# LEGAL CONTROL OF CYBER CRIMES

**HARSHITA AGARWAL**

**Submitted under the guidance of: Dr. Venu Gopal**

***This dissertation is submitted in partial fulfillment of the degree of***

***B.B.A., LL.B. (Hons.) in Corporate Laws***

**College of Legal Studies**

**University of Petroleum and Energy Studies**

**Dehradun**

**2015**

## CERTIFICATE

This is to certify that the research work entitled **"Legal Control of Cyber Crimes"** is the work done by Harshita Agarwal under my guidance and supervision for the partial fulfillment of the requirement of B.B.A., LL.B. (Hons.) at College of Legal Studies, University of Petroleum and Energy Studies, Dehradun.

This dissertation is fit for submission and evaluation for the above purpose.

**Dr. Venu Goapl**
**Professor**
**COLS, UPES**

**Date:**

## DECLARATION

I declare that the dissertation titled **"Legal Control of Cyber Crimes"** is the outcome of my own work conducted under the supervision of Dr. Venu Goapl, Professor, at College of Legal Studies, University of Petroleum and Energy Studies, Dehradun.

I declare that the dissertation comprises only of my original work and due acknowledgement has been made in the text to all other material used.

**Harshita Agarwal**

**Date:-**

# CONTENTS

# CHAPTER I

# INTRODUCTION

With liberalization, the Indian economy opened to the global markets and it was the start of the development of India globally. Liberalization brought about growth in various sectors and touched every household in India. But one of the star features of liberalization was information technology revolution that it brought about. Information technology facilitated liberalization and people adopted the useful technology to grow and develop. With the increased use of the information technology, some people found ways to misuse the very same information technology to fulfil their illegal or bad intentions. The technology was new to India but not to other countries like US. Information technology helped people to connect formally as well as informally and helped reduce the distance between people. It broke the barriers to communication and promoted free flow of information. But like everything has its pros and cons, information technology too had its pros and cons.

Web is a marvelous bit of data innovation and has ended up crucial piece of our lives. It has made existence of individuals simple the same number of the distinctive administration offered by the legislature can be profited through web, additionally diverse administration of purchasing and offering can be benefitted through web. Web has given a computerized business sector to the individuals everywhere throughout the world. All the main, organization are currently days are putting forth their item through web. As it give one of the biggest markets for the organization. Yet, genesis of new innovations prompted ascent of new open door for its ill-use, which thus offer ascent to legitimate limitation and arrangement of new dangers have formed with our move into data age. New mechanical advancements and an expanded dependence on PC based innovation has created a shift in origination of digital wrongdoing for all created and creating nations. This wrongdoing is the same as other manifestation of wrongdoing like trespass, intrigue, burglary and so forth. The genuine effect of the digital wrongdoing was felt without precedent for the real world with the evaluated misfortunes of property, significant databases, systems and data, aside from human life. The web has given terrorists nature a fatal new weapon in their armory. Indeed, even in assault on 26/11 or assault on WTO uncovered on examination that web was widely utilized for arranging and execution of

the assault. As the web contain a virtual reference book of data that the terrorists can use to plan and execute each part of these sorts of assaults. It likewise furnishes them with worldwide system over which they can trade data and convey, hack touchy information bases and obtain assets. This all movement of wrongdoing everywhere throughout the world has affirmed the dread that the internet can be successfully utilized for the terrorist exercises, offering emerge to new manifestation of wrongdoing "digital terrorism". The part of terrorism is that of advanced hoodlum who can take more with the PC than with the firearm. The terrorist may have the capacity to accomplish more harm with a console than with a bomb. An increment in digital war initiates is calm likely, as in 21st century will be battled on the web and in the internet as opposed to in this present reality.

Terrorism and the web are interrelated. The web has given new stage to terrorist gatherings and individual terrorist use it to spread their message of contempt and savagery and to convey the same. These offenders may be delegated digital terrorists whether they singularly depend on digital terrorism to further their reason or whether they utilize it as a part of expansion to other more ordinary manifestations of terrorism. These terrorists are utilizing web more than assaulting it. They utilize it to send encoded email or to spread their publicity. The trepidation encompassing digital terrorism is that terrorists and criminal infiltrate framework PC framework and imperil human lives by upsetting military systems; telecom and so forth digital terrorism is another instrument as are unstable and programmed weapons. Assault on PC frameworks can go unnoticed even after entrance. A digital terrorist may be in the framework a few times before the demonstration happens for surveillance or experimentation.

Digital terrorism is the new type of terrorism, which misuses the framework we have put set up. With the episodes of digital terrorism it is grievously clear that terrorism has come to new level of refinement. As opposed to utilizing conventional technique for executing, taking prisoner and guerrilla fighting, terrorists now utilize the web to bring about much more extensive harm to a nation. PC is the new device which they use for their movement despite the fact that it is utilized in a roundabout way. This joining of the physical and virtual planets, this grid, is becoming bigger and more unpredictable as we wander further

into mechanical reliance. We are getting to be much all the more inseparably dependent and subject to union of these planets[1].

But the use of internet is inevitable to keep pace with the fast growing world. It facilitated business between different countries and provided for e- business, e- commerce, e- governance and e- procurement. The information technology has impacted every household in some or the manner. To mention a few are as following-

1. Trading in the stock market through demat forms.
2. Mostly companies keep their records and valuable data or client information in the electronic mode.
3. To make it convenient and decrease the burden of papers, many forms are now filled online only be it the income tax returns or the other various forms required to be filled by the companies at various stages.
4. The amount of people switching over to online shopping has tremendously increased due to its benefits and, therefore, use of debit and credit cards has also increased.
5. Use of various social networking websites and e- mails to communicate.
6. Digital signatures and e- contracts
7. But not just limited to above which lists the various ways of cyber crimes, the computers also give important evidences in other cases like of murder, frauds, kidnappings, tax evasions, etc[2].

All of the above require users to store in their personal information over the computer and other details also like bank details for online shopping which attracts the prospective cyber criminals.

With increase in use of the technology in terms of illegal usage of the information technology in terms of various crimes inclusive of terrorism, it required a check. But it involved a major problem as to detect the source or origin of the illegal act. The other major issue it involves is its wide spread nature which creates jurisdictional problems for the Governments and what law shall be applicable. These are the reasons which

[1] R.C. Mishra, "cyber crime: Impacts in the new millennium" pg. 47-48(2202)

[2] http://www.indiancybersecurity.com/cyber_law/2_need_of_cyber_law.html

motivated the Governments of various countries to enact the cyber laws to check upto their capacity and extent[3].

The Government of India also enacted the Information Technology Act, 2000 (referred to as "the IT Act") which was further amended in 2008. The amendment was a much required change in light of the unimaginable advancements in the field of information technology. Besides the particular codified law in India, there are some general laws also in this respect which have been framed as early as in the 19th century. But those did not suffice the growing level of crimes committed on the forum, thereby, paving way for a specialized enactment. The general laws referred to are the Indian Penal Code, 1860 (IPC) which is the penal code and the Indian Evidence Act, 1872 (Evidence Act) which lays down the laws pertaining to the admissibility of evidences in both civil as well as criminal trials[4].

[3] http://www.insightsonindia.com/2014/12/14/effects-liberalization-indian-economy-society/

[4] Cyber Crime Law in India: Has law kept pace with the emerging trends? An Empirical Study by N.S. Nappinai, Journal of International Commercial law and Technology, Vol. 5, Issue 1 (2010)

## *HISTORY OF CYBER CRIME IN INDIA*

As stated earlier that information technology is wide spread and therefore, the countries faced the problem of jurisdiction and the applicable law. So, a resolution was passed in the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce on International Trade Law. The Model law required the states to adopt the Model Law according to the domestic legal regime so that all the countries have a uniform legal system regarding the cyber crimes applicable to alternatives to paper based methods of communication and storage of information.

In pursuance of the same a bill was drafted by the Department of Electronics (DoE) in July 1998 but that could not be presented in the house for around next one and a half years. It was introduced in the House on December 16, 1999 after the new IT ministry was formed. It had under gone substantial changes to be in line with the World Trade Organization (WTO) obligations and regulations regarding e- commerce which were suggested by the Commerce Ministry. And finally the joint draft was vetted by the Ministry of Law and Company Affairs.

After it was introduced in the House, the bill came under a 42- member Parliamentary Standing Committee due to demands made by the members. Many suggestions were made by the Standing Committee, one of them being which was argued over a lot, related to maintenance of registers by the cafe house owners. It required the cafe house owners to maintain a database in the form of a register which shall record the details of the people who use the services of the cafe and also the websites they visit but it was contradicted stating that it would invade upon an individual's right to privacy to surf the net. Not all but only those suggestions which were finalized by the Ministry of Information Technology were incorporated and, however, the suggestion of maintaining registers was not taken in the final draft by the Ministry.

The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000; both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000[5].

[5] http://www.indiancybersecurity.com/cyber_law/8_history_of_cyber_law_in_india.html

## *DATA OF CYBER CRIMES IN INDIA*

The National Crime Records Bureau (NCRB) shows as per its data that 4192 cyber crimes were recorded in 2013 only in States in comparison to 2012 which recorded a total of 2761 cyber crimes, showing a variance of around 51.8%. Maharashtra was to lead the race and recorded a total of 681 cyber crimes in 2013 which was 471 in number in the year 2012. These crimes were booked under only the IT Act. Under the IPC, Uttar Pradesh lead recording a total of 310 cases in the year 2013[6].

As per the records of the NCRB the most vulnerable age group to the cyber crimes are people aged 18-30. A total of 1163 number of cyber crimes in the states only have been recorded under the IT Act only to have been committed by the particular age group[7].

Under the provisions of IPC, there have been no crimes committed by teenagers but people aged 30-45 have been the most vulnerable in this category, recording a total number of 598 crimes in the states[8].

