International Journal of Legal Expatiate Vol 1 (2021) Pg. 15-36 ISSN: 2583-7885(Online)
Published by Author Lens

INTERNET, CYBERSPACE, CYBER CRIMES AND FRAUD- A CONCEPTUAL ANALYSIS WITH HISTORICAL DEVELOPMENT

-Abhishek T[1]

ABSTRACT

Cyberspace is also considered to be a metaphor that is used to disseminate the "sense of a specific social setting that exists purely in relation within a space of representation and communication. It exists entirely within a computer space, distributed across increasingly complex and fluid networks". "Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures (ITI) including the internet, telecommunication networks, computer systems, and embedded processors and controllers".

Internet fraud/ computer fraud the word computer fraud is used in various ways, however, to find any clear and precise definition of what is it actually being talked about is still in a dilemma though the warnings and dangers of 'computer frauds' and 'internet frauds' are frequently reported in the newspapers and other media. This dilemma prevails because there is no definite definition in the English law relating to fraud other than a strong indication as to what are the essential elements of the word fraud.

Keywords: *Cyber Fraud; Cyberspace; IT Act; Computer Frauds; Cyber Jurisdiction.*

I. INTRODUCTION

In order to understand the topic of this study, it is important for us to understand as to what are the various words and phrases that need to be understood for making a through reading of Internet Frauds. In furtherance to understand this meaning, it would be important to understand the meaning of various words that are commonly connected to the research topic. In this chapter, the researcher would attempt to bring in various definitions[2] and meanings of the words that are reflective in this study. The most important words, are the outline of the meaning

[1] B.A.LLB(Hons); LL.M (PhD), KLEF, AP, India.

[2]Cyberspace (cspace) – "the purist may regard cyberspace as incorrectly referring to the Internet, particular services available on the Internet, webspace, or the domain of electronic communications in general". Available at, http://www.kevcom.com/words/cspace.1.1.pdf (Last Visited, June10,2021)

of the word Cyber space, Internet, Computer Crimes/Cyber Crimes, Fraud and the most important for this study i.e., Internet Fraud.

II. INTERNET

Internet is considered to be mother of all networks. Although it started only with a smaller capacity for the purpose to use for the defense purpose in the US as ARPANET, 40 years ago, it has become the largest network in the world. It basically has three level hierarchies that are composed as backbone networks, mid-level networks and stub networks. These networks include commercial, university and other research networks including the military networks. These networks operate through the Internet protocol. Till the advent of the WWW, Internet was rarely known to the world other than to the universities and the corporate research departments including the defense departments. During this period, it was mostly accessed through the Telnet or the FTP. Once it turned out to be commercial, it has become ubiquitous to the modern-day information system and widely used for commercial activities. The fast development of commercial activities and the use of the internet for contractual purpose of sales of products and services have exploded the transformation system of information for either free of cost or for a minimal cost for advertising, sales, services and market building purpose. Due to this huge connectivity, it has become the largest network of all times. It has connected the whole world through an interconnected system of networks that connects the computers of the world through TCP/IP protocols and it is well known as Internet[3]. In simple usage the Internet can also be called as "the Net,". It provides for persons to talk directly to users at other computers[4]. Michael L. Rustad and Thomas F. Lambert Jr (2009) in the first chapter of their text book titled 'An overview of the Internet', both the pre-commercial internet stage and the post commercialization, with the development of technology has been quoted, with the brief history of Internet development. This gives a preliminary understanding that the development of internet was for the scientific and defense purpose and now with the development of the WWW, and Social Network Websites, the culture for students of the Internet law has drastically changed the perception about Internet[5].

[3] http://www.answers.com/topic/internet (10/06/21)

[4] http://searchwindevelopment.techtarget.com/sDefinition/0,,sid8_gci212370,00.html (10/06/21)

[5] Michael L. Rustad, Thomas F. Lambert Jr. Professor of Law, Suffolk University Law School, Internet Law in Nutshell, Research Paper 09-05 Jan 21, 2009 Available at http://ssrn.com/abstract= 1329092

According to the *Federal Networking Council*[6] an Internet *Monthly Reports (October 1995*) in its explanations accepts that;

a) "Able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols"; and
b) those that provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described with Humanities and Arts: which has a sharing and the center stage on the Internet: Here it involves People, Computers and Information that are electronically linked around the world by a common Protocol for communicating with each other[7].

Grammatically, Internet[8] is a noun which is defined to be a vast computer network processing of linking smaller computer into networks worldwide (usually prec. by *the*). Internet has originated and associated with the information technologies and is being well documented. But in order to understand its impact on the cybercrimes, many aspects need to be understood[9]. The social and the economic reasons are the major impact on the society. Its highly modern colonization has led to "lifting out of the local contexts of interaction and restructured across indefinite spans of time-space" (Bottoms & Wiles, 1996 p 14). The changes in the information society and an overall increase in numbers of intellectual property laws for the establishment of the ownership of ideas and the commodification of information capital in the new political economy has given immense opportunities for business and social development and this in turn has brought in the entirely new realms of criminal opportunity for the individuals to commit crimes. The networked crimes are increasing because of this social interaction and economic background. Internet has many components. But the most well know of all the component is the WWW. Though the WWW has been defined in various ways, one of the most acceptable definitions is:

[6] http://www.cs.columbia.edu/~hgs/internet/definition.html (10/06/21)

[7] Last updated 01/10/2008 05:08:43 by Henning Schulzrinne

[8] SEC. 202.Federal Trade Commission Sanctions. (A BILL on 'Telemarketing Fraud and Seniors Protection Act.) (b) INTERNET is DEFINED- as a term that means "collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio".

