IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPACT OF CYBER SECURITY IN FINANCIAL SECTOR IN INDIA WITH CHI SQUARE CALCULATION

Prof. (Dr). P. SUKUMAR MCA., MBA., M.Phil., PGDCA., (PhD).,
Assistant Professor-Department of MBA - SAN International Business School - Coimbatore

Dr.S.Prabakaran - MA., M.Phil. D.N.C.C., Ph.D., SET.,
Assistant Professor of Economics, Gobi Arts & Science College, Gobichettipalayam, Erode District, Tamilnadu

ABSTRACT : Internet, the worldwide connection of loosely held networks, has made the waft of information and data among exceptional networks less complicated. With statistics and statistics being transferred between networks at distant locations, security issues have come to be a chief situation from the past few years. The internet has additionally been used by few human beings for criminal sports like unauthorized get right of entry to others networks, scams, etc. these crook activities related to the internet are termed as Cyber Crimes. With the growing recognition of on-line activities like on line banking, on line shopping, and so forth., it's far a time period that we regularly hear inside the information now-a-days. therefore, so one can stop and punish the cyber criminals, "Cyber regulation" changed into added. Cyber law may be described as regulation of the internet, i.e., it is a part of the legal systems that offers with the internet, cyberspace and with other prison problems like on line protection or online privateness. consequently, keeping the targets in thoughts, this chapter is divided into distinct sections in an effort to offer a brief assessment of what's cybercrime, the perpetrators of cybercrime-hackers and crackers, special types of cybercrimes and the evolution of cyber laws in India. The chapter in addition throws light on how these laws paintings and the various preventive measures which can be used to fight this "hi-tech" crime in India.

Key words: Internet, Cyber Crime, Cyber Law, Cyberspace, Online security, Online privacy, Hi-Tech Crime, Hackers, Crackers, Unauthorized access.

I. INTRODUCTION

A laptop may be described because the system that shops and strategies facts which are informed through the user. Our on-line world, i.e., the internet, has made the float of statistics and statistics among unique networks easier and greater powerful. The internet generation is used for various functions ranging from online dealing to on-line transactions. because many years majority laptop customers are utilising the computer, either for their private blessings or for other advantages. Therefore, security related issues have come to be a chief subject for the administrators. This has given birth to "Cyber Crimes". Cyber Crime can as a result, be defined as the crimes committed through using laptop or laptop community and generally take region over the our on-line world specially, the net. In simple terms, cybercrimes are the offences that take location over electronic communications or records structures. A Cybercriminal may also use a device to have access to users' private information, personal commercial enterprise information, and authorities statistics or to disable a device. selling any private facts or facts without the consent of the owner additionally falls beneath cybercrime. Criminals appearing such sports are often referred to as hackers. therefore, cybercrimes are also called electronic crimes or e-crimes, computer-associated crimes, excessive-tech crime, virtual crime and the new age crime.

WHAT IS CYBER CRIME?

Sussman and Heuston became the primary to propose the time period "Cyber Crime" inside the 12 months 1995. Cybercrime has no unmarried definition; it is considered as a set of acts or behavior- those acts are based on the material offence object and modus operandi that affect computer statistics or systems . through definition, Cybercrimes are "crook acts carried out thru use of a computer or other form of digital communications" (Anderson & Gardener, 2015). In easy words, acts which are punishable by the facts era (IT) Act, 2000 are known as "Cyber Crimes". In India, the IT Act, 2000 offers with the cybercrime troubles. positive amendments have been made on this Act in 2008; thereby passing the information technology (IT) Act, 2008 protecting a extensive range of region which include on-line commercial transactions, digital signatures, e-trade, and so on. therefore, "Cyber Crime" can be described as any malefactor or different offences wherein electronic communications or statistics structures, along with any device or the internet or each or extra of them are involved .

THE PERPETRATORS-HACKERS AND CRACKERS:

i. Hacker: in step with section 66A of statistics era (IT) Act, 2000 , someone whosoever with the purpose to motive or knowing that he is possibly to purpose wrongful loss or damage to the public or any character destroys or deletes or alters any records living in a laptop resource or diminishes its price or software or outcomes it injuriously by way of any method is a hacker.

ii. Crackers: in line with the Jargon Dictionary , the time period "cracker" is used to distinguish "benign" hackers from hackers who maliciously reason damage to targeted computer systems. In different words, a "cracker" is defined as a hacker with criminal purpose who maliciously sabotages computers, scouse borrow facts located on cozy computers and cause disruption to the networks for private or political reasons.

