Journal of Advances and Scholarly Researches in Allied Education
Vol. XIV, Issue No. 2, January-2018, ISSN 2230-7540

The Effectiveness of Cyber Crime Law Policing System

Navpreet Kaur[1]* Yogesh Sharma[2]

[1]Research Scholar, Computer Science, JJT University, Jhunjhunu, Rajasthan

[2]Associate Professor, Computer Science, JJT University, Jhunjhunu, Rajasthan

Abstract – The merging of computer system and data communications encouraged by the computerized technologies has brought forth a typical space called 'the internet'. This the internet has turned into a stage for a system of human activities which merge on the web. The internet has, truth be told, turned into the most happening place today. Web is progressively being utilized for correspondence, business, promoting, saving money, instruction, research and diversion. There is not really any human movement that isn't touched by the web. Along these lines, Internet has a comment to everyone and in the process it just increments and never lessens. The 'digital manthan' has presented many endowments to mankind yet they accompany startling entanglements. It has turned into a place to do all kind of activities which are denied by law.

Keywords: Cybercrimes, Cyber law, Internet, Phising.

----------X----------

1. INTRODUCTION

Crime is both a social and economic phenomenon. It is as old as human society. Many ancient books right from pre-historic days, and mythological stories have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Kautilya's Arthashastra written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offences. Different kinds of punishments have been prescribed for listed offences and the concept of restoration of loss to the victims has also been discussed in it. Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration, up to the lowest level of petty shop keepers computerizing their billing system, we find computers and other electronic devices pervading the human life. The penetration is so deep that man cannot spend a day without computers or a mobile. Snatching some one's mobile will tantamount to dumping one in solitary confinement! Cyber Crime is not defined in Information Technology Act 2000 or in the I.T. Amendment Act 2008 or in any other legislation in India. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber-crime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offence or crime in which a computer is used is a cyber-crime'. Interestingly even a petty offence like stealing or pick-pocket can be brought within the broader purview of cyber-crime if the basic data or aid to such an offence is a computer or an information stored in a computer used (or misused) by the fraudster. The I.T. Act defines a computer, computer network, data, information and all other necessary ingredients that form part of a cyber-crime, about which we will now be discussing in detail. In a cyber-crime, computer or the data itself the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence, all such acts of crime will come under the broader definition of cyber-crime.

Let us now discuss in detail, the Information Technology Act -2000 and the I.T. Amendment Act 2008 in general and with particular reference to banking and financial sector related transactions. Before going into the section-wise or chapter-wise description of various provisions of the Act, let us discuss the history behind such a legislation in India, the circumstances under which the Act was

passed and the purpose or objectives in passing it. The Genesis of IT legislation in India: Mid 90's saw an impetus in globalization and computerisation, with more and more nations computerizing their governance, and e-commerce seeing an enormous growth. Until then, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidences and records, until then, were predominantly paper evidences and paper records or other forms of hard-copies only. With much of international trade being done through electronic communication and with email gaining momentum, an urgent and imminent need was felt for recognizing electronic records ie the data what is stored in a computer or an external storage attached thereto. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record. Objectives of I.T. legislation in India: . It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself. "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication 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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000. The Act essentially deals with the following issues: Legal Recognition of Electronic Documents Legal Recognition of Digital Signatures Offenses and Contraventions Justice Dispensation Systems for cyber-crimes.

2. REVIEW OF LITERATURE:

Goodman, (2001), the prominent issues found in the ways PC crime and PC blackmail are starting at now had a tendency to are far reaching in range and address the two issues of law execution workplaces and external considerations. The most essential issue raised in the composition regards the nonappearance of a uniform definition for both PC crime and PC deception. As was in advance stated, the nonappearance of a uniform way to deal with portrays what constitutes a PC crime makes usage troublesome. Moreover, without a uniform definition, the veritable degree and nature of the PC crime and blackmail designs can't be reviewed, which furthermore speaks to a further test for workplaces as they choose their staffing and resource needs concerning PC crime issues.

Brette, Olivier (2003), T.Veblen and Karl Marx have been called as determinists. Marx was financial determinist (since he assumed that every social change came on account of advance in the techniques for age), Veblen assumed that each and every social change come in view of changes in development. Since he has laid weight on advancement, Veblen has been called as "Techno – Logical Determinist". Advancement alone changes even the penchants for the all-inclusive community from one point of view and material conditions on the others. He in like manner assumed that material circumstances are continually hinting at change and every individual needs to alter him to those movements. There are also changes in penchants, examinations and social relationship on account of mechanical changes.