[9]. Wall, D.S (2005) 'The Internet as a Conduit for Criminals', pp.77-98 in Pattavina, A. (ed) Information Technology and the Criminal Justice System, Thousand Oaks, CA: Sage (ISBN: 07619301910) at pp 1-2.

"The World Wide Web is a mechanism or system, for linking together millions of electronic documents, or web pages, each of which can be accessed through a unique, yet changeable, Universal Resources Locator (URL). A website is simple a collection of web pages".

WWW was open to the world around 1990, which was mostly of a public nature. The further developments of the technology forced password protected sites as people realized that access to certain documents could be restricted. Once the Internet commercialized, websites as we see today turned out as private sites in the form of Intranets and extranets. Most of the universities, companies, law firms make extreme use of intranet for sharing information within the organization. However, the Extranets[10] are developed with the extensive and large networks with the main purpose of use of the internet system, which is generally created and utilized by large institutions and corporations, which are partially open for the access by the general public. Such access is provided by the corporations through the interface with the WWW, or through a separate system of networks with public access portals[11].

III. Nature of Internet

The nature of internet is discussed in detail by the court in *American Civil Liberties Union, et al v. Janet Reno, Attorney General of the United States*[12]. Although there was no dispute relating to history and basic technology relating to internet in the case, the court set out few important features/natures that are usually accepted relating to the internet. The following points were set and accepted by the court in respect to the nature of Internet:

a. The inception of the internet and innovation of cyberspace

Internet is a network of networks. It does not have a physical or tangible entity, but rather a giant network that interconnects innumerable smaller[13] groups of linked computer networks. It has its origin in 1969 as an experimental project of the ARPA[14] well known as ARPANET. Later it came

[10] The simplest example of extranet is the system used by the airlines for booking seats on flights. The network once used by airlines to check seat availability and prices can now be accessed not only by the travel agents but also by the members of the public.

[11] Yee Fen Lim, Cyberspace Law Commentaries and Materials, Oxford UP, Second Edition, Indian Edition, 2008 (Chapter 1)

[12] 929 F Supp 824 (1996)

[13] Small network here are ubiquitous and are called the Local Area Network (LAN)

[14] Advanced Research project Agency. This network linked the computers and computer networks owned by the military, defense contractors, and the university laboratories conducting defense related research.

to be known as DARPA[15] and ultimately titled as Internet. Some networks may be closed and the others might be any network that communicates with other computers. This global web of linked networks and computers is referred to as the internet. So, the computers and the computers networks those *in toto* make the internet. They are commonly owned by the government and other public institutions, some are owned by the non-profit organization, and some are privately owned. So, when it comes to the question of who owns the internet it can be quintessential answered that it is 'No body'. However, the resulting of these organizations entirely put together is doing a decentralized activity for the global medium of communications. It is in turn well known as "Cyberspace", that links the people, institutions, corporations, and the governments around the world. So, Internet can be considered to be an international system[16]. With further developments and more linked networks many networks developed like BITNET, CSNET, FIDONET and USENET. Eventually when there was overlapping of many of these networks, so the series of linked networks[17] today is well known commonly as Internet. However, not a single entity by itself administers or controls this internet.

B. Individuals can access internet in various modes

In general individuals can access cyberspace in a wide variety of avenues including the internet. Physically there are mostly two common way methods to establish an actual link to the internet. One way is to use computer or computer terminals that are directly connected to the computer network, which is in turn connected to the Internet. The other method is by use of computer 'personal computers' with a 'modem' connected to the telephone line that is directly or indirectly connected to a larger computer or computer network and in turn to the Internet. Colleges, offices (including academic and research), corporations, free-nets, computer coffee shops, commercial and non-commercial "Internet Service providers and many online services, bulletin board systems are the varied modes through which the individuals can access the internet. With such varied facility the commercial access to the Internet is growing rapidly.

[15] When the network linked computers evolved beyond researches across the country to access directly and to use extremely powerful supercomputers located at a few key universities and laboratories. When it went beyond research origins in the US to include all the three, i.e., Universities, corporations and the people it was called DARPA and later as Internet.

[16] Yee Fen Lim, Cyberspace Law Commentaries and Materials, Oxford UP, Second Edition, Indian Edition, 2008(Chapter 1 at p 5)

[17] (Themselves linking computers and computer networks)

C. Varied methods of communicating over the internet

The methods used to access the Internet for communication and information purposes are constantly evolving and therefore specifically mentioning only few categories is very difficult. However, the most commonly used methods can be grouped as follows[18]:

1. One-to-one messaging like the e-mail comparable to a 'first class letter'
2. One-to-many messaging like the 'listserv' or 'mail exploders'
3. Distributed message databases like that of 'USENET newsgroups' where the information or message is mostly through an automated process and may not require direct human intervention. Even few newsgroups use distributed messages to thousands of individuals.
4. Real time communications like the 'Internet Relay Chat' (IRC), which is analogous to a telephone party line, using a computer and the keyboard rather than a telephone. Some of the IRC are 'moderated' or has 'channel operators.
5. Real time remote computer utilization like the 'telnet' used to connect to some remote library to access the library's online card catalog program.

Remote Information Retrieval like the 'ftp', 'gopher' and the 'WWW' are well known forms for retrieval of remote information. These are the major categories and well-known use of Internet. Here the information on the required topic can be retrieved from the computer files available on a remote computer. Other than these forms, there are Voice over Internet Protocol (VoIP), Instant Messaging are used for communication.

