ISSN 2278-8808
An International Peer Reviewed
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

A Study of Cyber Crimes & Cyber Laws In India

PARDEEP MITTAL

Professer, Guru Kashi University, Talwandi Sabo, Punjab, India

&

AMANDEEP SINGH

(Research Scholar), Guru Kashi University, Talwandi Sabo, Punjab, India

Abstract

Today's in techno-savvy environment, the world is becoming more and more digitally sophisticated. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum. in this research paper introduction about various cyber crimes, their classifications, IT-Act 2000 and the methods to registered the complaints has been included for the effective implementation of cyber laws in India and to aware the common men to registered their complaints when they suffered any cyber crime.

Key words:- *Cyber Crimes, Cyber laws, IT-Act., Penalties and Offences,*

I. Introduction

Day by day the use of computer is increasingly & more users are connecting to the internet. So the crimes are also increasing. But mostly peoples are unaware about cyber crimes. Although the term cybercrime is usually restricted to describing criminal activity in which the computer or network is an essential part of the crime. Cyber Crimes are defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication

networks such as Internet (Chat rooms, emails,) and mobile phones (SMS/MMS)".Such new crimes devoted to the Internet are email “phishing”, hijacking domain names, virus imitation, and cyber vandalism.

Cyber crimes actually means: It could be hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. It can also include ‘denial of services’ and viruses attacks preventing regular traffic from reaching your site. Cyber crimes are not limited to outsiders except in case of viruses and with respect to security related cyber crimes that usually done by the employees of particular company who can easily access the password and data storage of the company for their benefits. Cyber crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.

II. Classifications of cyber crimes: Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber crime and what is the conventional crime so to come out of this confusion, cyber crimes can be classified under different categories which are as follows:

Cyber crimes against Persons:

- **Harassment via E-Mails**: It is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Face book, Twitter etc. increasing day by day.
- **Cyber-Stalking:** It means expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.
- **Dissemination of Obscene Material:** It includes Indecent exposure/ Pornography (basically child pornography), hosting of web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind.
- **Defamation:** It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.
- **Hacking:** It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programmers. Hackers usually hacks telecommunication and mobile network.
- **Cracking:** It is amongst the gravest cyber crimes known till date. It is a dreadful feeling to know that a stranger has broken into your computer

systems without your knowledge and consent and has tampered with precious confidential data and information.

- **E-Mail Spoofing:** A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.
- **SMS Spoofing:** Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.
- **Carding:** It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always unauthorized use of ATM cards in this type of cyber crimes.
- **Cheating & Fraud:** It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.
- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.
- **Assault by Threat:** refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

Cyber crimes against persons/property:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- **Intellectual Property Crimes:** Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.
- **Cyber Squatting:** It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.
- **Cyber Vandalism:** Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.
- **Hacking Computer System:** Hacktivism attacks those included Famous Twitter, blogging platform by unauthorized access/control over the

computer. Due to the hacking activity there will be loss of data as well as computer. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

- **Transmitting Virus:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks plays major role in affecting the computerize system of the individuals.
- **Cyber Trespass:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuse, or damage data or system by using wireless internet connection.
- **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

Cyber crimes against government:

There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

- **Cyber Terrorism:** Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.
- **Cyber Warfare:** It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation.
- **Distribution of pirated software:** It means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
- **Possession of Unauthorized Information:** It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives.

Cyber crimes against society:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- **Child Pornography:** It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity.

- **Cyber Trafficking:** It may be trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cyberspace is also a gravest crime.
- **Online Gambling:** Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.
- **Financial Crimes:** This type of offence is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally.
- **Forgery:** It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

III. Need of Cyber Laws & Awareness: information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the user of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the cyber crimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the cyber space authority to regulate criminal activities relating to cyber and to provide better administration of justice to the victim of cyber crime. In the modern cyber technology world it is very much necessary to regulate cyber crimes and most importantly cyber law should be made stricter in the case of cyber terrorism and hackers. Mostly peoples don't know about cyber crime/cyber laws. so today's need to aware the society about cyber crimes and cyber laws.

IV. Information Technology Act 2000 (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on October 17, 2000 to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes.