CLASSIFICATION OF CYBER CRIMES:

Data technology has been misused for criminal activities in today's world. Such crimes may be committed against the governments, individuals and institutions. diverse varieties of cybercrimes exist in India and everywhere in the global. The common sorts of cybercrimes are discussed as follows:

i. Hacking: It in reality refers to have an unauthorized get right of entry to to any other computer system. it's far the maximum risky and generally acknowledged cybercrime. The hackers ruin down into the computer systems machine and steal precious statistics, called records, from the machine with none permission. Hacking can be performed for more than one functions like data robbery, fraud, destruction of statistics, and inflicting harm to computer system for private gains. therefore, hackers are able to spoof the facts and replica the IP address illegally.

in step with the research committed via the SANS Institute (2004), there are 3 distinctive forms of hackers:

- White Hat Hackers: these are the ethical hackers that use their hacking capabilities for exact motives and do no longer harm the pc device.
- Black Hat Hackers: those kinds of hackers use their pc know-how to gain unauthorized access to a computer device with a malicious or harmful goal. they'll scouse borrow, adjust or erase information, and insert viruses and damage the system.
- gray Hat Hackers: they are the skilled hackers that generally do no longer hack for personal gains. therefore, they may be hybrids between white hat and black hat hackers .

ii. Cyber Terrorism: It refers to illegal assaults against computers, networks and the records stored therein which are accomplished to intermediates or coerce a country's government or citizens, having political or social goals. consequently, terrorism acts which can be devoted in cyberspace are called cyber terrorism . The cyber terrorism assaults and threats encompass:

- Malicious software: those are net-primarily based software program or programs that can be used to gain access to a device to thieve sensitive information or information or disrupt the software program present in computer gadget.
- Domain Hijacking: It refers back to the act of converting the registration of a website call with out the permission of its original registrant.

iii. Cyber Stalking: it's far a criminal exercise in which an character makes use of the net to systematically harass or threaten someone. it's miles a willful conduct via the cyber stalkers thru any on line medium like e-mail, social media, chatrooms, and so forth., that in reality reasons the sufferer to feel apprehensive, intimidated or molested. normally the stalker knows their sufferer and majority of the sufferers are women. Earlier, the cyber stalkers had been booked underneath phase 509 of the IPC because of lack of punishment beneath the IT Act, 2000. After the change of the IT Act in 2008, the cases concerning cyber stalking may be charged under section 66A of the Act and the wrongdoer is punishable with imprisonment up to a few years, and with nice.

iv. Cyber Bullying: in keeping with the Oxford Dictionary , Cyber Bullying may be described because the "use of digital conversation to bully a person, usually with the aid of sending messages of an

intimidating or threatening nature". It takes place when youngsters including teenagers are threatened, careworn, humiliated, or in any other case targeted via other youngsters the use of digital technologies. Cyber bullying may also stand up to the extent of a cyber harassment fee, or if the child is young enough it can bring about the price of adlescent delinquency .

Cyber Pornography: It refers back to the act of the usage of our on-line world to create, show, distribute, or publish pornography or obscene substances. In different words, stimulating sexual or other erotic activities over the our on-line world, specially the net is known as Cyber Pornography . Many web sites showcase pornographic pictures, movies, etc., which may be produced speedy and cost effectively either thru morphing or through sexual exploitation of women and kids. Morphing refers back to the modifying of an original image via a fake identification or by an unauthorized user that is punishable below IPC and phase sixty six of the IT Act, 2000.

Infant pornography is abundant on the net. on line baby pornography involves underage humans being lured into pornographic productions or being sold or pressured into cybersex or lives of prostitution (CNN staff creator, 2001). Kidnapping and global smuggling of younger girls and boys for these purposes is now a transnational crime phenomenon often instigated in impoverished international locations wherein sufferers face dire financial instances (Chinov, 2000).