D. The most popular been the WWW

Among many categories that are used for connecting to the Internet, WWW is that utilizes the 'hypertext' formatting the essential language called hypertext markup language (html), and programs that browse the web can display html documents that can link to other types of information or resources. Once a link is established through the resource locator, it will be connected by the hyperlinks. So, when the WWW was created, it was basically brought in with an objective to serve the world with knowledge available at online stores, and a plat form which contains information from the diversified sources and accessible to internet users around the

[18] Yee Fen Lim, Cyberspace Law Commentaries and Materials, Oxford UP, Second Edition, Indian Edition, 2008(Chapter 1 pp 10-13)

world. As individual computers are connected to the Internet through the W3C[19] protocols, the information which is on different computers becomes part of a single body of knowledge[20]. The WWW is actually a series of text documents stored in different computers all over the Internet, including the information stored in still images, sounds and videos.

E. Multiplicity of content on the internet

Internet is not only used for commercial communication that are generally used by the commercial entities to inform the potential consumers about the goods and services offered by the companies and to solicit purchases, but many other such web sites exist solely for the purpose in relation to dissemination of non-commercial information also. Most forms of the Internet communications like the e-mail, bulletin board, newsgroups and the chat rooms are not frequently used for commercial use. The Journals, popular magazines, and titles of compact discs and the entire card catalogue of the Carnegie Library are online. Availability of such diverse and plentiful information is possible because Internet provides an easy and inexpensive way for a speaker to reach a large audience, potentially millions. The startup as well as the maintenance cost of the communications in the Internet is significantly low compared to that of the other mass communication forms like the television, radio, newspapers and the magazines. So, it can be easily operated by both large and small organizations. The easy communication technique is facilitated by the 'html' as it allows the 'hyperlinks' or 'links. Compared to the other modes of communications, Internet is unique and wholly a new medium of worldwide human communications due to its diverse uses and interactive forms that makes it more attractive for the users to communicate.

F. Ability to restrict access to unwanted on-line material

Though there is large content available on the Internet. The content may be useful or may not be, but access to them is easy, even to the kids. With such form of information available, sometimes the parents may have to restrict some content that may be inappropriate to their children. In order to give this facility of restricting the content various entities have begun to build systems intended to enable parents or the government to control the material. In order to facilitate these restrictions,

[19] W3C was originally developed at CERN, the European Particle Physics Laboratory and was initially used to allow information sharing within internationally dispersed teams of researches and engineers. However now it has extended beyond the academicians and the researchers to include communications by individuals, non-profit organizations and businesses.

[20] *American Civil Liberties Union, et al v. Janet Reno, Attorney General of the United States*, 929 F Supp 824

the W3C launched the PICS program in order to develop technical standards that would support parents' or the government 's ability to filter and screen material that their children or people should not see. So based on the decision of the court in Reno's case the above is the nature of Internet is been described. In addition to the above view, they stated that Internet been unique, has certain features, which were absent in the earlier mode of communications. With this ubiquitous nature, the next question which the regulators would certainly be interesting in knowing, is there a need for the new or specific legislations i.e., laws to control and regulate the Internet.

IV. IS INTERNET A CONDUIT OF CRIME?

If this question has to be answered, first and foremost thing we have to look into is the key transformative that has impacted by the internet technologies and distributed systems. Based on these definitions and the meaning provided to various words that are often used in this research topic, the researcher would further the study on the above aspects. In the light of these definitions and meaning, the technology and the medium used by the perpetrators are understood. Technology has challenged the investigators to have novel and varied techniques to learn and understand physical and psychological development of the perpetrators/wrongdoers, unless the art of this new words are not absorbed into the existing laws or widely defined, so that the thought of combating the Cybercrime, including the Internet Frauds would be possible within the ambit of the existing laws, or else there may be need for continuous and rigorous process of making various specific-context laws day after day in the phase of technological growth.

V. Is there a requirement for Internet Law?

In order to answer this question, the most important question that needs to be addressed here is to understand as to who has the ownership and control of the Internet. Though instantly it can answer as "No one", it can be ultimately proficiently said that the ownership of the physical infrastructure of the internet is with the government, individuals, corporations, telecommunications utilities, who are technically owning it. Though indirectly government policies and its decisions play a vital role in the working of the internet, Internet is one of the first major global institutions that have no government directly involved in it[21]. However, internet is a culmination of agreements that has evolved between the telecommunications providers. It is generally argued that there is no one who

[21] Yee Fen Lim, Cyberspace Law Commentaries and Materials, Oxford UP, Second Edition, Indian Edition, 2008(Chapter 1)

actually has the ownership of Internet. However, it would be a conceptually a misleading statement, if the same is accepted. So, it can be concluded that even though no single body can actually claim control of the Internet, it is in fact organized and controlled by various cooperative groups, with varying degrees of formalities that will play an important role in the ongoing administration of the Internet. The groups that control the internet are basically of two levels, one is the technical level and the other is the policy control level. Among various groups that control the internet, the organizations that need a special mention are the Internet Architecture Board[22](IAB), Internet Corporation for Assigned Names and Numbers[23] (ICANN) and the World Wide Web Consortium(W3C)[24]. These three including the other organizations make it as the Internet Executive. The operations of the most of the organizations are informal and highly dynamic and their relationship is mostly based on *ad hoc* and with quasi –democratic ideas. They work with a mixture of commercial contracts, memorandum of understanding and other private arrangements.