NCRB has also given data which shows the incidence of cases registered under various categories of cyber crimes. NCRB had collected data in regard of the following crimes-

1. Tampering computer source documents
2. Hacking with computer systems
    i. Loss/ damage to computer security
    ii. Hacking
3. Obscene publication/ transmission in electronic form
4. Failure
    i. Of compliance/ orders of certifying Authority
    ii. To assist in decrypting the information intercepted by the Government Authority
5. Unauthorized access/ attempt to access of protected computer system

[6] National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, Incidence of cases registered under Cyber Crimes

[7] National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, Persons arrested under IT Act by Age- group

[8] National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, Persons arrested under IPC sections of Cyber Crimes by Age- group

6. Obtaining License or Digital Signature Certificate by misrepresentation/ suppression of fact
7. Publishing false Digital Signature Certificate
8. Fraud Digital Signature Certificate
9. Breach of confidentiality/ privacy
10. Other

The maximum numbers of cases were registered under Hacking causing loss/ damage to computer security. Hacking is the most common type of cyber crime and many people have been affected of it. A total of 1966 cases were registered and around 818 arrests were made. Hacking can lead to commission of further cyber crimes by collecting information from the computer system which may be confidential or bank details or other account details.

The offences under IPC which were considered by NCRB are as follows-

1. Offences by/ Against public servant
2. False electronic evidence
3. Destruction of electronic evidence
4. Forgery
5. Criminal breach of trust/ Fraud
6. Counterfeiting
    i. Property/ Mark
    ii. Tampering
    iii. Currency/ stamps

Forgery is another very common type of cyber crime booked under the provisions of the IPC. It registered a total of 747 cases and 626 arrests were made[9].

[9] National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, incidence of Cases registered and number of Persons Arrested under Cyber crimes (IPC+ IT) During 2013

# CHAPTER II

# INFORMATION TECHNOLOGY ACT, 2000

Information Technology Act was the first codified law in India in the field of cyber crimes but the IT Act could not keep pace with the global requirements. The initial aims of the IT Act were to facilitate e- commerce in the country and give sanctity to the electronic records as well as their protection. But with the 2008 Amendment Act the Act was made capable to make the illegal acts over the cyber space punishable which was not the case before.

The IT Act, 2000 came at a time when cyber-specific legislation was much needed. It filled up the lacunae for a law in the field of e-commerce. Taking cue from its base-document, i.e. the UNICITRAL Model Law on electronic commerce, adopted in 1996, a law attuned to the Indian needs has been formulated. Apart from e-commerce related provisions, computer crimes and offences along with punishments have been enumerated and defined. The powers of the police to investigate and power of search and seizure, etc have been provided for. However, certain points need a re-working right from the scratch or require revamping.

At the first instance, though the IT Act, 2000 purports to have followed the pattern of the UNICITRAL Model Law on Electronic Commerce, yet what took people by surprise is its coverage not only of e-commerce, but something more, i.e. computer crime and amendments to the Indian Penal Code. The UNICITRAL Model Law did not cover any of the other aspects. Therefore in a way, the IT Act, 2000 has been an attempt to include other is sues relating to cyber world as well which might have an impact on the ecommerce transactions and its smooth functioning. Though, that of course is not reflected even from the Statements of Objectives and reasons or the preamble of the Statute. Amendments to the Indian evidence Act are evidently made to permit electronic evidence in court. This is a step in the right direction.

Secondly, a single section devoted to liability of the Network Service Provider is highly inadequate. The issues are many more. Apart from classification of the Network Service provider it there can be various other instances in which the Provider can be made liable especially under other enactments like the Copyright Act or the Trade Marks Act.

However the provision in the IT Act, 2000 devoted to ISP protection against any liability is restricted only to the Act or rules or regulations made there under. The section is not very clear as to whether the protection for the ISP‟s extends even under the other enactments.

It has been argued that the Act of this nature would divide the society into digital haves and digital have-nots. This argument is based on the premise that with an extremely low PC penetration, poor Internet connectivity and other poor communication infrastructure facilities, a country like India would have islands of digital haves surrounded by digital have-nots. Logically speaking, such an argument is untenable as the "digital core" has been expanding horizontally and everyday communication connectivity is rising across India.

There has been a general criticism of the wide powers given to the police under the Act. Fear, especially among cyber café owners, regarding misuse of powers under the IT Act, 2000 is not misplaced. Anyone can be searched and arrested without warrant at any point of time in a public place. But at the same time, the fact that committing a computer crime over the net and the possibility of escaping thereafter is so much more viable, that providing such policing powers check the menace of computer crimes is also equally important. Yet this is no reason for giving draconian powers to the police. For example, interception of electronic messages and emails might be necessary under certain situations but the authorities cannot be given a free- hand in interception as and when they feel. Similarly, we need to enquire and delve deeper into the police power of investigation, search and warrant under the IT Act, 2000 and look for a more balanced solution.

In addition to this, various other Advantages and Disadvantages of the IT Act, 2000 can be attributed which are highlighted below:-

## *MERITS*

The Act offers the much- needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.

Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

Second, Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Third, Digital signatures have been given legal validity and sanction in the Act.

Fourth, the Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

Fifth, the Act now allows Government to issue notification on the web thus heralding e-governance.

Sixth, the Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

Seventh, the IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Eighth, under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

## *LACUNAE*

The IT Law 2000, though appears to be self sufficient, it takes mixed stand when it comes to many practical situations. It loses its certainty at many places like

First, the law misses out completely the issue of Intellectual Property Rights, and makes no provisions whatsoever for copyrighting, trade marking or patenting of electronic information and data. The law even doesn't talk of the rights and liabilities of domain name holders, the first step of entering into the e-commerce.

Second, the law even stays silent over the regulation o f electronic payments gateway and segregates the negotiable instruments from the applicability of the IT Act, which may have major effect on the growth of e-commerce in India. It leads to make the banking and financial sectors irresolute in their stands.

Third, the act empowers the Deputy Superintendent of Police to look up into the investigations and filling of charge sheet when any case related to cyber law is called. This approach is likely to result in misuse in the context of Corporate India as companies have public offices which would come within the ambit of "public place" under the Act. As a result, companies will not be able to escape potential harassment at the hands of the DSP.

Fourth, internet is a borderless medium, it spreads to every corner of the world where life is possible and hence is the cyber criminal. Then how come is it possible to feel relaxed and secured once this law is enforced in the nation?

Fifth, the Act initially was supposed to apply to crimes committed all over the world, but nobody knows how can this be achieved in practice, how to enforce it all over the world at the same time?

Sixth, the IT Act is silent on filming anyone's personal actions in public and then distributing it electronically. It holds ISPs (Internet Service Providers) responsible for third party data and information, unless contravention is committed without their knowledge or unless the ISP has undertaken due diligence to prevent the contravention. This is a practically impossible approach.

Further according to the researcher, the recently proposed IT Act, 2000 amendments are neither desirable nor conducive for the growth of ICT in India. They are suffering from numerous drawbacks and grey areas and they must not be transformed into the law of the land. These amendments must be seen in the light of contemporary standards and requirements. Some of the more pressing and genuine requirements in this regard are as follows-

1. There are no security concerns for e- governance in India.
2. The concept of due diligence for companies and its officers is not clear to the concerned segments.
3. The use of ICT for justice administration must be enhanced and improved.
4. The offence of cyber extortions must be added to the IT Act, 2000 along with Cyber Terrorism and other contemporary cyber crimes.
5. The increasing nuisance of e- mail hijacking and hacking must also be addressed.
6. The use of ICT for day to day procedural matters must be considered.
7. The legal risks of e-commerce in India must be kept in mind.
8. The concepts of private defence and aggressive defence are missing from the IT Act, 2000.
9. Internet banking and its legal challenges in India must be considered
10. Adequate and reasonable provisions must be made in the IT Act, 2000 regarding "Internet censorship"
11. The use of private defence for cyber terrorism must be introduced in the IT Act, 2000
12. The legality of sting operations (like Channel 4) must be adjudged.
13. The deficiencies of Indian ICT strategies must be removed as soon as possible.
14. A sound BPO platform must be established in India, etc.

The act, on an overall analysis, demonstrates a lack of discussion and incorporation of various issues relating to cyber law. Through the Act has been given the name „Information Technology Act" yet many legal many legal issues like online rights of cons umers, privacy concerns, domain names disputes, payment and security-bugbears, etc have not been addressed. Finally, how the act will be implemented by a Court of law and its implementation and flaws in the long run are yet to be tested in the case-specific factual terrain[10].

[10] Cyber Crimes and effectiveness of Laws in India to Control Them, Mubashshir Sarshar, January 2009, NLUD

## *INFORMATION TECHNOLOGY ACT, 2008*

In the year 2000, India enacted its first law on Information Technology namely, the Information Technology Act, 2000. The IT Act, 2000 is based on the Model law of Ecommerce adopted by UNCITRAL in 1996. The preamble to the IT Act, 2000 points out a threefold objective , firstly, to provide legal recognition for transactions carried out through electronic means, secondly, to facilitate the electronic filing of documents with government agencies, and thirdly to amend certain Acts, interalia, the Indian Penal Code,1860, Indian Evidence Act, 1872. The IT Act, 2000 gave legal validity and recognition to electronic documents and digital signatures and enabled conclusion of legally valid & enforceable e-contracts. It also provided a regulatory regime to supervise the Certifying Authorities issuing digital signature certificates and created civil and criminal liabilities for contravention of the provisions of the IT Act, 2000.

(1) Electronic signatures introduced: With the passage of the IT (Amendment) Act, 2008 India has become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures. This is a positive change as India has different segments people and all may not be technologically adept to understand and use the digital signatures .Further, in a move to secure the flow of data and information on the internet, and promote e-commerce & e governance, the amended Act in Section 84A has empowered the Central Government to prescribe modes or methods for encryption. These parameters should be laid down in consultation with organizations such as Nasscom and/or governmental agencies that can assist in formulation of necessary standards and related rules.

(2) Corporate responsibility introduced in S. 43A The corporate responsibility for data protection is incorporated in S 43A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of ‘reasonable security practices‟ to maintain its secrecy, failing which they may be liable to pay damages. Also, there is no limit to the amount of compensation that may be awarded by virtue of this section. This section must be read with Section 85 of the

IT Act,2000 whereby all persons responsible to the company for conduct of its business shall be held guilty incase offence was committed by a company unless no knowledge or due diligence to prevent the contravention is proved.

(3) Important definitions added Two very important definitions are added to the IT Act through IT Amendment Act,2008- Section 2(ha)- "Communication device " and Section 2 (w) –"intermediary". Although cell phones and other devices used to communicate would fall under the definition of computer in the IT Act. This amendment removes any ambiguity and brings within the ambit of the Act all communication devices, cellphones, ipods or other devices used to communicate, send or transmit any text ,video ,audio or image. The insertion of definition of „intermediary" similarly clarifies the categories of service providers that come within its definition that includes telecom service providers, network service providers, internet service provider, webhosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes.