Schell and Martin(2004) described cybercrime as a crime related to advancement, PCs and the web and it concerns governments, organizations and subjects worldwide where cybercrime shows up as either burglary, phreaking (getting free telephone calls), cyber stalking, cyber terrorism and cyber pornography.

PBS (2001), Aside from definitional issues, law prerequisite also faces a jurisdictional test. PC crime and coercion consistently incorporate intersection breaking points and edges not seen in ordinary infringement. This speaks to another game plan of challenges for state and close-by workplaces as they fight to explore cases that consistently take them outside of their area. As one source states, While most law usage has genuinely been left to the states, states are ineffectively outfitted to deal with the extraterritoriality of PC crime. State law usage associations can't execute court orders, subpoena witnesses, or make catches past their own edges. However PC crimes are barely anytime restricted to a specific zone since computerized crime is an as of late amassed field creating in advanced laws, there is emphatically no broad law on advanced crime wherever on the planet. This is effectively the inspiration driving why inspecting associations are finding the web significantly difficult to manage. The diverse advanced infringement fall inside the ambit of Internet law that is neither totally nor to some degree secured by the present laws or more all that too in a couple of countries. India woke up to the Cyber reality, fairly late in the day, and brought into drive the IT (Information Technology) Act, 2000, which gets its help from UNCITRAL's (United Nations reward on International Trade Laws) Model law on web business. An UN General Assembly assurance in 1997 pushed the determination of

UNCITRAL Model Law in the area laws of part countries to keep up consistency before long.

Das and Nayak (2013) gave a proficient cognizance of advanced infringement and their belongings over various domains like Soci-eco-political, customer trust, youngster and so forth with the future examples of computerized crimes are cleared up.

Singh and Geeta (2013) cleared up that PC crime uncommonly affects the world in which we live. It impacts every individual paying little heed to where they are from. Ironicly the people who in secret break into PCs over the world for joy have been set apart as variation from the norm. Various software engineers see the Internet as open space for everyone and don't see their activities as criminal. Developers are as old as the Internet and many have been instrumental in making the Internet what it is as of now. In my view point hacking and PC crime will be with us for whatever time allotment that we have the Internet.

Jaishankar (2007) proposed "Space Transition Theory" It clears up the lead of the general population who draw out their changing and non-adjusting conduct in the physical space and virtual space. Virtual space gives an individual such space where he can express his feelings and even vent out his stun against anyone. Advanced stalking and Cyber defaming are situations where miscreants use online space in perspective of its lack of clarity and extensive approach. It moreover battles that people demonstration particularly when they move beginning with one space then onto the following.

Kshetri (2010) According to him, "Advanced Crime is portrayed as a criminal activity in which PCs or PC frameworks are the fundamental strategies for executing an offense or manhandling laws, rules or headings".

The business needs to oversee trial of advanced crime and to ensure information secret in the matter of information dealing with industry. Nasscom president Dr. Kiran ensured the PM that in India information getting ready industry is totally devoted to answer the most vital checks of information security. The head overseer has requested the division from Information Technology and Nasscom to guide all accomplices and propose changes in existing law. If found fundamental, to ensure that any burst of riddle, some other sort of computerized crime is made a guilty offense, Nasscom is building a database for all delegates in the BPO business to ensure that there is tasteful quality assertion. It was similarly urged to guide getting ready class to spread regard for best practices in information and framework security among part associations.

Goyal (2012), Discussed about the various ethics of computerized crime. The ethics incorporate business ethics, legal ethics, bioethics, restorative ethics, building ethics, and PC ethics have bounced up. Which are proposed to take a gander at the consequences of good measures and practices in all circles of human development on our lives. Computerized crime is ascending as a certifiable hazard. General governments, police divisions and understanding units have started to react and constrained to set laws against these crimes.

Sharma (2012), Cyber security is the development of guaranteeing information and information structures with fitting frameworks and specific wellbeing endeavors. Antivirus programming, firewalls and other mechanical responses for protecting individual information and PC frameworks are key however not sufficient to ensure security. As our nation rapidly collecting its Cyber-Infrastructure, Digital Ethics, Cyber-Safety, and Cyber-Security issues ought to be facilitated in the guideline. Wellbeing endeavors help ensure the arrangement, availability, and uprightness of information systems by keeping or assuaging asset mishaps from Cyber security strikes. Starting late computerized security has ascended as a developed instruct for PC structures and establishments with a consideration on protection of imperative information set away on those systems from the people who need to get, worsen, hurt, obliterate or refuse get to.