Penalties and Offences, Section under IT Act, 2000 Offence Penalty

Sec.43 Damage to computer, computer system, etc. Compensation not exceeding one crore rupees to the person so affected

Sec.43A Body corporate failure to protect data Compensation not exceeding five crore rupees to the person so affected

Sec.44(a) Failure to furnish document, return or report to the Penalty not exceeding one lakh and fifty thousand rupees for each such failure Controller or the Certifying Authority

Sec.44(b) Failure to file any return or furnish any information, books or other documents within the time specified Penalty not exceeding five thousand rupees for every day during which such failure continues

Sec.44(c) Failure to maintain books of account or records Penalty not exceeding ten thousand rupees for every day during which the failure continues

Sec.45 Where no penalty has been separately provided Compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees

Sec.65 Tampering with Computer source documents Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both

Sec.66 Hacking with Computer systems, Data alteration etc. Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both

Sec.66A Sending offensive messages through communication service etc. Imprisonment for a term which may extend to three years and with fine

Sec.66B Retains any stolen computer resource or communication device Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both

Sec.66C Fraudulent use of electronic signature Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh

Sec.66D Cheats by personating by using computer resource Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees

Sec.66E Publishing obscene images Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both

Sec.66F Cyber terrorism Imprisonment which may extend to imprisonment for life .

Sec.67 Publishes or transmits unwanted material Imprisonment for a term which may extend to three years and with fine which may extend to five lakh rupees & in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees

Sec.67A Publishes or transmits sexually explicit Imprisonment for a term which may extend to five years and with fine material which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

Sec.67B Abusing children online Imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees

Sec.67C Preservation of information by intermediary Imprisonment for a term which may extend to three years and shall also be liable to fine

Sec.70 Un-authorized access to protected system Imprisonment for a term which may extend to ten years and shall also be liable to fine

Sec.71 Misrepresentation to the Controller or the Certifying Authority for obtaining license or Electronic Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Sec.72 Breach of Confidentiality and Privacy Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

Sec.72A Disclosure of information in breach of contract Imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both

Sec.73 Publishing false digital signature certificates Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

V. Methods for Registered the Complaints:

You can registered your complaint against cyber crime in any police station of your state. The second method for register complaints is online method; you can lodge a complaint by E-Mail on cyber crime Cell Mail Id.

Address of Cyber Crime Investigation Cells In India

Punjab	**Haryana**	**Rajasthan**
Deputy Inspector General of Police,State Crime Branch & Cyber Investigation **Phase IV, Mohali (Punjab)** Complaints can be lodged by	Cyber Crime and Technical Investigation Cell, Old S.P.Office complex,Civil Lines Gurgaon E-mail: jtcp.ggn@hry.nic.in Website :	Ph: +91-9672700012 Website: http://www.cybercellindia.com

Delhi Central Bureau of Investigation, Plot No. 5-B, 6th Floor, CGO Complex, Lodhi Road, New Delhi – 110003, Ph:+91-11-4362203, +91-11-4392424 Website:http://cbi.nic.in/ E-Mail: cbiccic@bol.net.in	**Thane** 3rd Floor, Office of Commissioner of Police, Khalkar Lane, Court Naka, Thane (W) Ph: 022-25410986 Email: police@thanepolice.org Website: http://thanepolice.org/cybercell.php	**Madhya Pradesh** Inspector General of Police State CYBER POLICE, Bhopal (M.P.) Ph:0755-2770248 Email: mpcyberpolice@gmail.com Website:
Bangalore Cyber Crime Police Station, CID Annex Building, Carlton House, # 1, Palace Road, Bangalore - 560001. Telephone: +91- 080- 22942475, +91- 080- 22943050 Email: cybercrimeps@ksp.gov.in Website: http://www.cyberpolicebangalore.nic.in	**Uttar Pradesh** Cyber Complaints Redressal Cell, Nodal Officer Cyber Crime Unit Agra, Agra Range 7,Kutchery Road, Baluganj,Agra-232001 Uttar Pradesh Ph : 0562-2463343, Fax: 0562-2261000 E-mail: info@cybercellagra.com, digraga@up.nic.in Website: http://www.cybercellagra.com	**Chennai** SIDCO Electronics Complex, Block No. 3, First Floor, Guindy Industrial Estate, Chennai -32 Ph: 044 22502526 Email: spcybercbcid.tnpol@nic.in Website:http://cbcid.tn.nic.in
Hyderabad Cyber Crime Police Station, Hyderabad City. Email : cybercell_hyd@hyd.appolice.gov.in Ph:04027852040 Website:http://www.hyderabadpolice.gov.in	**Nagpur** Cyber Crime Investigation Cell, Crime Branch, 4th Floor, Administrative Building No. 1, Near Udyog Bhavan, Civil Lines, Nagpur-01. Email:cybercell@nagpurpolice.nic.in Tel: +91 - 712 â€“ 2566766	**Kerala** Website: http://www.keralapolice.org/newsite/ccps.html Helpline Numbers: 0471-3243000 0471-3244000 0471-3245000