• Identification theft: It refers to the fraud which an person does with the aid of creating a fake identification at the net on the way to steal money from bank debts, credit score or debit cards, and so forth. it is punishable offence underneath segment 66C of the IT Act, 2008 .• Phishing: it's far a some other very commonplace sort of cybercrime which is used by hackers to thieve records which is private like passwords, usernames, bank account wide variety, credit card info, and so forth. it is usually finished with the assist of e mail spoofing.

• Forgery: It approach making of fake document, signature, forex, sales stamp, and so forth.

• Net jacking: It refers to hello jacking of the victims account with the help of a fake internet site with the intention to harm it or trade the facts of the victims' web site. The attacker sends a link to the sufferers e mail. while the sufferer opens the link, a brand new page appears with the message of clicking some other link. by means of clicking at the link, the sufferer may be redirected to a faux page.

• Cyber Embezzlement: Such form of crime is done through employers who have already got legitimate get right of entry to the corporation's automatic machine. An employee may also perform such against the law for you to earn extra cash.

• corporate Espionage: that is a type of crime devoted by using people for you to benefit aggressive benefit in the marketplace. under this crime, the cybercriminal can be from within or out of doors the company and he/she may additionally use the business enterprise's network to steal the list of customers, advertising techniques, monetary statistics, change secrets, and so on.

• Plagiarism: it is used to scouse borrow a person else authentic writings and call it as their very own. for the reason that most of the statistics is available online and people are actually having extra get entry to to the net and the computer systems, the problem of plagiarism is growing day-by using-day. There are positive software's which might be used to hit upon plagiarism.

vii. e mail Spoofing: according to Techopedia, electronic mail spoofing is a fraudulent electronic mail pastime/technique used to cover the authentic cope with of the email message, although the mail seems to have come from a valid supply . it's far very common now-a-days. Such tactics are usually achieved via spammers having malicious intentions which includes to benefit get admission to to someone's banking data or to unfold virus. The offender is charged with forgery underneath phase 463 of the IPC for committing such offences.

SMS Spoofing is also located in today's present day international of technology. It permits changing the call or quantity textual content messages appear to have come from.

Prevention of cyber crimes:

With the intention to prevent crimes dedicated through the laptop resources and internet era, "Cyber law" was brought. "Cyber laws" may be defined as the legal troubles which might be related to the usage of verbal exchange technology, concretely "cyberspace", i.e. the net. it is an endeavor to integrate the demanding situations provided by human motion at the net with legacy gadget of legal guidelines relevant to the physical international. it's far critical as it is worried to nearly all components of activities and transactions that take area both on the internet or other communique gadgets. whether we are aware about it or now not, each action in cyberspace has a few felony and cyber felony perspectives .

Primarily based on the United international locations model regulation on digital trade (UNCITRAL), 1996, the Indian Parliament exceeded the information technology Act, 2000 (also known as the IT Act no. 21 of 2000) on 17th October, 2000. This law changed into brought in India to deal with the digital crimes or cybercrimes and electronic trade.

A few key factors of the statistics era (IT) Act, 2000 are as follows:

- Digital signatures are given criminal validity inside the Act.
- The Act has given beginning to new commercial enterprise to companies to trouble digital certificate through turning into the Certifying government.
- This Act allows the government to trouble notices on net via e-governance.
- The verbal exchange between the organizations or among the enterprise and the government can now be via net also.
- Addressing the issue of protection is the most critical function of this Act. It brought the idea of digital signatures that verifies the identity of an character at the internet.
- In case of any loss or harm accomplished to the business enterprise through criminals, the Act affords a remedy inside the form of money to the corporation. The data generation Act, 2000 did now not included all the aspects of cybercrimes dedicated; amendments have been achieved within the Rajya Sabha on twenty third December, 2008, renaming the Act because the records technology (modification) Act, 2008 and turned into known as ITAA, 2008. eight new Cyber Offences were brought to ITAA, 2008 under the subsequent sections: apart from the above referred to Sections under the IPC and ITAA, 2008, the authorities of India has taken the following steps for prevention of Cybercrimes:

- Cybercrime cells were set up in states and U.T's for reporting and research of Cybercrime instances.
- The authorities beneath the IT Act, 2000 has also set up Cyber Forensic and schooling Labs in states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc., for recognition creation and education in opposition to Cybercrimes.
- In collaboration with statistics safety Council of India (DSCI), NASSCOM, Cyber Forensic Labs had been set up at Mumbai, Bengaluru, Pune and Kolkata for attention creation and training.
- Numerous packages had been performed through the authorities of India to generate recognition approximately Cybercrimes. national law college, Bengaluru and NALSAR university of regulation, Hyderabad are engaged in carrying out several awareness and education packages on Cyber legal guidelines and Cybercrimes for Judicial officials.