Prasanthi and Ishwarya, (2015) inspected about Cyber-crime and computerized security and particular advanced infringement that keep running over and repugnance techniques and area methodology, for instance, Tripwires, setup checking instruments, Honey Pots, irregularity ID system and working structure orders.

3. EXAMINATION OF INDIAN CYBER LAWS AND POLICING SYSTEM

Noted computerized law ace in the nation and Supreme Court advocate Shri Pavan Duggal, "While the authorities must be supplemented for their respectable work emptying distinctive insufficiencies in the Indian Cyber law and making it imaginatively impartial, yet it gives there has been a critical puzzle between the want of the nation and the resultant effect of the changed establishment. The most odd and startling piece of the new changes is that these modifications attempt to make the Indian advanced law a Cybercrimes welcoming authorization; – a sanctioning that goes to an awesome degree fragile on computerized offenders, with a sensitive heart; an establishment that engages advanced convicts by decreasing the quantum of discipline agreed to them under the

present law; … .. an establishment which makes a bigger piece of cybercrimes stipulated under the IT Act as bailable offenses; an order that is most likely going to clear course for India to twist up evidently the potential Cybercrimes capital of the world… … "

Let us not be important that the present institution is computerized criminal friendly or gets ready to extend infringement. Totally, it doesn't. It is a magnificent piece of authorization, a memorable point beginning advance and an extraordinary defining moment in the mechanical improvement of the nation. Regardless, let us not be pompous that the present law would take care of business. Allow us to recall that the law breakers reliably go speedier than the inspectors and constantly endeavor to be one phase ahead in innovation.

There are a couple of stipulations in IT Act as:-

- The hustle, in which the establishment was passed, without sufficient open common contention, did not by any methods fill the desired need. Authorities are of the appraisal that one explanation behind the lack of the sanctioning has been the surge in which it was passed by the parliament and it is furthermore a reality that satisfactory time was not given for open common contention. Nevertheless, various issues of the exhibit were modified by the adjusted show of 2008. (Lane, 2001).

- **Uniform law**

Mr. Vinod Kumar holds the supposition that the need of incredible significance is a general uniform computerized law to fight Cyber-crimes. Cybercrimes is an overall ponder and in this way the movement to fight it ought to begin from a comparative level.

- **Lack of care**

The Act of 2000 isn't gaining completed ground because of the nonappearance of care among the larger part about their rights. Help most of the cases are going unreported. In case select the overall public are careful about their rights, can the law guarantee their rights.

- **Raising a computerized furnished power**

There is a necessity for an especially arranged group to deal with the new examples of hello tech wrongdoing. The lawmaking body has taken a bounce toward this way by constituting Cybercrimes cells in all metropolitan and other basic urban groups. Encourage the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI).

- **Cyber canny seat**

Computerized adroit judges are the need of the day. Lawful accept a basic part in framing the establishment as demonstrated by the demand of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerala High Court has recognized through an email.

- **Dynamic kind of Cybercrimes**

Chatting on the dynamic thought of Cybercrimes FBI Director Louis Freeh has expressed, "essentially, regardless of the way that we have particularly improved our capacities to fight computerized intrusions the issue is ending up significantly speedier and we are falling further behind." The (de)creativity of human identity can't be checked by any law. In this way the primary way out is the liberal advancement while applying the statutory courses of action to Cybercrimes cases.

- **Hesitation to report offenses**

As communicated more than one of the fatal drawbacks of the Act has been the cases going unreported. One clear reason is the non-pleasing police oblige. "The police are a serious power today which can accept an instrumental part in foreseeing cybercrime. Meanwhile, it can in like manner end up utilizing the bar and bugging innocents, shielding them from moving toward their ordinary computerized business." For complete affirmation of the game plans of this Act a supportive police compel is required (Schell, & Martin, 2004).

Beside these escape conditions and issues the present kind of police system and many police experts are not familiar with the digital wrongdoings and they require getting ready to be OK with the "Standard technique" of Cybercrimes s however the current germane act is careful establishment yet from the judicious point of view there are a couple of deficiencies in the errant sort of the showing. It is the need of awesome significance that the capability of police system at all positions should be updated similar to Cybercrimes s. The obscene, destructive identities of criminals take central purposes of inefficient police structure.

Both seat and Bar should comprehend the level of advanced infringement. They should familiarize themselves with the complexities of computerized law, else they would find it enormously difficult to oversee Cybercrimes cases.