Pune	**Mumbai**
Office of Commissioner of Police 2, Sadhu Vaswani Road, Camp, Pune - 411001 Phone: +91-20-020-26126296, 26122880, 26208250 Fax: 020 26128105. Website: www.punepolice.gov.in E-Mail: crimecomp.pune@nic.in /	Cyber Crime Investigation cell,Annex III, 1st floor, Office of the Commissioner of Police,D.N.Road, Mumbai - 400001 Ph: +91-22- 24691233,Web site:http://www.cybercellmumbai.gov.in E-mail id: cybercell.mumbai@mahapolice.gov.in

West Bengal	**Himachal Pradesh**
DIG CID IIIrd Floor ,Bhawani Bhawan,Alipore, Kolkata - 700 0027; Phone Numbers - 033 2450 6100 Fax Number - 033 2450 6174 Email :mail@cidwestbengal.gov.in	CID Office , Dy.SP Himachal Pradesh +91-94180 39449 E-mail:soodbrijesh9@gmail.com

VI. Conclusion: Since users of computer system and internet are increasing worldwide, where it is easy to access any information easily within a few seconds by using internet which is the medium for huge information and a large base of communications around the world. Certain precautionary measures should be taken by netizens while using the internet which will assist them to handel the threat of cyber crimes.

In the present era of rapid growth of information technology is encompassing all walks of life all over the world. These technological developments have made the transition for paper to paperless transaction possible. We are now creating new standards of speed, efficiency and, accuracy in communication, which has become key tools for boosting innovations, creativity and increasing overall productivity. With the rapid growth of information technology cyber crimes are also increasing, So it's the time to aware the society about various cyber laws for reducing cyber crimes.

References:

[1] Brenner, S. *(2007) Law in an Era of Smart Technology, Oxford: Oxford University Press*

[2] Csonka P. (2000) Internet Crime; the Draft council of Europe convention on cyber-crime: *A response to*

the challenge of crime in the age of the internet? Computer Law & Security ReportVol.16 no.5

[3] Easttom C. *(2010) Computer Crime Investigation and the Law*

[4] Fafinski, S. *(2009) Computer Misuse: Response, regulation and the law Cullompton: Willan*

[5] Grabosky, P. *(2006) Electronic Crime, New Jersey: Prentice Hall*

[6] McQuade, S. (ed) *(2009) The Encyclopedia of Cybercrime, Westport, CT: Greenwood Press*

[7] Moore, R. (2005) "Cyber crime: *Investigating High-Technology Computer Crime," Cleveland,*

Mississippi: Anderson Publishing.

[8] Paul Taylor. Hackers: Crime in the Digital Sublime *(November 3, 1999 ed.). Routledge; 1 edition.*

p. 200. ISBN 0-415-18072-4

[9] Robertson, J. (2010, March 2). Authorities bust 3 in infection of 13m computers. Retrieved March 26,

[10] Wall, D.S. *(2007) Cybercrimes: The transformation of crime in the information age, Cambridge:*

Polity.2010, from Boston News: Boston.com

[11] Walden, I. *(2007) Computer Crimes and Digital Investigations, Oxford: Oxford University Press.*

[12] Williams, M. *(2006) Virtually Criminal: Crime, Deviance and Regulation Online, Routledge, London.*

[13] Yar, M. *(2006) Cybercrime and Society, London: Sage*