  Schooling is imparted to law enforcement officials and Judicial officers inside the training Labs hooked up via the government.

OBJECTIVE OF THE STUDIES

i. To unfold expertise at the crimes/crook activities like unauthorized access to others networks, scams, and so forth., which are taking area via our on-line world particularly, the net;

ii. To Generate recognition among the hundreds on "Cyber laws" which might be imposed a good way to stop the cybercrime and/or punish the cyber criminals; and

iii. To suggest other preventive measures other than the Cyber regulation in order that there may be protection of the customers inside the our on-line world.

REVIEW OF LITERATURE

Ankita P. (2011) The author has discussed about the E commerce activities in India, the competitive and anti competitive factors affecting the E commerce future. Major focus is on the credit card activities affecting the E commerce. In the paper author has also discussed some international case studies. Lastly the role of CCI in dealing these issues is discussed.

Nappinai N. S. (2010) The author in his paper "Cyber Crime Law in India has law kept pace with Emerging Trends? AnEmpirical Study" highlighted some important provision of the criminal laws in India relating to data protection, privacy, encryption and other cyber crime activities and to the extent said provisions are enforced to fight not just the present but future trends in Cyber Crime.

Rohas N. (2008) In this book "e commerce legal issues" author has explained about e commerce activities, legal andtechnical issues of digital signatures. Also a in depth knowledge about e certificates, electronics contracts and step by step method to digitally sign a word document and email is provided, author has also focused on how to obtain digital signature certificates and discussed many case studies.

Waghmare G.T. (2012) Prof. Waghmare in his Research Paper "A Business Review of Ecommerce in India" has mentionedabout the market scope of the country in ecommerce industry, advantages and disadvantage of ecommerce. According to the author there is great potential in India to flourish E commerce Industry because of Low PC cost and Availability of Internet but the same time awareness

amongthe people, low security and maintenance, Taxation, Vendor Management etc. Impact of ecommerce on retailers is also discussed briefly.

Dr. Khandelwal A. (2011) The author discusses E commerce management practices in India it is felt that there is need toincrease trust by providing additional security. In this paper author have mentioned new approach inwebsite security, systems build using whitelist paradigm may create secure websites. There shouldlittle customers fear and risk associated with sensitive and vital information. There by increasing the creditability of online shopping in market

Nisha C. and Sangeeta G. (2012) Authors have explored Indian E Commerce Industries and its Opportunities in upcoming years. Paper gives overview of the future of E-Commerce in India and discusses the future growthsegments in India's E-Commerce and represents various opportunities for retailers, wholesalers, producers and for individuals. Paper givers only the positive aspect of e commerce and its future growth.

Shilpan V. (2012) In this paper "E-banking and E-Commerce in India and USA" author discusses about E Banking a Major Field related to E commerce Activity and has shown a direct comparative study between the developing countries like India and US. The future of E- Banking in developing Countries appears bright but consumers and merchants face many barriers like reliable tele communication infrastructure, power supplies, less access to online payment mechanism.

Talwant S. (2004) A Addl. Distt. & Sessions Judge has taken up a crucial and rare topic of discussion that is the importance of harmony between the law enforcement agencies and computer professionals. According to author both the parts are equally important for enabling strong cyber security incountry and make internet a safe place for its users. Author has also made a comparative study onlaw definition in US and India.

Ashwini B. (2012) Author discusses broadly about the ratio of increasing cyber crime and there effect on the societyand e business and retailers. The paper briefs about the cyber threat and frauds, it also briefs about the internet user in India, its scope and future. Author also puts light on the governmental measures to stop cyber crime and talks about the challenges that India needs to face to beat cyber threat.