Orin. S. Kerr[25] (2003) explains about the Internet's inability to generate a virtual reality that creates the problems in the perspective of the internet. The distinctions between the internal perspective (Virtual reality) and the external perspective (Physical reality) are discussed to understand both the perspectives. "The computer network and the internet provide widespread technology that creates a virtual world for its users that can compete on an equal footing with the real one. As a result, the internet law prompts us to comfort the problem of perspective for the first time". The authors explain the new perspectives with four examples like The Fourth Amendment in Cyberspace in related to search warrants, Internet Governance with the highlight of Code is law- or is it? Later part of the article is about the computer crimes and the copyright law and the internet with few case laws that are critically analyzed with the existing laws and the flaws that may arise while interpreting the laws and making a judgment. In the later part of the article, the author finds out varied answers to the above four problems and the different answers while

[22] The IAB is also responsible for the management of the IETF protocol parameter registries. http://www.livinginternet.com/i/iw_mgmt_iab.htm (last visited June 17, 2021)

[23] ICANN was formed in 1998. It is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet's unique identifiers. ICANN doesn't control content on the Internet. Through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet; however, it coordinates the name and number through unique identifiers across the world, without which it would not be possible to have a coordination of one global Internet. http://www.icann.org/ (last visited June 17, 2021)

[24]The W3C mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web. http://www.w3.org/ (last visited June 17, 2021)

[25] Orin S. Kerr, The Problem of Perspective in Internet Law - Georgetown Law Journal Jan 2003, 357 (91 Geo.L.J.357)

making interpretation by judges in the internal perspective and the external perspective. Few suggestions that can be followed by the courts while interpreting the external and internal perspective of internet, as and when deciding the cases, especially for making the laws relating to internet are the main focus of the article. However, Susan W. Brenner (2001) questions the realities of something know as cybercrimes. The author explains the traditional crimes and their four elements for each crime in the Real World. The anecdotes of the criminal liability of the Anglo- American law has been explained addressing few crimes like burglary, criminal trespass, forgery, fraud, stalking (considered to be relatively new to the cyber world) etc. The later part of the article is the criminal liability in the virtual world that quite clearly explains all the above offences in the real world and elucidates as to how they are not different in the virtual world of crime and commission. The main ingredients like *actusreus, mens rea*, attendant circumstances and harm are given with the specific illustrations of few crimes in the virtual world to explain the similarity and application of criminal law. Other than new medium i.e., the computer, the crimes like fraud are committed with no actual difference. This article is very relevant to the topic of my research and the necessary requirements for research are explicitly explained by the author. However, few new crimes like the Denial of Service, Hacking and Cracking that are similar to the real-world crime like burglary and trespass are compared. The explanation of existing laws that can be easily made applicable to the newer crimes in the virtual world are illustrated by the author and has been suggested, that law needs no urgent change, unless something very imminent comes up and that cannot be dealt with in the existing i.e., real world laws. The author also touches upon the inchoate offences including the cyber-inchoate offences. The case of LambdaMoo the case of virtual rape and its repercussions has been explained in detail. The author concludes the application of the real-world laws are for the time being, is enough to deal with the crimes in the virtual world[26].

In this book review titled "Beyond Our Control" Confronting the limits of our legal system in the Age of Cyberspace by Stuart Biegal; David McPhie (2002) considers this book to be one of the well-researched and carefully organized texts, on the Internet law. It has covered wide range of internet related legislations, treatises and cases. The book is considered to be a self-contained, introduction course on the Internet Laws. In the four parts of its framework, the book has the categorization of the problem, existence of the consensus, uniqueness, and regulatory models. In

[26] Susan W.Brenner, Is There Such A Thing As "Virtual Crime"?, 4 Cal. Crim.L Rev.1 (California Criminal Law Review, June, 2001)

part I, the Internet Stakeholders have been identified and the journey of the real space law to the new cyberspace laws is explained that may lead to unexpected results. The complexity of the internet is also explained. In part two the basic regulatory model for controlling the internet is given as follows: Legal Framework within individual countries, international cooperation and the changes in the architecture (or code) of the internet itself. In the later part, the concept of consensus and the problems of the cyberspace are attempted to be resolved. However, the author warns that if there is no solution in the existing laws, it is better to live it as it is, than to tinkering with the existing laws, as they may create newer problems. The author suggests six various regulatory models[27].

When it comes to questioning the requirement of new Internet law, as a separate field, many scholars say that the existing law can be stretched to encompass Internet-related issues. However irrespective of varied arguments relating to requirement of new laws for regulating the internet related transactions various body of statutory laws are developing all over the world with numerous pieces of individual legislations has been made in the US or as a Convention or as EC Directives or like that of India by enacting a special law relating to law for Internet transactions. However, the effectiveness of these legislations will always be a sort of limited because, there is a requirement of balancing large number of interests like that of the government, corporations, consumers, beyond these the economy in general and the international parties are a whole, where all the laws need to fulfill the international obligations. The government and the law makers are pressed by protecting various interests and therefore the resulting legislative results are frequently ill-considered and just reactionary. The existing institutions like the United Nations, Organization for Economic Cooperation and Development (OECD) and the EU, may be giving variety of models with an increasing support with other new legal institutions which may be both conceptual and practical with direct international negotiations by providing options to create most effective means with a legal and technical innovations to provide models in internet technologies as well a law to face the challenges of the Internet[28].

[27] David McPhie (2002)[27], Book Review, Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace, Stuart Biegel (Cambridge MA: The MIT Press Pp.452 ISBN 0-262-02504-3 Published in Harvard Journal of Law and Technology, Volume 15, Number 2 Spring 2002.

