
UNIT 7 CONVENTIONAL CRIMES THROUGH COMPUTER

Structure

- 7.1 Introduction
- 7.2 Objectives
- 7.3 Cyber Defamation
 - 7.3.1 Quantitative Impact of Cyber Defamation
 - 7.3.2 Qualitative Impact of Cyber Defamation
 - 7.3.3 Corporate Cyber Smear
 - 7.3.4 Indian law
- 7.4 Digital Forgery
 - 7.4.1 Indian Law
 - 7.4.2 Convention on Cyber Crime – Council of Europe
- 7.5 Cyber Pornography
 - 7.5.1 Increase in Cyber Pornography
 - 7.5.2 Child Pornography
 - 7.5.3 Indian Law
 - 7.5.4 Cyber Crime Convention
- 7.6 Cyber Stalking/Harassment
 - 7.6.1 Preferred Mode of Harassment
 - 7.6.2 Indian Law
- 7.7 Online Gambling
 - 7.7.1 Indian Law
- 7.8 Online Sale of Illegal Articles
 - 7.8.1 Indian Law
- 7.9 Summary
- 7.10 Terminal Questions
- 7.11 Answers and Hints
- 7.12 References and Suggested Readings

7.1 INTRODUCTION

In the previous unit we have tried to give the general introduction of the computer wrongs. In this unit we shall discuss the offences which are known as the technologically neutral offences. These offences do not depend on computer for their commission although their quantitative and qualitative impact changes when committed on the cyberspace.

Many of the wrongful acts enlisted as an offence under the Indian Penal Code, 1860 are capable of being committed with the use or aid of or through computers and technology. The technology acts only as a new medium to commit such

crimes. With the ease of use and anonymity available on the Internet, many of the crimes like defamation, forgery, pornography, etc. are being committed online.

While studying this unit you should keep the copy of the IPC for the quick references of the definitions of the offences discussed in this unit.

7.2 OBJECTIVES

After studying this unit, you should be able to:

- discuss the offences defined under Indian Penal Code which are capable of being committed on the internet;
- examine the new dimensions that have been added to these offences by the use of information and communication technology (ICT); and
- analyse whether the provisions of Indian Penal Code dealing with these offences are capable enough to address the challenges posed by the information and communication technology with regard to these offences.

7.3 CYBER DEFAMATION

Every individual has a private right to protect his reputation. Every individual has a right to its own personal space and he would not want others to interfere in that 'space'. However, a public right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India makes enforcement of our private right a challenge. A delicate balance has to be maintained. The law of defamation has been designed to protect the reputation of an injured person and provide such balance between private and public rights by giving him the right to sue for damages. Defamation comprises of both libel (defamation by means of writing) and slander (defamation by speaking).

In the good old days, slander was more popular and possible. After the popularity of the printing press, one witnessed the increase in libel. With the advent of information technology and the Internet, libel has become much more common and of course, easier. In this context, arises cyber defamation. In simple words, it implies defamation by anything which can be read, seen or heard with the help of computers/technology. Since the Internet has been described as having some or all of the characteristics of a newspaper, a television station, a magazine, a telephone system, an electronic library and a publishing house, there are certain noticeable differences between online and offline attempt of defamation which makes the online defamation more vigorous and effective.

In *SMC Pneumatics Ltd. v Jogesh Kwatra*,¹ defamatory e-mails were allegedly sent to the top management of SMC Numatics by the defendant, who has since been restrained by the Delhi High Court from sending any form of communication to the plaintiff. The High Court granted an ex-parte injunction restraining the defendant from defaming the plaintiffs by sending derogatory, defamatory, abusive and obscene e-mails either to the plaintiffs or their subsidiaries. [*Avinash Bajaj v State (NCT) of Delhi*. Bail Appl. no. 2284 of 2004 decided on 21 Dec. 2004 [116 (2005) DLT 427].

7.3.1 Quantitative Impact of Cyber Defamation

Quantitatively, a comment defaming a person can be sent to a large number of persons through e-mail by a click of the mouse. Much easier would be to publish it on a discussion board known to be visited by thousands of persons every day. On the number game, it is still more convenient to make available the defamatory sentence to millions of people by merely publishing it on the website. The number of people a comment defaming a person might reach is gigantic and hence would effect the reputation of the defamed person much more than would an ordinary publication. Of course, there is a rider to it. In as much as there is a possibility of a large number of people reading the defamatory sentence on a website, unless such website is known, it might not even reach a single person at all. Thus, a defamatory sentence published on a newspaper website would have a bigger impact than being published on a website hardly known to the world at large.