Susheel B. and Durgesh P. (2011) Authors in their paper "Study of Indian Banks Websites for Cyber Crime Safety Mechanism" discusses that security plays an important role in implementation of technology specially in bankingsector. Paper talks about the cyber security required at the core banking level as the money is just only single click away. Through this paper authors have tried to put forward different issues that Indian banking system face and importance of cyber security mechanism.

RESEARCH METHODOLOGY

Research design:

A research scholar is also required to plan well before he can start his work. The researcher is required to prepare a plan of action is known as research design. Research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure.

Convenient sampling

This sampling method involves purposive (or) deliberate selection of particular units of the universe of the universe for constituting a sample, which represents the universe. When population elements are selected for inclusion in the sample based on the cause of access it can be called convenient sampling

Size of the sample:

It refers to the number of items to be selected from the universe to constitute a sample. Here the researcher has selected 100 elements of end users. The sample is 60.

Collection of data:

There are several ways of collection the appropriate data, which differ considerably in context of money cost, time and other resources at the research data collection can be done through collections of primary data and Secondary data

Primary data:

The primary data are those, which are collected a fresh and for the first time and thus happen to be original in character. An interview schedule has been used to collect the primary data schedule. It means the data collection resembling the collection of data through questionnaire with a difference that schedule is filled by the researcher.

Secondary data:

The secondary data on the other hand includes those data, which are collected for some earlier research work and are application in the study. The researcher has presently under taken, for this analysis the sales data are collected from marketing information system.

Analysis of data:

The primary data has been analyzed using the simple percentage analysis method.

STATISTICAL ANALYSIS

Proposed Sampling Methods:

The data was processed using the SPSS

1. Sampling design chosen for the present study has been non probability sampling.

Statistical Tool:

1. Percentage Analysis.
2. Chi-square analysis

$$\% \text{ of Respondents} = \frac{\text{No of respondents}}{\text{No of Total Respondents}} \times 100$$

Chi-Square Analysis

A statistical test used to determine the probability of obtaining the observed results by chance, under a specific hypothesis. It is used to test if the standard deviation of a population is equal to the specific value. Chi-square is a statistical significance test based on frequency of occurrence; it is applicable both to qualitative and quantitative variables. Among its many uses, the most common are tests of hypothesized probabilities or probability distributions, statistical dependence or independence

and common population. A Chi-square test is any statistical hypothesis test in which the test statistic has a Chi-square distribution if the null hypothesis is true.

Formula:

$\chi^2 = \sum \{ (Oi-Ei)^2 / Ei \}$

Oi = Observed frequency.

Ei = Expected frequency.

CHI SQUARE ANALYSIS:

Aim: To test the significance of respondent's opinion about cybercrimes and Cyber law in India

Null Hypothesis (Ho):

There is no significance of respondent's opinion about the cybercrimes and Cyber law in India

Alternate Hypothesis (H1):

There is significance of respondent's opinion about the cybercrimes and Cyber law in India

S.No	Respondents opinion about cybercrime and cyber law	No. of the respondents	Percentage
1	Strongly Disagree	3	4
2	Disagree	5	7
3	Neutral	0	0
4	Agree	22	29
5	Strongly agree	45	60
	Total	75	100

CHI SQUARE TABLE

Observed **O**	Expected **E**	**O-E**	**$(O-E)^2$**	**$(O-E)^2 / E$**
4	3	1	1	0.333
4	2	2	4	2
29	28	1	1	0.035
60	65	-5	25	0.384
			Calculated Chi square value	$\sum^2 = 2.752.$

Degree of freedom = (n-1) = (4-1) = 3

Level of significance = 5%

For 3 degree of freedom at 5% significance the Chi square table value is = 7.81

Calculated value < Table Value

2.752. < 7.81 So, **Ho is Accepted**

Inference

There are four castigatory respondent's opinion calculated through statistical tools, the finding value is lesser than expected chi square table value So, Ho value is accepted.