(4) legal validity of electronic documents re-emphasized : Two new sections Section 7A and 10A in the amended Act reinforce the equivalence of paper based documents to electronic documents. Section 7A in the amended Act makes audit of electronic documents also necessary wherever paper based documents are required to be audited by law. Section 10A confers legal validity & enforceability on contracts formed through electronic means. These provisions are inserted to clarify and strengthen the legal principle in Section 4 of the IT Act, 2000 that electronic documents are at par with electronic documents and e-contracts are legally recognized and acceptable in law. This will facilitate growth of e-commerce activity on the internet and build netizen"s confidence.

(5) The Role of Adjudicating officers under the amended Act: The Adjudicating officer „s power under the amended Act in Section 46 (1A) is limited to decide claims where claim for injury or damage does not exceed 5 crores. Beyond 5 crore the jurisdiction shall now vest with competent court. This has introduced another forum for adjudication of cyber contraventions. The words „competent court" also needs to be clearly defined. As per Section 46(2), the quantum of compensation that may be awarded is left to the discretion of Adjudicating officers. This leaves a wide room for subjectivity and quantum should be decided as far as possible objectively keeping in view the parameters of amount of unfair advantage gained amount of loss caused to a person (wherever quantifiable), and repetitive nature of

default. The Information Technology (qualification and experience of adjudicating officers and manner of holding enquiry) Rules, 2003 lay down the scope and manner of holding inquiry including reliance on documentary and other evidence gathered in investigations. The rules also provide for compounding of contraventions and describe factors that determine quantum of compensation or penalty.

(6) Composition of CAT The amended Act has changed the composition of the Cyber Appellate Tribunal .The Presiding officer alone would earlier constitute the Cyber Regulations Appellate Tribunal which provision has now been amended. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint. The qualifications for their appointment, term of office salary , power of superintendence, resignation and removal, filling of vacancies have been incorporated. The decision making process allows more objectivity with Section 52 D that provides that the decision shall be taken by majority. It is pertinent to note that there has not been any amendment in Section 55 by 2008 amendments which states that no order of CAT shall be challenged on ground that there existed a defect in constitution of appellate tribunal. However, in my view this runs contrary to principles of natural justice. An analogy is drawn to Arbitrations where defect in constitution of a tribunal renders an award subject to challenge as per Indian laws.

(7) New cybercrimes as offences under amended Act Many cybercrimes for which no express provisions existed in the IT Act,2000 now stand included by the IT (Amendment) Act, 2008. Sending of offensive or false messages (s 66A), receiving stolen computer resource (s 66B), identity theft (s 66C), cheating by personation (s 66D), violation of privacy (s 66E). A new offence of Cyber terrorism is added in Section 66 F which prescribes punishment that may extend to imprisonment for life . Section 66 F covers any act committed with intent to threaten unity integrity,security or sovereignty of India or cause terror by causing DoS attacks, introduction of computer contaminant, unauthorized access to a computer resource, stealing of sensitive information, any information likely to cause injury to interests of sovereignty or integrity of India, the security, friendly relations with other states, public order, decency , morality, or in relation to contempt of court, defamation or incitement to an offence , or to advantage of any foreign nation, group of individuals or otherwise. For other offences mentioned in

Section 66 , punishment prescribed is generally upto three years and fine of one/two lakhs has been prescribed and these offences are cognisable and bailable. This will not prove to play a deterrent factor for cyber criminals. Further, as per new S. 84B, abetment to commit an offence is made punishable with the punishment provided for the offence under the Act and the new S. 84C makes attempt to commit an offence also a punishable offence with imprisonment for a term which may extend to one half of the longest term of imprisonment provided for that offence.

(8) Section 67 C to play a significant role in cyber crime prosecution Section 67 C brings a very significant change in the IT Act,2000 .According to this section, intermediaries shall be bound to preserve and retain such information as may be prescribed by the Central government and for such duration and format as it may prescribe. Any intermediary that contravenes this provision intentionally or knowingly shall be liable on conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lac or both. Many cybercrime cases cannot be solved due to lack of evidence and in many cases this is due to the fact that ISP failed to preserve the record pertaining to relevant time .This provision is very helpful in collection of evidence that can prove indispensable in cybercrime cases.

(9) Section 69B added to confer Power to collect, monitor traffic data .As a result of the amendments in 2008, Section 69 B confers on the Central government power to appoint any agency to monitor and collect traffic data or information generated ,transmitted, received, or stored in any computer resource in order to enhance it cybersecurity and for identification, analysis, and prevention of intrusion or spread of computer contaminant in the country . The Information Technology (procedure and safeguard for monitoring and collecting traffic data or information ) Rules, 2009 have been laid down to monitor and collect the traffic data or information for cyber security purposes under Section 69B .It places responsibility to maintain confidentiality on intermediaries, provides for prohibition of monitoring or collection of data without authorization. This prescribes stringent permissions required to exercise the powers under this Section which are fully justified as abuse of this power can infringe the right to privacy of netizens. It also provides for review of its decisions and destruction of records. The intermediary

that fails to extend cooperation in this respect is punishable offence with a term which may extend to 3 yrs and imposition of fine.

# CHAPTER III

# CYBER SECURITY

The UN 2010 general Assembly Resolution also underlined cybercrime as one of the major threats posing to the world[11]. Cyber security is very important to protect the cyberspace and help in the further development of the information technology. Not just promoting the information technology but it is important for the security of the nation also. Because the highly developed technology is used by the Government also for its communication and any illegal activity in that cold prove to be fatal to the security of the nation also. But it does not have to be only a Governmental initiation but participation from other stakeholders is also required. Other stakeholders include the public at large and in general. The Department of Electronics and Information Technology (DeitY) has drafted a cyber security strategy which aims to be implemented by following methods-

i. Security Policy, Compliance and Assurance
ii. Security Incident Early Warning & Response
iii. Security training skills/ competence development & user end awareness.
iv. Security R&D for securing the infrastructure, meeting the domain specific needs and enabling technologies
v. Security promotion & publicity[12].

Cyber security is very important to fight against the cyber crimes and, therefore, their advancement and support is also very essential. As stated earlier that cyber crimes have no jurisdiction and are far spread and hence need a global reach towards them and that can be only done within a framework of international cooperation. Cyber security involves legal, technical and institutional issues and all the three elements are complex for the very same reason of their wide reach and international cooperation. The World Summit for the Information Society (WSIS) in its Tunis Agenda for Information Society has laid down a framework for multi stakeholder implementation at the international level which is called the WSIS Plan of Action explaining the multi stakeholder implementation

[11] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

[12] http://deity.gov.in/content/cyber-security-strategy

process according to eleven action lines and allocating responsibilities for facilitating implementation at different lines. The WSIS Action Plan states the following-

i. The role of governments and all stakeholders in the promotion of ICTs for development
ii. Information and communication infrastructure: an essential foundation for the Information Society
iii. Access to information and knowledge
iv. Capacity building
v. Building confidence and security in the use of ICTs
vi. Enabling environment
vii. ICTs application: benefits in all aspects of life like business, health, environment, employment, etc
viii. Cultural diversity and identity, linguistic diversity and local content
ix. Media
x. Ethical dimensions of the Information Society
xi. International and regional cooperation[13].

[13] http://www.itu.int/wsis/docs/geneva/official/poa.html

# CHAPTER IV

# CYBER CRIME

Cyber Crimes can be categorized into two: computer crimes and computer related crimes. Computer crime is in a narrower sense meaning any illegal behaviour that is directed by means of electronic operations targeting the security of the computer systems and the data processed by them. And in a broader sense computer related crimes means any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing the information by means of a computer system or network[14]. But in specific there is no definition of a cyber crime. It is a general term which encompasses all the illegal activities that take place over the cyber space using the medium of computers or computer networks. The Indian Law does not provide with a specific definition for the cyber crimes. And the IPC also which has sections making such activities illegal does not also expressly state "Cyber crimes". The tool used is the computer system or the network to commit any illegal act which is punishable in the eyes of law like to collect some confidential information, financial crimes, to blackmail someone, etc. The reasons for cyber crimes are as follows-

i. Utility- One of the most important feature of the Computer is that it allows us to store a big amount of information or data in a small space which is very convenient also.

ii. Easy to access- though there are ways to protect the computer system or network from any unauthorized access but still the technology has been growing so tremendously that they have even found ways to overcome the hurdle of passwords, biometric systems and firewalls easily by implanting logic bombs, key bloggers which are easily able to steal the access codes and other passwords. Like said before that everything has its two sides so along with the development, the negative technology or the harmful technology has also developed.

---

[14] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE, September 2012, Telecommunication Development Sector

iii. Complexity- The computers and these networks are the creation of the human mind but no technology is perfect and it is natural that there are to be some loopholes of which the advantage is taken by these nasty minds to get into the computers and the networks.

iv. Negligence- Based on the human conduct which allows he criminals to gain the access[15].

Cyber crimes can be categorized further as following-

i. Against Individuals
ii. Against Organization
iii. Against Government

a. Against Individuals- It includes crimes like transmission of child pornography, financial crimes, blackmailing via email, etc. The trafficking, distribution, posting and dissemination of obscene material including pornography and indecent exposure is one of the most known and common form of Cyber crime. The most vulnerable age group to this type of cyber crime is the teenager. They are influenced with it and fall into such traps. Cyber harassment is very common over the cyber space by luring in the teenagers and it is very important to control them otherwise it will damage the growth of the teenagers. Harassment is just not limited to sexual it can be religious, racial, etc. It is also a cyber crime because you make an unwanted entry into someone's privacy and the victim is asked to do things which are not within their comfortable zone or are illegal.

b. Against Property- it basically involves destroying the computer system or the network of any other person. It may be through transmission of a programme which is harmful or may contain a virus or computer vandalism. There are various examples or instances of such computer infections few of them being "Melissa" and "love bug", which showed up on the web in March of 1999. It spread quickly through all computer systems and networks in the United States and Europe. It is

[15] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm, Cyber Crime by Parthasarati Pati

evaluated that the infection created 80 million dollars loss to the computers around the world. Organizations lose much cash in the business when the adversary organizations, take the specialized database from their computers with the assistance of a corporate cyberspy and also when they aim to destroy the computer system of other companies.

c. Against the Government- The cyberspace is being used just not against the individuals or the properties but against the Governments also to terrorize them and all because of the far reached development of the technology. The computers and their complex programmes are used by the Government to store and process their information. Hacking is one of the other common crimes committed in the cyber space. By hacking into a computer system or a specialized programme, the hacker is able to access the information which he is not authorized to access legally. The hacker may also tamper with the information which could prove to be more fatal to the Government and its plans and at large to the society[16].

