dr. M. Dasgupta has concisely characterized the significance, nature, extension, highlights and components of cybercrime in his book "Cyber Crime in India: A Comparative Study" he said, Noting the scope of cyber-crimes, "It is very important to stress that the world is no longer run by weapons, energy, or money. It is run by some and zeros.... little data bits.... it is all electrons. There is a war here out, a war in the world. It's not who gets the most bullets about. It's about who controls the information–what we see and hear, how we work, what we think, and so on. It's all about information."(Id. at p. 8) He also investigated the normal technique of

several major cybercrimes, such as cyber hacking, cyber-psychological exploitation, cyber-sex entertainment, cyber-extortion, and so on, and also Communicated the national and universal efforts to avoid and monitor such cyber wrongdoing.

S.K. Verma and Raman Mittal in their book "Legal Dimensions of Cyber Space" Explained the basic concepts of the virtual environment, such as the purpose, forms, characteristics and key components of PCs; Internet history and improvement; Internet benefits and limitations; various PC pollutants, such as viruses, worms, Trojans, etc. Emphasizing the role of PCs and the Internet in their everyday activities, they have shared their opinion that "today it affects almost every part of our lives and influences them.

Research Methodology

The research procedure shifts as the subject has indicated. That review is doctrinal in nature. There was an effort to do a close investigation of the cyber laws of different nations. This monograph is an effort to gain a world-view on cyber crimes by examining a universal way of dealing with them. The content was selected from UK, United States of America, and Indian courts. The specific knowledge was taken from the instances chosen by the United Kingdom's High Court and House of Lords, U.S. District Court, U.S. Court of Appeal, U.S. Preeminent Court, and India's High Court and Supreme Court.

What is Cyber Crime?

As the use of internet is increasing, a new face of crime is spreading rapidly from in-person crime to nameless and faceless crimes involving computers. Cyber crime includes all unauthorized access of information and break security like privacy, password, etc. with the use of internet. Cyber crimes also includes criminal activities performed by the use of computers like virus attacks, financial crimes, sale of illegal articles, pornography, online gambling, e-mail spamming, cyber phishing, cyber stalking, unauthorized access to computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system, etc.

Evolution of Cyber Crime

The most thorough cybercrime came with the introduction of "Loom," a gadget developed in 1820 by a material manufacturer called "Joseph-Marie Jacquard," which used to allow steps to be reused for weaving fabrics that threatened representatives with their traditional work and employment. As a result they submitted counterattack to demoralize the further use of the invention. Cybercrime includes, for example, conventional criminal activities such as counterfeiting, theft, robbery, underhandedness, and slander, as well as web defacing, hacking, web jacking, and cyber stalking which have progressed due to Software misuse.

Online Cyber Crimes in India

We find many products on TV and Internet promoted by popular celebrities as its brand ambassador. There are many hoardings at every street corner and advertisement for products. The name of products is constantly hammering every one's mind. Think, what may happen if product is not seen in market.

It is also true for service segments. Despite of making product demand again and again, when product is not reaching the customer, people will drop their demand and may forget products. Same thing is happening with cyber crimes in India.

India is Second largest market in world for smart phone. India is at second place regarding face book users and thirty million twitter users. Whatsapp users are around one million. It is expected that in next one year, mobile internet users will be three hundred twenty million and total internet users shall be five hundred million (Gujarat Samachar, 2016). We have large network of users but we just have only twenty three cyber crime cell. As per government National Crime Bureau report, there were 9,600 cases reported in year 2014. Unofficial sources indicate that it is beyond 3 lacs. It is unfortunate that government policy to use cyber crime cell to assist police to solve criminal cases. Thus it often kills basic purpose of this cell. Let us assume that average staff in a cell is 50 then there are 1000 – 1100 people in entire India. Because of internet users are many and limited people in cyber cell, we find that there are lacs of online cyber criminals which are out of control.