CONCLUSION:

Cyber law is imperative since it touches all parts of exchanges and activities on and concerning the Internet, the World Wide Web and Cyberspace. At

first it might appear that a Cyber law is an exceptionally specialized field and that it doesn't have any bearing to most activities in Cyberspace. In any case, the genuine truth is that nothing could be more remote than reality. Regardless of whether we understand it or not, each activity and each response in Cyberspace has some legitimate and Cyber legal points of view.

As the idea of Internet is changing and this new medium is being viewed as a definitive medium at any point developed in mankind's history, each movement of yours in Cyberspace can and will have a Cyber legal viewpoint. From the time you enroll your Domain Name, to the time you set up your site, to the time you advance your site, to the time when you send and get messages, to the time you lead electronic trade exchanges on the said site, at each purpose of time, there are different Cyber law issues included. You may not be made a big deal about these issues today since you may feel that they are exceptionally far off from you and that they don't affect your Cyber activities. Be that as it may, at some point or another, you should fix your belts and observe Cyber law for your own particular advantage.

REFERENCES:

Brette, Olivier (2003). "Thorstein Veblen's Theory of Institutional Change: Beyond Technological Determinism". European Journal of the History of Economic Thought, Vol 10(3), pp. 455–477.

Cameron S. D. Brown (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology Vol. 9 Issue 1 January – June 2015

Das, S. & Nayak, T. (2013). International Journal of Engineering Sciences & Emerging Technologies, October 2013.

Denning, Dorothy E.R. (1999). Information Warfare and Security, Pg.166, Addison Wesley, Indian Reprint.

Goyal (2012). Ethics And Cyber Crime In India, International Journal Of Engineering And Management Research, Vol.2, Issue-1, Pages 1-3

http://www.legalservicesindia.com/article/article/issue-of-jurisdiction-in-combating-cyber-crimes-issues-and-challenges-pornography-and-indian-jurisdiction-1386-1.html
http://perry4law.org/cecsrdi/?p=302

Jaishanksr K. (2007). Establishing a Theory of Cyber Crime, Pg 7-9 International Journal of Cyber Criminology ,Vol 1 Issue 2.

Kshetri, Nir (2010). The Global Cybercrime Industry, Pg 3, Springer, New York.

Lane, F. (2001). Obscene Profits : The Enterpreneurs of Pornography in the Cyber Age ,pg. 66, Routledge, London

N. Leontiadis, T. Moore, and N. Christin (2011). “Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade”. In Proceedings of USENIX Security 2011, San Francisco, CA, August 2011.

Narinder Singh and Moirangmayum Sanjeev (2014). International Journal of Social Science & interdiscipilinary research, Jan 2014, ISSN 22773630

Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.

Ompal, Tarun Pandey and Bashir Alam (2017). How to report cyber-crimes in indian territory International Journal of Science Technologies and Mangement, Vol. 6 issue no 4, April 2017

Prasanthi and Ishwarya (2015). Cyber Crime: Prevention & Detection, International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue 3

Rajarshi Rai Choudhury, Somnath Basak, Digbijay Guha (2013). Cyber Crimes- Challenges & Solutions, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (5), pp. 729-732

Salkever (2003). “‘Phishing’ Is Foul on the Net,” Business Week Online, 21 Oct. 2003

Schell, B. & Martin C. (2004). “Cybercrime: A Reference Handbook”. Santa Barbara: ABC-CLIO.

Sharma (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6.

Singh & Geeta (2011). Cyber-crime- A threat to persons, property government and societies, International journal of advanced

research in computer science and software engineering,

Steel.C. (2006), Windows Forensics: The Field Guide for Corporate computer Investigations, Wiley.

The Hindu, India's National Magazine, Volume 18 - Issue 16, Aug. 04 - 17, 2001

Thomas, Douglas and Loader Brian (2000). Cybercrime Law Enforcement, Security and Surveillance in the Information Age, Pg 8, Routledge, London.

Williams, P. (2002). Organized crime and cyber-crime: implications on business. Retrieved June 27, 2009, from http://www.cert.org/archive/pdf/cybercrimebusiness.pdf

Yougal Joshi and Anand Singh (2013). A Study on Cyber Crime and Security Scenario in INDIA, International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013 ISSN No.: 2250-0758

Corresponding Author

Navpreet Kaur*

Research Scholar, Computer Science, JJT University, Jhunjhunu, Rajasthan

E-Mail – virk.navpreet@gmail.com