The Computer Ethics Institute had laid down a framework within which computer users should work for ethical decisions. They are called as "The Ten Commandments" which are as follows-

1. Do not use a computer to harm another.
2. Do not interfere with other's computer's works or the information stored in it.
3. Do not spy over anyone else's files in their computer system or network.
4. Do not use a computer for any illegal purpose.
5. Do not use a computer to bear false witness.
6. Do not use or copy proprietary software to which you don't have a legal or authorized access or not have paid.
7. Do not use one's computer or computer system which is not allowed.
8. Do not take advantage of any other person's intellectual productivity.
9. Do not make a programme or software which may adversely affect the society.

[16] Cyber Crimes and effectiveness of Laws in India to Control Them, Mubashshir Sarshar, January 2009, NLUD

10. Use the computer in a way which does not hurt any other individual[17].

## *VARIOUS KINDS OF CYBER CRIME*

Cyber crimes are widespread and can be categorized as follows-

### *HACKING*

Hacking means unauthorized access to a computer system[18]. It is the most common type of Cyber crime being committed across the world. The word "hacking" has been defined in section 66 of the Information Technology Act, 2000 as follows, "whoever with the intent to cause or knowingly that he is likely to cause wrongful loss or damage to the public or any person , destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking"

Punishment for hacking under the above mentioned section is imprisonment for three years or fine which may extend up to two lakh rupees or both[19].

### *VIRUS, TROJANS AND WORMS*

Virus is a program that attaches itself to a computer program or a file and then automatically attaches to other files and keeps on transferring. They usually affect the data on the computer by deleting it or altering it or by affecting the whole file. And worms on the other hand, unlike viruses do not require a host but they keep attaching and attacking to the files. They make functional copies of themselves and do this repeatedly until unless they eat up all the available space on the computer system. A Trojan, the program is an unauthorized program which functions from inside with what looks like an authorized program and keeps functioning internally by altering or deleting or affecting the computer system[20].

[17] http://www.computerethicsinstitute.org/images/TheTenCommandmentsofComputerEthics.pdf

[18] Section 66 of the IT Act, 2000.

[19] Ibid.

[20] Cyber Crimes & Law, Dr. Amita Verma, Central Law Publications, pg 58

***CYBER PORNOGRAPHY***

It includes access to pornography websites on the computer networks, from where an individual can download pornographic films, clippings, videos, magazines, etc. These websites are used to publish and transmit such obscene material. One of the victims unfortunately to the cyber pornography has been children. There are images and videos of children available on the internet performing sexual activities. Such acts of producing, publishing and transmitting obscene material are illegal not only on the cyber space but otherwise also. But the cyberspace has become one of the sources to transmit such material more easily and fast.

***CYBER STALKING***

Cyber stalking can be defined as the repeated acts harassment or threatening behaviour of the cyber criminal towards the victim by using the internet services. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker. Cyber Stalking is a problem which many people especially young teenage girls complain about.

***CYBER TERRORISM***

Cyber terrorism may be defined to be "the premeditated use of distruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideologic al, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives".The role of computer with respect to terrorism is that a modern thief can steal more with a computer than with a gun and a future terrorist may be able to cause more damage with a keyboard than with a bomb. No doubt, the great fears are combined in terrorism, the fear of random, violent, victamisation segues well with the distrust and out of fear of computer technology. Technology is complex, abstract and indirect in its

impact on individual and it is easy to distrust that which one is not able to control. People believe that technology has the ability to become the master and humanity its servant[21].

### *CYBER CRIME RELATED TO FINANCE*

There are various types of Cyber Crimes which are directly related to financial or monetory gains by illegal means. To achieve this end, the persons on the cyber world who could be suitably called as fraudsters uses different techniques and schemes to befool other people on the internet. Online fraud and cheating is one the most lucrative businesses that are growing today in the cyberspace. It may assume different forms. Some of the cases of online fraud and cheating have come to light are pertaining to credit-card crimes, contractual crimes, online auction frauds, online investment schemes, job offerings, etc[22].

### *CYBER CRIMES INVOLVING MOBILE AND WIRELESS TECHNOLOGY*

At present the mobile technology has developed so much that is becomes somewhat equivalent to a personal computer. There is also increase in the services which were never available on mobile phones before, such as mobile banking, which is also prone to cyber crimes. Due to the development in the wireless technology the cyber crimes on the mobile device is coming at par with the cyber crimes on the net day by day.

### *PHISHING*

In computing, phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit cards, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to a „fish‟ for users‟ financial information and passwords. The act of sending an email to a user falsely claiming to be an established and legitimate enterprise in an attempt to scam the user into surrendering private information

[21] Love, David, CYBER TERRORISM : IS IT A SERIOUS THREAT TO COMM ERCIAL ORGANISATION?www.crime-research.org/news/2003/04/Mess0204.ht ml.

[22] US Depart ment of Justice, Criminal Division, Fraud Section, http://www.usdoj.gov/criminal/ fraud/internet.

that will be used for identity theft. The email directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security no. and bank account no. that the legitimate organization already has. The website however is bogus and is setup only to steal the user's information. By spamming large group large group of people, the "phisher" counted on the email being read by a percentage of people who actually had listed credit cards numbers with legitimacy. Phishing also refers o a brand spoofing or carding, is a variation on "fishing", the idea being that the bait is thrown out with the hope that while most will ignore the bait, some will be tempted into biting it. With the growing no. of reported phishing incidents, additional methods of protection are needed. Attempts include legislation, user training and technical measures. More recent phishing attempts have started to target the customers of banks and online payment services. While the first such example are sent indiscriminately in the hope of finding a customer of a given bank or service, recent research has shown that phishers may in principle be able to establish what bank a potential victim has a relation with, and then sends an appropriate spoofed email to the victim. In general such targeted versions of phishing have been termed as spear phishing[23].

***DENIAL OF SERVICE ATTACKS (DoS Attack)***

This is an act by a criminal who floods the bandwidth of the victim's network or fills his email box with spam mail depriving him of the service he is entitled to access or provide Short for denial-of-service attack, a type of service attack on a network which is designed to bring the network down to its knees by flooding it with useless traffic. Many DoS attack such as Ping of Death and Teardrop attack, exploit limitation in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by hackers. This involves flooding computer resources with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS)

[23] Cyber Crimes and Effectiveness of Laws in India to Control Them, Mubashshir Sarshar, January 2009

attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer, exceeding the limit that the victim's server can support and making the server's crash. Denial-of-service attacks have had an impressive history in the past and have brought down websites like the Amazon, CNN, Yahoo and eBay[24].

***EMAIL BOMBING***

As the name suggests, it means to send a large amount of mails to the victim's mail id which causes the victim's email account or the mail server of a company to crash[25]. It is a type of net abuse which causes over flooding in the email account of an individual or the mail server of a company. This usually done to disrupt the work and cause annoyance to the victim. Besides sending a large number of emails to the victims account, the other way of email bombing is list linking. Sending large number of emails is of a simple nature which can be differentiated very easily by the spam. Whereas list linking refers to subscribing to many websites to a particular email id. This causes annoyance as the victim has to manually unsubscribe all the websites otherwise the emails keep flowing in[26].

***EMAIL SPOOFING***

It is fraudulent email activity to confuse the victim as to the source or origin of the mail. The sender address and other headers in the mail are changed to give it a valid look. By changing certain properties of the email, such as the From, Return-Path and Reply- To fields, ill intentioned users can make the email appear to be from someone other than the actual sender. It is often associated with website spoofing which mimic an actual well-known website but are run by other party either with fraudulent intentions or as a means of criticism of the organisation's activities.

It is forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual code. Distributors of spam often use spoofing in an attempt to get recipient to open, and possibly respond to such solicitations.

[24] Ibid.

[25] Cyber Crimes & Law, Dr. Amita Verma, Central Law Publications, pg 57

[26] Ibid.

Spoofing can be used legitimately. Classic examples of senders who might prefer to disguise the source of the email include a sender reporting mistreatment by a spouse to a welfare agency or a "whistle blower" who fears retaliation. However, spoofing anyone other than you is illegal in many jurisdictions.

Email spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending email, does not allow a authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, however this precaution is not always taken.

If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed messages, senders insert commands in headers that alter the message information. It is possible to send a message that appears from anyone and anywhere, saying whatever the sender wants to say[27].

***DATA DIDDLING***

It involves changing the raw data that is to be processed by the computer and again changing it when the computer has finished processing the data. Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the data, or a virus that changes data, or the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved the process of creating, recording, encoding, examining, checking, converting or transmitting data. This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing, the cost can be considerable. To deal with this crime, a company must implement policies and

[27] Ibid.

internal controls. This may include performing regular audits, using softwares with built in features to combat such problems, and supervising employees[28].

***SALAMI ATTACKS***

A salami attack is a series of minor data-security attack that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can be considered a Salami Attack. Crimes involving salami attacks are typically difficult to detect and trace. These attack are used for commission of financial crimes. These key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program into the bank servers that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount each month.

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been mistreated by his employers, he introduced a program into the bank systems. This program was programmed to take ten cents from all accounts in the bank and put them into the account of the person whose name was alphabetically the last name in the bank's rosters. Then he went and opened an account in the name of "Ziegler". The amount being withdrawn from each of the accounts in the bank was so insignificant that neither the account holders nor the bank officials noticed the fault. It was brought to their notice when a person by the name of "Zygle" opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.

From a systems development standpoint, such scams reinforce the critical importance of sound quality assurance throughout the software development life cycle[29].

[28] Ibid.

[29] Ibid.

***LOGIC BOMBS***

A logic bomb is a programming code, inserted surreptitiously or intentionally and which is designed to execute under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. Softwares that are inherently malicious, such as viruses and worms, often contains logic bombs that execute a certain payload at the pre-defined time or when some other conditions are met. Many viruses attack their hosts systems on specific days, e.g. Friday the 13th and April fool's day logic bombs. A logic bomb when exploded may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.

Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compresses files, with an up to date anti- virus program. For best results, the auto-protect and email screening functions should be activated by the user whenever the machine is online. A logic bomb can also be programmed to wait for a certain message from the programmer. However in some ways a logic bomb is the most civilized programmed threat, because it targeted against a particular victim. The classic use of a logic bomb is to ensure the payment for software. If payment is not made by a certain date, the logic bomb gets activated and the software automatically deletes itself[30].

***INTERNET TIME THEFT***

Theft of Internet hours refers to using someone else's internet hours. Section 43 (h) of the IT Act, 2000 lays down civil liability for this offence. It reads as, whosoever without the permission of the owner or any other person who is in charge a computer system or computer network, charges the service availed of by a person to the account of another person by tampering with or manipulating any computer, computer systems or network is liable to pay damages not exceeding one crore to the person in office.

In the Colonel Bajwa's case46, the economic offences wing, IPR section crime branch of Delhi Police registered its first case involving theft of internet hours. In this case, the accussed, Mukesh Gupta, an engineer with Nicom System (p) Ltd was sent to the residence of the complainant to activate internet connection. However, the accused used

[30] Ibid.

Col. Bajwa's login name and password from various places causing wrongful loss of 100 hours to him,

Initially the Police could not believe that time could be stolen. They were not aware of the concept of time theft at all and his report was rejected. He decided to approach the Times of India, New Delhi which in turn carried a report on the inadequacy of the Delhi Police in handling Cyber crimes. The Commissioner of Police then took the case in his own hands and the Police then registered a case under Section 379, 411, 34 of the IPC and section 25 of the Indian Telegraph Act[31].

***WEB JACKING***

This term is derived from the term hi jacking. This occurs when someone forcefully takes control of a website by cracking the password and then changing it. The actual owner of the website does not have any control over what appears on that website. In a recent incident reported in USA, the owner of a hobby website for children received an email informing her that a group of hackers had gained control over her website. The owner did not take the threat seriously. Three days later she came know from phone calls from across the globe that the hackers had web jacked her website. Subsequently they had altered a portion of text in the website which said "How to have fun with a goldfish" to "how to have fun with pirhanas". Many children believed the content of the website and unfortunately were seriously injured as they tried playing with the pirhanas which they bought from pet shops[32].

[31] Ibid.

[32] Ibid.

# CHAPTER V

# CYBER TERRORISM

Cyber terrorism is the new form of terrorism, which exploits the system we have put in place. With the incidents of cyber terrorism it is tragically obvious that terrorism has reached new level of sophistication. Instead of using traditional method of killing, taking hostage and guerrilla warfare, terrorists now use the internet to cause much wider damage to a country. Computer is the new tool which they use for their activity although it is used indirectly. This convergence of the physical and virtual worlds, this lattice, is growing larger and more complex as we venture further into technological dependence. We are becoming even more inextricably reliant and dependent on convergence of these worlds.[33]

## *Tools used by cyber terrorists*

a. **Hacking**- is the process of unauthorised access of computer or network of computer. In simple words, Hacking is the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data (leaving a trace) without the intention of destroying data or maliciously harming the computer. It is done through network programming.
b. **Trojans**-it is harmful software that looks legitimate. Users are typically tricked into loading and executing it on their systems. After it is activated, it can achieve any number of attacks on the host, from irritating the user (popping up windows or changing desktops) to damaging the host (deleting files, stealing data, or activating and spreading other malware, such as viruses). Trojans are also known to create back doors to give malicious users' access to the system it is program which pretend to do one thing while actually they are meant to for doing something else.[34]
c. **Computer virus-** it is self- replicating program that can spread by email or by inserting copies of itself into program or documents. These are malicious program

[33] R.C. Mishra, "cyber crime: Impacts in the new millennium" pg. 47-48(2202)

[34] http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html, what is the difference: Viruses, worms, Trojans and blots. Accessed on 18-2-2014

designed to infect and gain control over the computer without the owner's knowledge.[35]

d. **Cryptology-** The art of protecting information by transforming it (encrypting) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called *code breaking*, although modern cryptography techniques are virtually unbreakable.[36]

e. **Computer worms-** are malicious software application which spread through computer network. A worm takes advantage of file or information transport features on your system, which is what allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line.[37]

f. **Email related crime-** email has become one of the most preferred forms of communication. Billions of email messages are exchanged globally daily. It is also misused by criminals. The ease, speed and relative anonymity of email has made it powerful tools for mails. Some of the major email related crime are- email spoofing, sending malicious code through email, email bombing, defamatory mails.[38]

## *Adequacy of information technology act, 2000*

The evolution of internet has raised numerous legal issue and question. As such scenario continues throughout the world are resorting to different approaches towards controlling, regulating and facilitating electronic communication. In the year 2000, parliament of india passed first law on information technology namely information technology act,

[35]what is computer virus and how to avoid them, https://runbox.com/email-school/what-are-computer-viruses-and-how-to-protect-against-them/. Accessed on 18-2-2014

[36]Cryptology, http://www.webopedia.com/TERM/C/cryptography.html, accessed on 18-2-2014

[37] what is worm, http://www.webopedia.com/DidYouKnow/Internet/virus.asp

[38] central law publication,Cyber crimes and law, Dr. Amita Verma, pg. 185

2000. The IT act is based on the model law of E-commerce adopted by UNCITRAL in 1996. The act was with the objective to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India.[39] It is also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

But the act did not address the problem of cyber attack. A terrorist attack on Delhi's Red fort in the year 2000, The Taj Mahal case in which Uttar Pradesh alleged received e-mail from the Lashker-e-Toiba which threatened to blow up the Taj Mahal, the Supreme Court case in the year 2002 in which the apex court received an e-mail threatening to blow up the court and chief minister and similar other event in which on investigation it was revealed that the terrorist used the internet to achieve their objective. Cyber war and cyber terrorism do not find mention in India cyber law. These are priority activates, which needs to be prevented and regulated. There was urgent requirement of specific code on cybercrime and cyber terror that needs to be supplemented in the nature to the IPC. Covering only some crime under chapter I of the IT act, 2000 does not solve the problem and instead only binds against the offenders. India needs to come up with concrete steps to fight cyber terrorism and prevent cybercrimes. So, Information Technology Act was amended in 2008 and a new section 66F was added. It provides life sentence through definition is not considered comprehensive. Section 66F states that- 1) Whosoever,—

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—

(*i*) denying or cause the denial of access to any person authorised to access computer resource; or

(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(*iii*) introducing or causing to introduce any computer contaminant,

[39] IT act of India, 2000, www.cyberlawsindia.net/Information-technology-act-of-india.html , accessed on 18th -2-2014

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

As per this section cyber terrorism is an act of hacking, blocking and /or computer contaminating in order to restrict legally authorized persons to access computer resources in general, and /or to gain or obtain unauthorized access to any information which is a 'restricted information 'for the purpose of security of the state, or foreign relation etc. however, this section does not cover the circumstances when internet is used to communication which is basis for carrying out terrorist activity. To strengthen this section 66A, section 69B and section 66 was added.

Most of the emphasis has been on unauthorised access to the information. But the use of cyber space for communicating has been completely ignored, which is basis for planning of the attack.

Moreover the activities that are carried out to disrupt the sovereignty and integrity are strictly regulated by the Prevention of Terrorism Act, 2002 besides various provision of IPC**.**

### *Recommendation*

- ✓ The language of Section 66F must be stretched to cover cyber communication that is carried out with intent to fulfil terrorist missions. Further, the provisions of section 69, which speaks about power to issue for interception or monitoring or decryption of any information through any computer resource, must be included in the ambit of section 66 E. This could form a new chapter dedicated for cyber terrorism and extremist speeches in the main legislation.
- ✓ A specific act should be made to deal which cyber terrorism because such amendment may be able to stop cyber but not the terrorism.
- ✓ Further, internet surveillance should be made mandatory.

## *International Organisation protecting Cyber Terrorism*

Today cyber terrorism is so prominent in the every corner of the world that there is a need to protect it. Thus United Nations came up with the International Multilateral Partnership Against Cyber Threats (IMPACT). It serves as the cyber security executing arm of the United Nation's (UN) specialised agency for ICT's – the International Telecommunication Union (ITU). With 149 countries IMPCT serves as a global platform that brings together the governments of the world, industry and academia. It is the largest cyber security alliance of its kind. Headquarters are in Cyberiya, Malaysia. IMPACT is the operational home of ITU's Global security Agenda (GCA.

GLOBAL Response Centre which is a backbone of IMPACT is fully equipped with a crisis room, IT and communications facilities, a fully functional Security Operations Centre (SOC), well-equipped data centre, on-site broadcasting centre and a VIP viewing gallery. The GRC is involved in securing the objectives of ITU's Global Cyber security Agenda (GCA) by placing the technical measures to combat newly evolved cyber threats. IMPACT provides the global community with network early warnings system (NEWS), expert locator, team management, remediation, automated threat analysis system, trend libraries, visualisation of global threats, country-specific threats, incident and case management, trend monitoring and analysis, knowledge base, reporting, and resolution finder among others.

IMPACT formally collaborated with International Telecommunication Union (ITU) for securing cyber terrorism. It is a specialised agency, following a Cooperation Agreement signed during the World Summit for Information Society 2011. Under the Cooperation Agreement**,** IMPACT is tasked by ITU with the responsibility of providing cyber security assistance and support to ITU's 193 Member States and also to other organisations within the UN system.

IMPACT involvement was since 2008 when it became ITU's Global Cyber Security Agenda (GCA). The GCA is an international cyber security framework that was formulated following deliberations by more than 100 leading experts worldwide. The GCA contains many recommendations, which when adopted and implemented, are intended to provide improved global cyber security. IMPACT's Global Response Centre (GRC) acts as a global cyber threat resource centre and provides emergency responses to facilitate identification of cyber threats. Thus many efforts are been made internationally to protect cyber terrorism

As a new and insufficiently investigated criminal phenomenon, the cyber terrorism deserves separate attention and demands special approach to the problem. Special concern in law enforcement bodies is caused with the terrorist acts connected to the internet use. Its open source allows receiving manufacturing technique biological, chemical and even the nuclear weapons of the terrorists. Cyber terrorists get access to the information of different sort including confidential. Thus, it is necessary to understand cyber terrorism as deliberate, motivated attack to the information processed by the computer, computer system and network which might create danger to people life or health or approach the consequences if such actions were perpetrated with the purpose of infringement of public safety, intimidations of population, provocation of the war conflict. It is possible to explain growing popularity of cyber terrorism because the act of cyber terrorism is much cheaper than normal crime. Acts of cyber terrorism in cyber space can be made separate persons or terrorist groups but also by one state against another. In this aspect cyber terrorism does nit differ from any other form of terrorism.