Information Technology Act, 2000 and Information Technology Amendment Act 2008

In the digital world of the 21st century, Computer, twitter, and ICT or e-turmoil have changed the way of life for individuals. E-mail correspondence, paper-based exchange with Internet-based business and paper-based e-administration has been replaced by paper-based correspondence today. We have new terminologies such as cyber world, netizens, e-transaction, e-banking, e-return, and e-contracts, accordingly. Besides the positive side of the e-revolution, there is also a seamy side as a computer; in the hands of criminals, internet and ICT have become an offense weapon Likewise, a further piece of legislation was developed to tackle cybercrime problems in cyber space, such as cyber law or computer space law or the law on technology creation or Internet law. (Justice A.S. Anand-', 2001) The United Nations Commission for International Trade and Law (UNCITRAL) first adopted a Model Law on E-Commerce in 1996. It was further adopted by the United Nations General Assembly on 31 January 1997, by passing a resolution. Moreover, India was also a signatory to this Model Law and, under that Model Law, had to revert to its national legislation. In this way, India enacted the Information Technology Act, 2000 and it was amended by the Information Technology (Amendment) Act, 2008 as from late.

Offences under the It Act, 2000

The Researcher has critically analysed the statutory provisions related to cyber offences and their prevention, compensation and adjudication in this chapter. The following sections under the Information Technology Act, 2000 has deals with the offences –

1. Penalty and compensation for damage to computer, computer, etc. (Section 43)
2. Compensation for data protection failure. (Section 43A of the IT Act, 2000)

3. Penalty for failure to provide, return and so on (Section 44 of the IT Act, 2000)Residuary penalty. (Section 45 of the IT Act, 2000)
4. Power to adjudicate. (Section 46 of the IT Act, 2000)
5. Factors to be taken into account by the adjudicating officer. (Section 47 of the IT Act, 2000)
6. Tampering with source documents for computers. (Clause 65 of the IT Act, 2000)
7. Computer related offences.(Section 66 of the IT Act, 2000)
8. Punishment for sending offensive messages via a communication service, etc. (Section 66A of the IT Act, 2000)

Aims and Objectives of Information Technology Act, 2000

The main objectives and goals of the IT Act, 2000 were to:

1. Providing legal recognition of electronic records and digital signatures.
2. Providing legal recognition of business contacts and creating rights and obligations via electronic media;
3. To facilitate e-governance and to encourage the use and acceptance in government offices and agencies of electronic records and digital signatures. This would also make the interaction between citizens and government more hassle-free.
4. Establish a regulatory body to supervise the issuing of digital signature certificates by certifying authorities.
5. To legislate in accordance with the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the United Nations General Assembly.

Conclusion

Cybercrime, which is of a worldwide character, mostly influences the individual a long way from the scene of the offense, whether in a similar nation or in another nation. So it requires global policing just as the worldwide network's dynamic involvement. The European Convention on Cybercrime (Effective from June 2001) was a highly commendable undertaking, since it sets expectations for Member States to lead in the fight against cybercrime. The Convention proposed measures for States to begin reconstruction of their digital laws to cope with the new challenges. In addition to dealing with the improvements and amendments in the substantive aspect of criminal law, the Convention also referred to the procedural point of view that must be taken into account in the reproduction of existing law in the implementation in order to satisfy the new development needs.

References

1. *"Investigators Feel the Heat as Cyber Crimes on the Rise", The Pioneer, February22, 2010*
2. *20 Id.*
3. *A & M Records Inc v. Napster Inc, 114 F. Supp 2d 896(N.D. Cal 2000)*
4. *A concept in copyright law that allows limited use of copyright material without requiring permission from the rights holders, eg, for scholarship or review, education, research etc*
5. *A.S.A Krishnan and A.K. Chakravarti, "Intellectual Property Rights in the Ensuing Global Digital Economy", available at www.mit.gov.in*
6. *Ahmed Farooq, Cyber Law in India – Law on Internet, 2005.*
7. *Chetan Srivastava, Fundamentals of Information Technology, 2000*
8. *Christopher, R. Perry, "Trademarks as Commodities: The Famous Road Block to Applying Trademark Dilution Law in Cyberspace", Connecticut Law Review, 2000; p. 1127.*
9. *Pearson, Introduction to Information Technology, 2006, p. 189.*
10. *Rodney D. Ryder, Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection and the Internet), Wadhwa Publication, 2001*
11. *S.K. Verma and Raman Mittal, Legal Dimensions of Cyber Space, Indian Law Institute Publication, 2004*
12. *Saroj Mehta & Vikram Singh A study of awareness about cyber laws in the Indian society - ISSN (Online):2229-6166 Volume 4 Issue 1 January*