[28] L. Lessing, "The Law of the Horse: What Cyberlaw Might Teach", 113 Harvard law Review 501 cited in Yee Fen Lim, Cyberspace Law Commentaries and Materials, Oxford UP, Second Edition, Indian Edition, 2008(Chapter 1 at p 2-3)

"Cyberspace is a network of neighborhoods, businesses, and other nodes of social interaction, accessible from every continent, it is entirely man made, with an increasing variety of architectures"[29]. In Cyberspace[30], even though the architectures are largely invisible, the brilliance with which the WWW is created conceptualized and designed is aesthetic and pallid. In this article the author makes a comparison of the city of Venice and the dazzled contents of the Cyberspace. This comparison is supported by the author due to the diverse modes of artistic expression on the Internet-text, photographs, and the streaming media-play that so strongly attracts the viewers and users to have the visual experience. The sheer novelty and collective impact of the online visual experience that may have had its influence on some Internet visionaries to regard cyberspace like Venice: a place "outside" time and physical reality. The cyberspace has its foundation from its hardware and software that have certain weaknesses and instability. These artificial creations have made people vulnerable to be exploited and to put the users at personal and financial risks. The risks can sometimes be a gradual corrosion or a sudden catastrophic failure having a trivial to overwhelming impact because of the bugs from few glitches that can affect the Internet infrastructure to a full- blown system failures or deliberate assaults such as Distributed Denial of Services (DDoS) to attack on the robust computer system as a whole. These glitches and the catastrophic failures may have immediate impact as well long-term effect on public perceptions about the Internet and Computer Security[31]. So majorly to understand the economic crimes in the Internet infrastructure, it should be understood that the factors that influence the methods that are used by the criminals to commit the online economic crimes are[32]:

(1) The physical features of the Internet (i.e., the hardware and software that can govern what is technologically possible to do) and

(2) The psychological factors that influence people's interactions with others online.

So, it can be said that like the rest of the life has seen the physics and psychology as the great forces that affect the humans on decision making and action, when they interact with each other,

[29] Jonathan J. Rusch, Don't Look Now, 9 Geo Mason. L. Rev, 289, George Mason Law Review, Winter, 2000
[30]Ibid.
[31] Jonathan J. Rusch, Don't Look Now, 9 Geo Mason. L. Rev, 289, George Mason Law Review, Winter, 2000
[32] Ibid.

so does the cyberspace stand with the above factors in the everyday life. According to Lessing "The Code shapes the extent of liberty and control exercised over people in cyberspace"[33].

VI. DEVELOPMENT OF COMPUTER

According to the American Library Association: "Computer is a fast idiot; it has no imagination; it cannot originate action but it is a tool to man and will remain to be so"[34]. We are all mostly familiar with what a computer is in a specific, contemporary sense is. In the contemporary sense computers can also mean a personal computer that is found in most of aspects of our daily life. In this age it has become unimaginable to be in a world without computer or because of impossibility to work without a computer.

The computer of the modern times dates back to the early 19th century. It was Charles Babbage who invented the "difference engine". Later scientists continued their attempts to build a working computer and in 1943, IBM first constructed its mainframe computer, which was a five-ton Harvard Mark I. At this time, it was an era of mainframes and it lasted till 1980's[35]. The microprocessor that decreased the size and the cost of the computers was invented in 1971. In 1975 the Altair 8800, the first microprocessor computer was popularized in the Popular Electronics, which created the new "Personal Computers" and came in a kit form which had to be assembled. Many companies took up to customize this Altair and in 1976 the Apple II came up[36] and it was Jobs, who realized the importance of personal computers that could become the consumer product[37] while others were aiming to create the computers only for the computer enthusiasts[38]. By April 1977, the computer developed by the Apple and the Commodore Business Machines which adopted the same strategy, became an instant hit when it was first exhibited in West Coast Computer Faire. Later it was just the expansion of the variety of software's that were available in the market. The IBM personal Computers in 1981, the Macintosh by Apple in 1984 and eventually the developments in the Windows software that provided the GUI interface further increased the interest in the computers. More hardware and software's developed and evolved, but

[33] Cited in FN 41 by ParikshitKshrisagar, The problem of Identity Protection in Cyberspace and some suggestions, Working Paper Series, Electronic Copy Available at http://ssrn.com/abstract= 1520204, SSRN-id656272.doc (Last visited , June6, 2021)

[34]en.wikiquote.org/wiki/Libraries (Last Visited June7, 2021)

[35]Susan W. Brenner, Law in an Era of Pervasive Technology, 15, Widener. L.J 667, Widener Law Journal, 2006

[36]Steve Jobs and Stephen Wozniak created their Apple II in 1976.

[37]Ibid.

[38]Ibid.

it was in the 1990s that took a sudden and faster growth of personal computers through the rise of Internet.

VII. Internet Fraud/ Computer Fraud

The word Computer fraud is used in various ways, however to find any clear and precise definition of what is it actually being talked about is still in a dilemma though the warnings and dangers of 'Computer Frauds' and 'Internet Frauds' are frequently reported in the newspapers and other media. This dilemma prevails because there is no definite definition in the English Law relating to fraud other than a strong indication as to what are the essential elements of the word fraud. When the word fraud, which has been used since ages does not have a clear definition finding a definition for the computer fraud remains a problem due to its varied and unique nature. Even though the English law has not defined Fraud, there is a strong indication of what the courts have been interpreting the meaning of the word with the necessary elements of fraudulent conduct. In Re London & Globe Finance Ltd[39] the obiter dictum of Buckley J. was that fraud must have two essential elements are as follows:

a) Deception or concealment; and
b) Deprivation or loss to the victim.

So, the state of mind required for any act which is a fraud is done dishonestly to prejudice or to take the risk of prejudicing another's right, knowing that you have no right to do so[40]. Any offence of conspiracy to defraud is defined as an unlawful agreement that, if carried out, would result in the prejudice or risk of prejudice of another's rights. The Computer Misuse Act, 1990 has created three offences like:

a) Unauthorized access to a computer;
b) Unauthorized access with intent to commit a further offence;
c) Unauthorized modification of a computer.