Today in every sphere of life there is a cyber threat as on our daily basis there is a use of internet, thus protecting the cyber threat is necessary. And therefore each and every country has its own acts, organisation which protects its nation from cyber terrorism.

Since the cyber terror is so much that the United Nation made organisation internationally which can protect the cyber threat globally.

## *INDIAN CASES*[40]

### 1. Pune Citibank Mphasis Call Centre Fraud

US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it is a serious matter and we cannot ignore it. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centres in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering.

The call centre employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that's how the criminals were traced. Police has been able to prove the honesty of the call centre and has frozen the accounts where the money was transferred.

There is need for a strict background check of the call centre executives. However, best of background checks can not eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where a name can be referred to. In this case preliminary investigations do not reveal that the criminals had any crime history. Customer education is very important so customers do not get taken for a ride. Most banks are guilt of not doing this.

[40] Cyber Law & Information Technology, Talwant Singh, Addl. Distt & Sessions Judge, Delhi

**2. Bazee.com case**

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai city police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

**3. State of Tamil Nadu Vs Suhas Katti**

The Case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of 7 months from the filing of the FIR. Considering that similar cases have been pending in other states for a much longer time, the efficient handling of the case which happened to be the first case of the Chennai Cyber Crime Cell going to trial deserves a special mention.

The case related to posting of obscene, defamatory and annoying message about a divorcee woman in the *yahoo message group*. E-Mails were also forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting.

Based on a complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within the next few days. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet.

On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore by citing 18 witnesses and 34 documents

and material objects. The same was taken on file in C.C.NO.4680/2004. On the prosecution side 12 witnesses were examined and entire documents were marked as Exhibits.

The Defence argued that the offending mails would have been given either by ex-husband of the complainant or the complainant herself to implicate the accused as accused alleged to have turned down the request of the complainant to marry her.

Further the Defence counsel argued that some of the documentary evidence was not sustainable under Section 65 B of the Indian Evidence Act. However, the court relied upon the expert witnesses and other evidence produced before it, including the witnesses of the Cyber Cafe owners and came to the conclusion that the crime was conclusively proved.

Ld. Additional Chief Metropolitan Magistrate, Egmore, delivered the judgement on5-11-04 as follows:

**" The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.**"

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered as the first case convicted under section 67 of Information Technology Act 2000 in India.

## 4. The Bank NSP Case

The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients.

She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

### 5. SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[41]

Taking up jurisdiction in this case, the Delhi Court observed that they had jurisdiction in a case of defamation of a corporate name and reputation. This was the country's first cyber defamation case.

The court in addition passed an ex-parte injunction.

The defendant was an employee of the plaintiff in his company and was accused of sending of sending defamatory, vulgar, filthy and abusive messages and emails to the employers of the company and also to the various subsidiaries placed globally. It was alleged that all this was done with mala fide intentions to defame and hurt the reputation of the Company's Managing Director Mr. R.K. Malhotra. To prevent him from sending further such emails and indulging in such unlawful acts, a suit of permanent injunction was filed by the Plaintiff.

The plaintiff contended that such act on part of the accused was defamatory and humiliating and embarrassing for the plaintiff and these emails was obscene and filthy in nature. It was also contended that the emails were sent with the malicious intentions and destroy the reputation and business of the plaintiff even internationally. This infringed the legal rights of the plaintiff.

The employment of the defendant was terminated instantly after the discovery of nexus between the emails and the sender.

The Delhi High Court passed an ex-parte interim injunction restraining the defendant from sending such emails anymore that were termed to be "derogatory, defamatory, obscene, vulgar, humiliating and abusive". The defendant was also barred from "publishing, transmitting or causing to be published" any such material in cyberspace as well.

[41] Suit No. 1279/2001 in Delhi HC

This distinct order by the High Court of Delhi has immense worth as it's the first case of cyber defamation and also when an ex-parte injunction was issued to restrain the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

## 6. PARLIAMENT ATTACK CASE

The laptop seized from the two terrorists who attacked the Parliament and were subsequently gunned down when Parliament was under siege on December 13 2001, was sent to Computer Forensics Division of BPRD (Bureau of Police Research and Development) at Hyderabad.

There were many evidences contained in the laptop confirming the terrorists' involvement and intentions with regard to the attack. It mainly had "the sticker of the Home Ministry that they had made on the laptop and pasted on their ambassador car" to have access to the Parliament using the fake identity cards with the Government emblem and seal which were scanned and pasted with the address of the State of Jammu & Kashmir.

Such forgery was considered criminal.

## 7. Andhra Pradesh Tax Case

Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person.

The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days.

The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and

contents of his computers it revealed that all of them were made after the raids were conducted.

It later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

## 8. SONY.SAMBANDH.COM CASE

India saw its first cybercrime conviction recently. It all began after a complaint was filed by Sony India Private Ltd, which runs a website calledwww.sony-sambandh.com, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless head phone.

She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim.

The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code.

The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the

company's site. The CBI recovered the colour television and the cordless head phone.

In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted.

The court, however, felt that as the accused was a young boy of 24 years and afirst-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

## 9. Nasscom vs. Ajay Sood & Others[42]

In a landmark judgment in the case of National Association of Software and Service Companies vs Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages.

Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. Court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details.

The Delhi HC stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian

[42] 119 (2005) DLT 596

law as “a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused.” The court held the act of phishing as passing off and tarnishing the plaintiff’s image.

The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India’s premier software association.

The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of head- hunting, the defendants composed and sent e-mails to third parties in the name of Nasscom. The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad- interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants’ premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case, it became clear that the defendants in whose names the offending e-mails were sent were fictitious identities created by an employee on defendants’ instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff’s trademark rights. The court also ordered the hard disks seized from the defendants’ premises to be handed over to the plaintiff who would be the owner of the hard disks.

This case achieves clear milestones: It brings the act of “phishing” into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no “damages culture” in India for violation of IP rights; This case reaffirms IP owners’ faith in the Indian judicial system’s ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

## 10. Infinity e-Search BPO Case

The Gurgaon BPO fraud has created an embarrassing situation for Infinity e-Search, the company in which Mr Karan Bahree was employed.

A British newspaper had reported that one of its undercover reporters had purchased personal information of 1,000 British customers from an Indian call-centre employee. However, the employee of Infinity eSearch, a New Delhi-based web designing company, who was reportedly involved in the case, has denied any wrongdoing. The company has also said that it had nothing to do with the incident.

In the instant case the journalist used an intermediary, offered a job, requested for a presentation on a CD and later claimed that the CD contained some confidential data. The fact that the CD contained such data is itself not substantiated by the journalist.

In this sort of a situation we can only say that the journalist has used "Bribery" to induce an "Out of normal behaviour" of an employee. This is not observation of a fact but creating a factual incident by intervention. Investigation is still on in this matter.

# CHAPTER VI

# CASE ANALYSIS OF SHREYA SINGHAL V UOI[43]

### Sec 66A held unconstitutional

Section 66A: A Grey Area of Information Technology Act, 2000. This section deals with 'Punishment for sending false and offensive messages through communication service, etc'. This section was inserted by the Amendment Act of 2008. However, there lies a question on the constitutionality of the said provision. Considering the potential and (recently) demonstrated abuse of Section 66A in contravention of freedom of speech, the project focuses on the grey areas and the misinterpretation of Section 66A. There is a dire need to review Section 66A holistically, keeping in mind the constitutional tenets and international conventions that we are a signatory to. The project is based on a contention that this section violative of freedom of speech and expression guaranteed by Article 19 (1) (a) of the Constitution[44].

The project shall extensively deal with the violation of Constitutional Freedom of Speech and Expression by this section. There are Constitutional Curbs to freedom and there are Unconstitutional curbs too. Section 66A covers the domain of unconstitutionality in this regard.

Unconstitutional Curbs as elucidated in the project: If the police consider a tweet or blog 'grossly offensive' or 'of menacing character', or causing 'inconvenience, annoyance, danger, obstruction or insult', they can prosecute any citizen responsible under Section 66A of the IT Act, which carries a maximum imprisonment of three years. This is certainly a breach of the fundamental right to speech. The grounds provided are not in relation to those listed in Article 19(2). The question is that, how a statement when made outside the IT world is justified by virtue of Article 19 however, when the same is made on the Internet it is punishable. 'If an expression is not criminal when it is made in the brick-and-mortar world, it cannot become one in cyberspace'. The basic idea behind freedom of speech is to allow divergent critical views without looking into whether people are annoyed or inconvenienced.

[43] W.P. (Crl) No. 167 of 2012, (2013) 12 SCC 73

[44] http://indiankanoon.org/doc/110813550/

Section 66A is absolutely draconian as it gives rulers a weapon to misuse and deprive citizens of their personal liberty. Thus it not only violates Article 19(1)(a) but also Article 21, the right to life and liberty. Its chilling effect is already visible - the arrest of a professor in Kolkata, a businessman in Tamil Nadu and two young women in Mumbai for casual cyber writings and many more.

There are many terms used in the section which are new and not defined them become ambiguous and subject to personal interpretation of the police officers. At one level, the problem is that the wording of the Section makes it so vague as to be applicable to virtually anything anyone might find "grossly" offensive or causing "annoyance or inconvenience". This is also potential tool in the hands of rulers to curtail the voice of opposition. An analysis of the guidelines issued by the Apex Court to curb the misuse of the alleged section along with the PIL filed in the Supreme Court for declaring this section as unconstitutional will be done.

Section 66A should not be considered as a 'reasonable restriction' within the meaning of Article 19 of the Constitution and must be struck down as an unconstitutional restriction on freedom of speech. If political speech, that is, criticism of politicians and exposure of corruption continues to be punished by arrest instead of being protected, India's precious democracy and free society will be no more. The project ends with an open ended question on the Democratic Principles of the country if this section continues to be used in the manner as it is put to use now. The Section is too wide and vague and incapable of being judged on objective standards that it is definitely susceptible to abuse.