CONCLUSION:

To finish, we are able to say that the arrival computer networking and newly developed technology have given rise to cybercrimes inside the beyond few years. This has created super threats to mankind because the victim is known to the attacker and he/she with malicious intentions like inflicting damage to the computer machine, stealing or erasing records stored within the device, converting password, hacking credit card details, and bank account quantity, etc., commits such crimes. distinctive styles of cybercrimes like cyber stalking, cyber terrorism, cyber pornography, morphing, forgery, email spoofing, identification theft, and many others., have severe affects over the society. The cybercriminal gains unauthorized get right of entry to to laptop resources or another private facts of the sufferer by using hacking their account. it's far, consequently, very crucial for each person to be aware about those crimes and remain alert and lively to avoid any non-public or professional loss.

SUGGESTION :

Which will resolve the hassle of Cybercrime having worldwide dimensions, the authorities of India enacted the information generation Act in 2000 to deal with such "hi-tech" crimes. The Act turned into passed again in 2008 with sure amendments. 8 new offences have been added and the Act became renamed as the records technology (modification) Act, 2008 called ITAA, 2008. apart from this act, certain Sections underneath the Indian Penal Code (IPC) are also used as criminal measures to punish the people committing such crimes. felony provisions on Cyber Stalking and online Harassment are also protected beneath the Sexual Harassment of girls at workplace (Prevention, Prohibition and Redressal) Act, 2013. for this reason, to ensure justice to the victims and punish the criminals, the judiciary has give you the above discussed legislation.

REFERENCES:

1. Anderson, T. M. & Gardener, T.J. (2015). *Criminal Law: Twelfth Edition.* Stanford, CT: Cengage Learning

2. Bar Association of India (2015). *Anti-Bullying Laws in India.* Retrieved from https://www.indianbarassociation.org/wp-content/uploads/2015/11/Anti-bullying-laws-in-india.pdf

3. Brenner, W. Susan (2010). *Cybercrime: Criminal threats from cyber space.* Green Wood Publishing Group, Westport.

4. Chinov, Mike (2000). *Aid Workers Decry Growing Child Sex Trade in Cambodia.* CNN.com Retrieved from http://archives.cnn.com/2000/asianow/southeast/09/18/cambodia.pedophile/index.html

5. Staff Author, CNN (2001). *Sex Slavery: The Growing Trade.* CNN.com

Retrieved from https://archives.cnn.com/2001/world/europe/03/08/women.trafficking/

6. Flemming, P. and Stohl, M. (2000). Myths and Realities of Cyber terrorism. *International Conference on Countering Terrorism through Enhanced International Cooperation,* Page No. 22-24, September, Italy.

7. Hafele, D. M. (2004). Three different shades of Ethical Hacking: Black, White and Grey. February 23, 2004.

8. Higgins, George (2010). *Cybercrime: An Introduction to an Emerging Phenomenon.* Mc Graw Hill Publishing, New York.

9. Holt, Thomas J. (2011). *Crime Online: Correlates Causes and Contexts.* Caroline Academic press, USA.

10. International Journal of Social Science and Humanities Research (2016). *A Sociological Study of Different Types Of Cyber Crimes.* Vol.4, Oct-Dec 2016. Retrieved from http://www.researchpublish.com/journal/IJSSHR/Issue-4-October-2016-December-2016/0

11. Singh, Talwant (2011). *Cyber Law and Information technology.* New Delhi, India.

12. Wall, David S. (2001). *Crime and the Internet.* Routledge, London.

13. www.tigweb.org/actiontools/projects/download/4926.docx

14. http://www.interpol.int/public/technologycrime/crimeprev/itsecurity.asp#21/4/2015

15. https://www.tutorialspoint.com/information_security_cyber_law/introduvtion.htm

16. https://www.slideshare.net/bharadwajchetan/an-introduction-to-cyber-law-it-act-2000-india

17.http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW

18. http://deity.gov.in/sites/upload_files/di/files/downoads/itact2000/itbill2000.pdf

19. http://www.lawyersclubindia.com/articles/Classifiaction_Of_CyberCrimes_1484.asp

20. http://vikaspedia.in/education/Digital%20Literacy/information-security/cyber-laws

21. https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V518-0156.pdf

22. https://indiankanoon.org/doc/1439440/

23.http://police.pondicherry.gov.in/Information%20Technology%20Act%202000%20%202008%20%28amendment%29.pdf

24. https://cybercrimelawyer.wordpress.com/category/information-technology-act-section-65/