The above offences do not require the element of any dishonest or fraudulent intent and are directed primarily at hackers and those who use computers to commit other crimes having first gained unauthorized access to the computer. This law as it is will not be applicable to any person who has any legitimate access to an Internet site but uses that to obtain investment for a fraudulent

[39](1903) 1 Ch. 728 at 733

[40] Cited in Simon Dawson, Computer Fraud: Part 1: The Risk to Business, Computer and Telecommunications Law Review, 1999.

scheme. Therefore, it can be generally thought that "Computer-fraud" means no more than "using a computer to commit fraud". However, this definition can be far too narrower, to be given to the word 'Computer Fraud' where many businesses may suffer as a result of fraud, when there is use or misuse of a computer. In this article the author has used a more extensive working definition of computer fraud: "Using a computer to cause prejudice, in the sense of financial and/or reputational damage, to a business".

As per the various types of computer frauds, most of the frauds have as their object in some kind of financial benefit to the fraudster and thereby a consequential financial loss to the victim. However, there are serious threats to business that may arises from activities that are not actually fraudulent in the traditional sense of law but which may nonetheless have the potential to cause damage to the reputation of a business.

As the Computer Frauds are very different from the conventional kinds of frauds due to its unique, technological and transnational nature, various reasons for dealing with them and the difficulty to reach the fraudsters have to be understood. First reason is the easiness in hiding due to the anonymous nature and toughness in detecting because of its difference from the conventional frauds. They are not easily recognizable in audit trail and the fraud is likely to be hidden in enormous volumes of data.

The second reason is difficulty of collecting evidence in computer crimes. The same is not only hard to find but it is also difficult to present to a court in a way that is legally and effectively admissible. People dealing with the computer crime/fraud like the prosecutors and the defense are well aware of problems in obtaining evidence and ensuring that the evidence can be complied with the relevant statutes and also in trying to explain the judge or jury, who may not be experienced in dealing with the electronic evidence and its admissibility. Thirdly, the easiness of committing the computer crimes is also one of the obvious reasons of complexity in understanding the required procedures like:

- It involves the manipulation of "invisible" data;
- It may only require a few key strokes;
- a computer can be remotely accessed, both by employees and outsiders;
- huge amounts of data can be transported on a single floppy disk which can be written to in a matter of seconds.

The use of the computers has become part of our daily life and their usage have become frequent and a necessity[41]. The greater number of persons use it; there is more opportunity for the fraudsters to commit fraud through the computers. So, computer frauds have become rampant. In the new world of Internet, there are hundreds of new stories coming up, and Internet is touted as a powerful new force that will allow companies to tap into a new market of investors to raise even more money than on traditional exchanges[42]. The companies and even the individuals are benefitted from this innovation called Internet, however they are still taking time to accept that they must now face the fact that the new medium makes them vulnerable to an increasingly extent because Cyberspace law is still undeveloped.

So, it is recommended that the same precaution which we take, to care of our homes, when we lock while going out and at night, are the few precautions that should be taken to prevent and avoid computer fraud also, that will make their way onto the computers. Though there are ways to lock even the computers, the perpetrators or the experts have the technique of breaking those locks. The criminals have overcome the hurdles in technology and under the vacuums of laws that are enacted in a snail phase compared to the stronghold of the perpetrators in cybercrimes.

The laws enacted in various States define computer fraud in various ways. As per Section 1030 of the "***Computer Fraud and Abuse Act of 1986 in US*, the Act while defining Hacker deals with the meaning of Computer Fraud and it has been defined as, "fraud and associated activity aimed at or with computers". The *CFAA* was amended in 1994, 1996 and later amended in 2001 by the USA PATRIOT**[43] **Act.** A conviction for violation of most of the provisions of the CFAA can be up to five years in prison and up to a $500,000 fine for a second offense". It also allows any target suffering damage or loss by reason of a violation of the CFAA to bring a civil action against the perpetrator for damages. As per the CFAA there are various computer crimes defined under the Act[44]. In *Theofel v. Farey Jones*[45], the U.S. Court of Appeals for the Ninth

[41] http://www.wisegeek.com/what-is-computer-fraud.htm Last visited on June 17, 2021.

[42] Jim Drinkhall, (1993) "Internet Fraud", Journal of Financial Crime, Vol. 4 Iss: 3, pp.242 - 244 Computer Fraud, Internet Fraud(www.emeraldinsight.com/10.1108/eb025785)

[43] This Act may be cited as the `Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

[44] The definition under the Act is:

1)Knowingly accessing a computer without authorization in order to obtain national security data

2) Intentionally accessing a computer without authorization to obtain:

Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.

Circuit convicted by using a civil subpoena for an act which was "patently unlawful", "bad faith" and "at least grossly negligent" to gain access to stored email is a breach of CFAA and the Stored Communications Act.[46]

VIII. Primary Risks in Computer Crimes/Frauds

The primary risks to the businesses from the computer's frauds are many. However basically they can be divided into two:

a) Internal Threats

b) External Threats

In these two internal risks are greater than the external risks, as in major surveys it is found that in 80% of cases of computer frauds involve the employees. And in many other cases the employee usually will have a collusion to commit the fraud[47]. Some of the major computer fraud threats from the employees are:

- Misappropriation of confidential information[48]
- Manipulation of payment systems to divert legitimate payments and the creation of "ghost" employees and suppliers.
- Collusive fraud with suppliers to create false invoices;
- Virus infection[49]

Information from any department or agency of the United States

Information from any protected computer if the conduct involves an interstate or foreign communication

3) Intentionally accessing without authorization, a government computer and affecting the use of the government's operation of the computer.

4) Knowingly accessing a protected computer with the intent to defraud and there by obtaining anything of value.