In a writ petition filed in 2012, the law student Shreya Singhal challenged the constitutionality of Section 66A on grounds, inter alia, of vagueness and its chilling effect. More petitions were filed challenging other provisions of the IT Act including Section 69A (website blocking) and Section 79 (intermediary liability), and these were heard jointly by Justices Rohinton F. Nariman and G. Chelameshwar. Section 66A, implicating grave issues of freedom of speech on the internet, was at the centre of the challenge.

The Supreme Court struck down Section 66A of the Information & Technology Act today after hearing a clutch of petitions challenging it.

The case has been closely followed, mostly for its implications on how Indians can use the Internet and social media, and because of its implications on the freedom of speech.

WHAT DOES THE SECTION 66A OF THE IT ACT ACTUALLY SAY?

"Any person who sends, by means of a computer resource or a communication device,—
(a) any information that is grossly offensive or has menacing character; or
(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,
(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,
shall be punishable with imprisonment for a term which may extend to three years and with fine."

THE ISSUES WITH THE WORDING OF THE ACT[45]

One of the main problems with the act is the fact that it is framed in vague and sweeping language, which allows law enforcement authorities to interpret it in a subjective manner. What, for instance is information that is 'grossly offensive' and has menacing character'? If someone were pro-life, for instance, they may find an email forward endorsing abortion 'grossly offensive'. Similarly, if someone were a religious purist who believed God created the world in seven days, they may find a status update on evolution to be 'false information'. By making the act so open ended and subjective, the government is trying to save itself the trouble of having to define each and every cyber crime, but what they have overlooked or ignored is that in its present form, the act also easily lends itself to prosecuting people who dare to have and express a controversial or different opinion that may not necessarily be dangerous.

This issue was also brought up by the Supreme Court while it was hearing the petitions against the act.

[45] http://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/

Dealing with the word "grossly offensive", the bench referred to the judgment cited by the ASG and said, "what is grossly offensive to you, may not be grossly offensive to me and it is a vague term." "Highly trained judicial minds (judges of the UK courts) came to different conclusions by using the same test applied to judge as to what is grossly offensive and what is offensive," the court added.

In fact one of the judges on the case, Justice Nariman, even gave an example to the court of how the vague definition of 'grossly offensive' could be dangerously twisted. According to a Times of India report, he said in court, ""I can give you millions of examples but take one burning issue is of conversion. If I post something in support of conversion and some people, not agreeable to my view, filed a complaint against me then what will happen to me?"

THE PETITION AGAINST THE SECTION

Some of the petitions seek setting aside of section 66A of the Information Technology Act which empowers police to arrest a person for allegedly posting offensive materials on social networking sites.

The first PIL on the issue was filed in 2012 by law student Shreya Singhal, who sought amendment in Section 66A of the Act, after two girls -- Shaheen Dhada and Rinu Shrinivasan -- were arrested in Palghar in Thane district as one of them posted a comment against the shutdown in Mumbai following Shiv Sena leader Bal Thackeray's death and the other 'liked' it.

Most activists and policy experts pointed out that the Section 66A is loosely worded and puts too many powers in the hands of the police.

WHAT THE COURT HAS SAID SO FAR?

Apart from raising objections to who could determine what constituted 'grossly offensive content', the court has also not been impressed with the government argument that the section was needed to protect government data from hackers, and had pointed out that this eventuality was already dealt with viruses and hacking for which Section 65 of the IT Act was relevant.

The apex court had also on 16 May, 2013, come out with an advisory that a person, accused of posting objectionable comments on social networking sites, cannot be arrested without police getting permission from senior officers like IG or DCP.

The direction had come in the wake of numerous complaints of harassment and arrests, sparking public outrage.

It had, however, refused to pass an interim order for a blanket ban on the arrest of such persons across the country.

WHAT SPEECH IS PROTECTED?

There are three types of speech, the court says: Discussion, advocacy and incitement. Discussion and advocacy are at the heart of Article 19(1)(a), and are unquestionably protected. But when speech amounts to incitement - that is, if it is expected to cause harm, danger or public disorder- it can be reasonably restricted for any of these reasons: public order, sovereignty and integrity of India, security of the State and friendly relations with foreign states.

Section 66A, however, does not meet the legal standards for any of the limitation-clauses under Article 19(2), and so is unconstitutional. The Union of India argued that Section 66A is saved by the clauses "public order", "defamation", "incitement to an offence" and "decency, morality". But as the court finds that these are spurious grounds. For instance, Section 66A covers "all information" sent via the Internet, but does not make any reference (express or implied) to public order. Section 66A is not saved by incitement, either. The ingredients of "incitement" are that there must be a "clear tendency to disrupt public order", or an express or implied call to violence or disorder, and Section 66A is remarkably silent on these. By its vague and wide scope, Section 66A may apply to one-on-one online communication or to public posts, and so its applicability is uncertain. For these grounds, Section 66A has been struck down.

For freedom of speech on the internet, this is fantastic news! The unpredictability and threat of Section 66A has been lifted. Political commentary, criticism and dialogue are clearly protected under Article 19(1)(a). Of course, the government is still keen to

regulate online speech, but the bounds within which it may do so have been reasserted and fortified[46].

## INDIAN CASE STUDIES: SECTION 66A: SENDING OFFENSIVE OR FALSE MESSAGES

### SAJEESH KRISHNAN V. STATE OF KERALA (KERALA HIGH COURT, DECIDED ON JUNE 5, 2012)

Petition before High Court for release of passport seized by investigating agency during arrest. In the case of Sajeesh Krishnan v. State of Kerala (Decided on June 5, 2012), a petition was filed before the Kerala High Court for release of passport seized at the time of arrest from the custody of the investigating agency. The Court accordingly passed an order for release of the passport of the petitioner. The Court, while deciding the case, briefly mentioned the facts of the case which were relevant to the petition. It stated that the "gist of the accusation is that the accused pursuant to a criminal conspiracy hatched by them made attempts to extort money by black mailing a Minister of the State and for that purpose they have forged some CD as if it contained statements purported to have been made by the Minister." The Court also noted the provisions under which the accused was charged. They are Sections 66-A(b) and 66D of the Information Technology Act, 2000 along with a host of sections under the Indian Penal Code, 1860 (120B – Criminal Conspiracy, 419 – Cheating by personation, 511- Punishment for attempting to commit offences punishable with imprisonment for life or other imprisonment, 420 – Cheating and dishonestly inducing delivery of property, 468 – Forgery for purpose of cheating, 469 – Forgery for purpose of harming and 201 – Causing disappearance of evidence of offence, or giving false information to screen offender read with 34 of Indian Penal Code, 1860)

### NIKHIL CHACKO SAM V. STATE OF KERALA (KERALA HIGH COURT, DECIDED ON JULY 9, 2012) 29

[46] http://lawyerslaw.org/shreya-singhal-vs-union-of-india-on-24th-march-2015-supreme-court-of-india-case-brief/

Order of the Kerala High Court on issuing of the summons to the petitioner In another case, the Kerala High Court while passing an order with respect to summons issued to the accused, also mentioned the charge sheet laid by the police against the accused in its order. The accused was charged under Section 66-A, ITA. The brief facts which can be extracted from the order of the Court read: "that the complainant and the accused (petitioner) were together at Chennai. It is stated that on 04.09.2009, the petitioner has transmitted photos of the de facto complainant and another person depicting them in bad light through internet and thus the petitioner has committed the offence as mentioned above."

**J.R. GANGWANI AND ANOTHER V. STATE OF HARYANA AND OTHERS (PUNJAB AND HARYANA HIGH COURT, DECIDED ON OCTOBER 15, 2012)**

Petition for quashing of criminal proceedings under section 482 of the Criminal Procedure Code, 1973 In the Punjab and Haryana High Court, an application for quashing of criminal proceeding draws attention to a complaint which was filed under Section 66-A(c). This complaint was filed under Section 66-A(c) on the ground of sending e-mails under assumed e-mail addresses to customers of the Company which contained material which maligned the name of the Company which was to be sold as per the orders of the Company Law Board. The Complainant in the case received the e-mails which were redirected from the customers. According to the accused and the petitioner in the current hearing, the e-mail was not directed to the complainant or the company as is required under Section 66-A (c). The High Court held that, "the petitioners are sending these messages to the purchasers of cranes from the company and those purchasers cannot be considered to be the possible buyers of the company. Sending of such e-mails, therefore, is not promoting the sale of the company which is the purpose of the advertisement given in the Economic Times. Such advertisements are, therefore, for the purpose of causing annoyance or inconvenience to the company or to deceive or mislead the addressee about the origin of such messages. These facts, therefore, clearly bring the acts of the petitioners within the purview of section 66A(c) of the Act." 30

**MOHAMMAD AMJAD V. SHARAD SAGAR SINGH AND ORS. (CRIMINAL REVISION NO. 72/2011 FILED BEFORE THE COURT OF SH. VINAY KUMAR KHANA ADDITIONAL SESSIONS JUDGE – 04 SOUTH EAST: SAKET COURTS DELHI)**

Revision petition against the order of the metropolitan magistrate In a revision petition came up before the Additional Sessions Judge on the grounds that the metropolitan magistrate has dismissed a criminal complaint under Section 156(3) of the Criminal Procedure Code without discussing the ingredients of section 295-A, IPC and 66- A, IT Act. In this case, the judge observed that, "...Section 66A of Information Technology Act (IT Act) does not refer at all to any 'group' or 'class' of people. The only requirement of Section 66A IT Act is that the message which is communicated is grossly offensive in nature or has menacing character." He also observed that the previous order "not at all considered the allegations from this angle and the applicability of Section 66A Information Technology Act, 2000 to the factual matrix of the instant case."[47]

[47] http://www.thehindu.com/todays-paper/tp-national/tp-newdelhi/no-arrest-under-it-act-without-approval-from-dcp-police/article4919520.ece

# CHAPTER VII

# VOICE OVER INTERNET PROTOCOL (VOIP)

Since, its invention Internet has become a part of everyone's life. It has been used widely from individual to big corporate houses and it is still growing. It is Omnipresent. From past few years a new use of Internet has emerged which have made it a essential part of human life, it is communication over the Internet. It is like any other communication like on cell phone or like face to face communication. This information and communication technology (ICT) has connected the people from all over the World. The influence of ICT on society has been far more than establishing basis information infrastructure. The availability of ICT and new network based service offers many advantages. It has much wider application such as e-commerce, e-health, e-environment etc.