5) Knowingly causing the transmission of a program, information, code, or command that causes damage or intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in: Loss to one or more persons during any one-year period aggregating at least $5,000 in value.

The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals. Physical injury to any person; A threat to public health or safety; Damage affecting a government computer system

6) Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization.

[45] 2003 U.S. App. Lexis 17963, decided August 28, 2003

[46]http://en.wikipedia.org/wiki/cite_note-2#cite_note-2 last visited on June 10, 2021

[47] Audit Commission Report 1997, Cited in Simon Dawson, Computer Fraud: Part 1: The Risk to Business, Computer and Telecommunications Law Review, 1999

[48] This is not a new problem. Industrial espionage has a long and notorious history. What is worrying about electronic information is the ease with which it can be misappropriated and the difficulty of detecting that this has happened. Large quantities of sensitive data can be removed from a business on a single floppy disk without anyone ever knowing what has happened.

- Malicious alterations of e-mail[50].
- Personal use of computer systems involving staff running businesses; writing personal letters; copying company data for personal use; gaining unauthorized[51] etc.

Among the External threats, the danger of hacking is the most common one[52]. They usually cause loss to websites[53]. Hackers have now turned their attention to the high-profile activity of hacking into Internet sites of variety of organizations[54]. However, in such situations it is not difficult to imagine the damage that such similar attacks could cause to any business which is depended on the Internet. Another External threat that is rising day by day with varied kinds of fraudsters and victim is the Internet Fraud.

Internet fraud covers a wide range and variety of crimes. It includes the internet auction fraud[55] to the Nigerian Scams[56]. "Internet fraud is any type of intentional deception that uses the Internet. This includes fraud that occurs in chat rooms, message boards, Web sites and through email. It

[49] Not every virus outbreak is malicious. Most are accidental, and result from using unauthorized software or floppy disks. The tainted floppy disk is a very common means of transmitting viruses. The Audit Commission found that virus infection was the most common form of I.T. abuse, representing 48 per cent of all incidents. They give a typical example: when trying to load a file from a disk on to the computer of an NHS body, a virus was detected. Instead of following the approved policy of contacting the I.T. department and doing nothing further, the disk was inserted into several other computers until one was found that did not have a virus message. Unfortunately, this machine was not loaded with updated anti-virus software.

[50] This can happen when an employee has a grudge against another member of staff or a manager and can be troublesome, if not damaging.

[51]Internet access and downloading games and Internet pornography. In October 1998, two articles were published in Computer Fraud and Security relating to the increase in unauthorized employee use of the Internet at the time of the publication of the Starr report. One article warned that virus developers lay traps for unsuspecting users in areas of particular interest and noted a massive upsurge in unauthorized Internet access as sites were searched for information about the story. Another article noted that a plague of (usually obscene) "Bill and Monica" jokes and attachments was testing corporate I.T. defenses.

[52]The main threats from hacking are:

• removal of information;
• destruction of system integrity;
• transmission of viruses by e-mail;
• interception of e-mail;
• Interception of electronic payments.
• Interference with web pages.

[53]A website may be regarded as the ""shop window" of any company doing business on the Internet.

[54] Ibid.

[55] There are various types of Auction Frauds, Bid Shielding, Shill Bidding, and Non- delivery of the products/services auctioned by the seller, Nonpayment by the buyer after being the highest bidder or delivering a good which is much below the quality that was promised.

[56] According to the Internet Crime Report prepared by the Federal Bureau of Investigation, in 2007, Internet fraud resulted in the loss of "$239.09 million with a median dollar loss of $680.00 per complaint," an increase of $40.65 million from 2006. This is an article by Darcy Logan on Definition on Internet Fraud available at http://www.ehow.com/facts_4856098_what-definition-internet-fraud.html

occurs in the form of deceitful solicitations and fraudulent transactions"[57]. Among the Internet frauds, the most common type is internet Auction fraud, which has the 35-40% of complaints. The other most common internet fraud is the non-Deliverable merchandise and payment, which has been reported to be nearing 25%[58]. Such frauds include multi-leve marketing and home improvement scams. During the online transactions when the payments are made or processed there are chances of credit card fraud, debit card fraud, cheque frauds, computer frauds, identity theft and other financial frauds. Among these financial frauds, the investment frauds and the cheque frauds are rampant[59]. A scheme to defraud persons by using the internet is, as a primary means of communication can be considered to be a simple definition of internet fraud. It can entail through the WWW, Internet Relay Chat (IRC), e-mails, or instant messaging. But there is no statutory definition which can precisely define the exact meaning of the term internet fraud. It can only be understood, through various other definitions which are implications of internet fraud from the existing statues or laws. In this comment, Leda Mouallem (2002) articulates as to why most of the Internet frauds have antecedents in the Telemarketing Fraud. The size of the potential market; the relatively easy access and low cost with the required speed are the major factors for the perpetrators of scam. Even in the earlier days the elderly has been the victims of the consumer frauds and telephone have been the most popular medium among the perpetrator of fraud. Though the government and law enforcement agencies have been battling telemarketing fraud for years, the fraud has increased due to the newest guise threatening elderly persons is Internet Consumer Fraud. The author first gives the reasons for elderly being the target of such fraud, then the various types of telemarketing fraud schemes. In the next part the author places all the laws relating to the fraud like the Telephone and Consumer Fraud and Abuse Prevention Act, 1994 and the Telemarketing Sales Rule, Senior Citizens against Marketing Scams Act, 1991 and the Seniors Safety Act, 1999. Among these laws, SSA addresses the *Internet Fraud* especially if it is perpetrated against the elderly. The SSA (proposed) expands the existing telemarketing regulatory legislation by attempting to curtail the use of internet as a means by which telemarketers perpetrate fraud. As Internet is the modern-day analogue to the telephone calls it has been expanded to include "wire communications utilizing a phone service". But this inclusion by itself

[57] Ibid FN 34 (http://www.ehow.com/facts_4856098_what-definition-internet-fraud.html)

[58] This percentage is as per the 2007 study by (http://www.ehow.com/facts_4856098_what-definition-internet-fraud.html)

[59] FBI: Internet Fraud, U.S. Department of Justice: Internet and Telemarketing Fraud,2007 Internet Report, The Crime of Fraud, (http://www.ehow.com/facts_4856098_what-definition-internet-fraud.html)

is not sufficient, as the new technology may be wireless technology or there may be no phone service required to communicate. The same kind of frauds, which were exiting in the telephone services, has surged into the Internet and beyond where alternative devices can be used. In the analysis the author touches upon the anonymity and Internet Fraud. But the void in having an effective legislation may make the internet fraud rampant and imminent. In the proposal part, the author suggests legislations, education programs, the use of privacy through encryption; Digital Signatures, technical developments for securing the internet, etc. In the conclusion, author suggests that the congress should take steps to combat the Internet fraud to protect the elderly[60].

In India the term *Internet Fraud* has been given a very comprehensive meaning but it has not been specifically defined under the IT Act. As there is no specific definition provided under the Act, the word Internet Fraud can possibly include all frauds that are committed through Internet.[61] However there is difficulty of specifically classifying these frauds[62]. However, computer crimes, cybercrimes or in specific, the Internet fraud, can be considered to be new species of white-collar crime. The crime rate of internet frauds is growing in the same speed as that of the speed of the internet itself[63]. Most of the frauds in the internet take place during the online transactions like that of online auctions[64]. Generally, the frauds have been committed in a large way since time immemorial and computer and internet are the new tools used in committing crimes, as it is easier to alter the information as the input into a system or just as a manipulation in the operation of the programs, their processing of the information, till the altering of the output is very easy. This is the modern tool used by the perpetrators or the defendants to carry out their illegal or unlawful actions.

[60] Leda Mouallem- Oh No, Grandma Has a computer: How Internet Fraud Will Take the Place of Telemarketing Fraud Targeting the Elderly. 42 Santa Clara. Rev. 659 (Santa Clara Law Review 2002)

[61] An Introduction to Cyber Crime and Cyber Law, Dr. R K Chaubey, Chapter 7 at P 419-20, 2008. Edition, Kamal Law House

[62] However, in the IT Act, 2000 and IT AA ,2008 the word dishonestly and fraudulently, as defined in the Indian Penal Code ,1860 in sections 24 and 25 respectively are applicable to any fraud or dishonest act, committed under the IT Act.

[63] Ibid at P 419

[64] An Introduction to Cyber Crime and Cyber Law, Dr. R K Choubey, 2008 Edition, Kamal Law House. Chapter 7 at P 419-21

IX. CONCLUSION:

In India after the enactment of the IT Act, 2000 and the Amendment of the IT Act, 2008 the legislation has defined certain offences[65] and they are till date adequately used to prosecute or take action against the perpetrator. But the rise in the various types of crimes and the mode of its commission, the terminologies used are not been complete in its application and the law might not be adequate to bring in all the offences within the ambit of the laws.[66] The technology is as usually growing faster than law and it needs to take phase to safeguard the users of computer, internet and any other course in the internet world.

The choice and convenience in which the businesses can operate in the electronic marketplace has seen an unprecedented growth. The internet has given low-cost access to a global consumer base. The benefits have certainly added to the kitty of the business. However, with these benefits and profits for the businesses there are certain challenges in the virtual marketplace and puts pressure on the stakeholders of the Internet, when it comes to the question of a safe and secure place to purchase the goods, services and the digitalized information. As the e-commerce has grown, the law enforcements agencies have observed that there are a large number of fraudulent schemes that are growing in various forms with the use of Internet. The fraudsters communicate in the global market place with false and fraudulent representations to the prospective victims either to obtain their personal information or certain other resources that are necessary for the successes of their schemes[67].

In this Report the Vice President of US Al Gore said in 1999**:**

"Unlawful activity is not unique to the Internet - but the Internet has a way of magnifying both the good and the bad in our society... [W]hat we need to do is find new answers to old crimes".

The Attorney general Janet Reno in this Report quoted that:

"While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behavior".

[65] In chapter 9of IT Act,2000, Sec 43, 43A, 66, 66A 66B, 66C, 66D, 66E, 66F, 67, 67A,67B,72,72A

[66] An Introduction to Cyber Crime and Cyber Law, Dr. R K Choubey, 2008 Edition Kamal Law House. Chapter 7 at P 422

[67] The President's Working Group on Unlawful Conduct on the Internet, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the use of the Internet, March 2000. Available at http://www.justice.gov/criminal/cybercrime/unlawful.htm (Last visited November, 04, 2010)

Among many forms of Internet related crimes, Internet frauds that have a specific concern is 'Identity Theft', which generally is a scheme involved to obtain data from the individual consumers about relating to their financial transactions on the Internet or elsewhere. It includes those transactions where the consumer credit cards are billed for some nonexistent transactions or services. Some companies even purport to offer investments in nonexistent items, securities, software's, goods and services including the online auctions services. Some use Internet as a single path to commit the fraud, while in few forms of fraud the perpetrators may use a combination of internet websites, with the telemarketing 'boiler rooms' to develop direct contact with the prospective victims. Some fraud schemes are very efficient and contact the victims in multiple jurisdictions or more effective in evading prompt detection and investigation by the law enforcement. As the Internet Frauds transcends the traditional jurisdictional boundaries, it poses special challenges to the Internet Fraud investigators.