The introduction of this information and communication technology in everyday life has led to the development of the information society. This modern informative society offers great opportunity. As it offer unhindered access to information which can help in democratic process of the country. This technical advancement has improved daily life in many aspect like- online banking, shopping, use of mobile data service, Voice over Internet protocol etc.

However, growth of this information and communication technology has introduced new and serious threat. Attack on ICT has potential to harm society in critical way. In the past few years a new category of cyber crime has developed. Earlier it was dominated by sophisticated method of committing crime such as phishing, bottle attacks etc. but with the increase in the use of technology it has become difficult for law enforcement agencies to investigate and handle the matter, such as Voice over Internet Protocol. These are 21$^{st}$ century crimes.

## *What is VOICE over Internet Protocol?*

It is category of hardware and software which enable the people to use Internet to transmission medium for telephonic call. In other words, Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only

allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers.[48]

In simple words, it can be defined as the use of internet to communicate with the other person. Such a communication has been possible by the application like Skype, Viber, Facebook calling, email etc. through, these application it is possible to communicate using the internet. VoIP has many utility and is been used by in the call centre, corporate houses for meeting etc. Under the ambit of India's National Telecom Policy (NTP), 2012, the Telecom Commission has approved allowing voice over Internet protocol (VoIP) services. This move is aimed at making telecom services more affordable.[49]

But the same has become a challenge for the law enforcement agency. The VoIP has become a challenge for law enforcement agency as it has been used by the terrorist, leading to another form of cyber crime or cyber terrorism.

The terrorist has used the e-mail service in 2010 Delhi attack which was confirmed by the police. Moreover, LeT has been using VoIP for communication. Moreover, the same was used during the Mumbai attack by the Let, to carry out the operation effectively. [50] The threat of misuse of VoIP is very high in India. India has been on the target of Cyber terrorist and VoIP has been used to challenge the sovereignty of India. After Mumbai attack Intelligence bureau issued circular to block the VoIP.

Moreover, there is no specific act or provision dealing with the VoIP which further create a hurdle for government in regulating the VoIP. Though Information technology act provide for monitor and collect information through any computer resource. But interception of such information is not easy; moreover in India there is no specific tool which can be used to intercept the VoIP calls.

Though, VoIP has many uses but there is need to have a regulatory body or a specific policy dealing with the VoIP. Because the policy used for regulating telephonic communication can't be used for the VoIP as it involve internet which has much wider

[48] http://www.fcc.gov/encyclopedia/voice-over-internet-protocol-voip, last accessed on 13-4-2015.

[49] http://egov.eletsonline.com/2012/03/voip-will-be-allowed-under-national-telecom-policy/ last accessed on 13-4-2015.

[50] Responsibility of National Security and the Indain Government,

reach, moreover telecommunication services are regulated by the telegraph act, 1885[51] which is itself obsolete and outdated that the matter relating to VoIP can't be dealt under this act.

[51] http://www.tatacommunications.com/legal/india-telecom-regulations, India Telecom Regulation, last accessed on 15-4-2015

# *CHAPTER VIII*

## *Conclusion*

The ICT Trends of India 2009 have proved that India has failed to enact a strong and stringent Cyber Law in India. On the contrary, the Information Technology Act 2008 (IT Act 2008) has made India a safe haven for cyber criminals, say cyber law experts of India. The problem seems to be multi- faceted in nature. Firstly, the cyber law of India contained in the IT Act, 2000 is highly deficient in many aspects. Thus, there is an absence of proper legal enablement of ICT systems in India. Secondly, there is a lack of cyber law training to the police, lawyers, judges, etc in India. Thirdly, the cyber security and cyber forensics capabilities are missing in India. Fourthly, the ICT strategies and policies of India are deficient and needs an urgent overhaul. Fifthly, the Government of India is indifferent towards the ICT reforms in India. This results in a declining ranking of India in the spheres of e-readiness, e-governance, etc. While International communities like European Union, ITU, NATO, Department of Homeland Security, etc are stressing for an enhanced cyber security and tougher cyber laws, India seems to be treading on the wrong side of weaker regulatory and legal regime.

Police in India are trying to become cyber crime savvy and hiring people who are trained in the area. The pace of the investigation however can be faster, judicial sensitivity and knowledge needs to improve. Focus needs to be on educating the Police and district judiciary. IT Institutions can also play an integral role in this area. We need to sensitize our prosecutors and judges to the nuances of the system. Since the law enforcement agencies find it easier to handle the cases under IPC, IT Act cases are not getting reported and when reported are not dealt with under the IT Act. Lengthy and intensive process of learning is required. A whole series of initiatives of cyber forensics were undertaken and cyber law procedures resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems are invented. We need to move faster than the criminals. The real issue is how to prevent cyber crime. For this there is a need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility, authenticity, accuracy and completeness to convince the judiciary. The challenges in cyber crime cases include getting evidence that will stand scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same

that has been analysed and reported in the court based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it.

Criminal Justice systems all over the world, must also remember that because of certain inherent difficulties in the identification of the real cyber criminal, cybe r law must be applied so as to distinguish between the innocent and the deviant. A restraint must be exercised on the general tendency to apply the principle of deterrence as a response to rising cyber crime, without being sensitive to the rights of the accused. Our law makers and the criminal law system must not forget the basic difference between an accused and a convict. There is only a delicate difference between the need to ensure that no innocent is punished and the need to punish the cyber criminal.

Thus lastly, there were two research questions which were proposed by the researcher for the purpose of the project. The first one being, is the Information Technology Act, 2000 effective and efficient enough for controlling the recent developments in Cyber Crimes in India? The Hypothesis for the question was "No" and it has been proved.

There is need to pass a special legislation or a policy which will help in interception of the VoIP and will impose a strict penalty. Moreover, the government need to utilise the enhanced power provided under section 69A, 69B, 70A, and 70B of the Information technology act, 2000. Further, the government can mandate the intermediaries or network service providers or any person in charge of a computer resource to provide technical assistance and extend all facilities to governmental agencies to give online access or to secure and provide online access to computer resources generating, transmitting, receiving or storing traffic data or information. It will be prudent for the government to invoke the powers under the new amended Information Technology Act in order to secure its telecom lines.[52]

[52] http://news.rediff.com/interview/2009/sep/20/inter-our-cyber-cells-cant-deal-with-cyber-crimes.htm, last accessed on 13-4-2015

# *CHAPTER IX*

## *BIBLIOGRAPHY*


1. R.C. Mishra, "cyber crime: Impacts in the new millennium" pg. 47-48(2202)
2. http://www.indiancybersecurity.com/cyber_law/2_need_of_cyber_law.html
3. http://www.insightsonindia.com/2014/12/14/effects-liberalization-indian-economy-society/
4. Cyber Crime Law in India: Has law kept pace with the emerging trends? An Empirical Study by N.S. Nappinai, Journal of International Commercial law and Technology, Vol. 5, Issue 1 (2010)
5. http://www.indiancybersecurity.com/cyber_law/8_history_of_cyber_law_in_india.html
6. National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, Incidence of cases registered under Cyber Crimes
7. National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, Persons arrested under IT Act by Age- group
8. National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, Persons arrested under IPC sections of Cyber Crimes by Age- group
9. National Crime Records Bureau, Ministry of Home Affairs, http://ncrb.gov.in/, incidence of Cases registered and number of Persons Arrested under Cyber crimes (IPC+ IT) During 2013
10. Cyber Crimes and effectiveness of Laws in India to Control Them, Mubashshir Sarshar, January 2009, NLUD
11. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211
12. http://deity.gov.in/content/cyber-security-strategy
13. http://www.itu.int/wsis/docs/geneva/official/poa.html
14. http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE, September 2012, Telecommunication Development Sector
15. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm, Cyber Crime by Parthasarati Pati
16. Cyber Crimes and effectiveness of Laws in India to Control Them, Mubashshir Sarshar, January 2009, NLUD

17. http://www.computerethicsinstitute.org/images/TheTenCommandmentsofComputerEthics.pdf
18. Cyber Crimes & Law, Dr. Amita Verma, Central Law Publications, pg 58
19. Love, David, CYBER TERRORISM: IS IT A SERIOUS THREAT TO COMMERCIAL ORGANISATION? www.crime research.org/news/2003/04/Mess0204.ht ml.
20. US Department of Justice, Criminal Division, Fraud Section, http://www.usdoj.gov/criminal/ fraud/internet.
21. Cyber Crimes and Effectiveness of Laws in India to Control Them, Mubashshir Sarshar, January 2009

22. R.C. Mishra, "cyber crime: Impacts in the new millennium" pg. 47-48(2202)
23. http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html, what is the difference: Viruses, worms, Trojans and blots. Accessed on 18-2-2014 what is computer virus and how to avoid them, https://runbox.com/email-school/what-are-computer-viruses-and-how-to-protect-against-them/. Accessed on 18-2-2014.Cryptology,http://www.webopedia.com/TERM/C/cryptography.html, accessed on 18-2-2014. What is worm, http://www.webopedia.com/DidYouKnow/Internet/virus.asp
24. IT act of India, 2000, www.cyberlawsindia.net/Information-technology-act-of-india.html , accessed on 18th -2-2014
25. Cyber Law & Information Technology, Talwant Singh, Addl. Distt & Sessions Judge, Delhi
26. http://indiankanoon.org/doc/110813550/
27. http://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/
28. http://lawyerslaw.org/shreya-singhal-vs-union-of-india-on-24th-march-2015-supreme-court-of-india-case-brief/
29. http://www.thehindu.com/todays-paper/tp-national/tp-newdelhi/no-arrest-under-it-act-without-approval-from-dcp-police/article4919520.ece
30. http://www.fcc.gov/encyclopedia/voice-over-internet-protocol-voip, last accessed on 13-4-2015.
31. http://egov.eletsonline.com/2012/03/voip-will-be-allowed-under-national-telecom-policy/ last accessed on 13-4-2015.

32. Responsibility of National Security and the Indain Government, http://www.tatacommunications.com/legal/india-telecom-regulations, India Telecom Regulation, last accessed on 15-4-2015.http://news.rediff.com/interview/2009/sep/20/inter-our-cyber-cells-cant-deal-with-cyber-crimes.htm, last accessed on 13-4-2015