7.3.2 Qualitative Impact of Cyber Defamation

Qualitatively, the impact of an online comment defaming a person would again depend upon the fact as to where it has been published. Putting a defaming message in specific a newsgroups (for example, a lawyer's group in case one wants to defame a lawyer) would necessarily have a more effective negative impact on the reputation of the person being defamed rather putting the same on a ladies' kitty party group.

7.3.3 Corporate Cyber Smear

Harmful and defamatory online message has been termed as *Corporate cyber smear*. It is a false and disparaging rumour about a company, its management or its stock that is posted on the Internet. This kind of criminal activity has been a concern especially in stock market and financial sectors where knowledge and information are the key factors for businessmen. Persons indulging in corporate cyber smear include disgruntled employees or insiders, ex-employees, envious ex-colleagues, impostors, competitors, creditors, and even those seeking a forum when they are denied employment or former shareholders.

False and defamatory statements made against Amazon Natural Treasures, Inc. led to a stock price decline from an April 1997, 52-week high of \$3.56 per share to approximately 12 cents per share. The low stock price led to a delisting from the OTCBB to the pink sheets. It transpired that the statements were made by the owner of Demonte & Associates, a New York public relations firm, who claimed that a collection agency was suing Amazon for about \$7,000.

7.3.4 Indian Law

Cyber defamation is covered under section 499 of Indian Penal Code (IPC) read with section 4 of the IT Act. Section 499 of the IPC *inter alia* reads as under:

Cyber Crimes and Torts

499. Defamation. Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

Explanation 1 — It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

Explanation 2 — It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

Explanation 3 — An imputation in the form of an alternative or expressed ironically, may amount to defamation.

Explanation 4 — No imputation is said to harm a person's reputation, unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state, or in a state generally considered as disgraceful.

A bare perusal of the section above makes it clear that no specific mention has been made with regard to any electronic publication. Section 4 of the IT Act, however, gives legal recognition to electronic records. It reads as under:

4) **Legal recognition of electronic records.**

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—

- a) rendered or made available in an electronic form; and
- b) accessible so as to be usable for a subsequent reference.

Keeping in mind the legal fiction being created by section 4 of the IT Act, if any defamatory information is posted on the Internet either through e-mails or chat rooms or chat boards, such posting would be covered under the section 499 requirement of 'publication' and would amount to cyber defamation. That is the legal position of cyber defamation in India.

Please answer the following Self Assessment Question.

Self Assessment Question 1

Spend 3 Min.

What is defamation? Discuss its quantitative and qualitative impact when it is committed on the cyberspace.

.....
.....

- 2) Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters an electronic record in any material part thereof, after it has been made, executed or affixed with digital signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or
- 3) Who dishonestly or fraudulently causes any person to sign, execute or alter an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the electronic record or the nature of the alteration.

Explanation 3 to section 464 has also been inserted which, for the purpose of this section, provides for the expression 'affixing digital signature' to have the same meaning as assigned to it in section 2(1)(d)³ of the IT Act.

Section 463 of the IPC, after amendment, defines forgery, in relation to electronic records, as making of any false electronic record or part thereof with intent to cause damage or injury to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed. Section 466 (forgery of record of Court or of Public register, etc.), section 468 (forgery for purpose of cheating), section 469 (forger for purpose of harming reputation), section 470 (forged document or electronic record), section 471 (using as genuine a forged document), section 474 (having possession of document described in section 466 or 467, knowing it to be forged and intending to use it as genuine) and section 476 (counterfeiting device or mark used for authenticating documents other than those described in section 467, or possessing counterfeit marked material) have also been suitably amended to include 'electronic records'. It may, however, be noticed that section 467 which pertains to forgery of valuable security, will, etc., has not been amended for the reason that section 1(4) bars the applicability of IT Act to certain documents including will, trust, power-of-attorney, contract for sale or conveyance of immovable property, etc. Therefore, digital forgery and offences related to it are now covered under the IPC pursuant to the amendments made by the IT Act.

7.4.2 Convention on Cyber Crime – Council of Europe

The Convention on Cyber crime, Article 7 requires the member-States to make laws to establish as criminal offences, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Cyber Crimes and Torts

materials. The consumer of such publications is more comfortable in opening a website and viewing/watching. With availability of broadband connections and high downloading speeds, the demand, though privately, seems to have risen.

On the other hand, anonymity has encouraged the offender to come out with more explicit and real material with higher degrees of inducement. Anybody can upload information onto a website from anywhere with the entire world as its market/consumer. It is extremely difficult to pinpoint persons responsible for such activities. It is also important to note that in countries where certain degree of pornographic material is permitted to be published and distributed, offenders quite often publish their information online from such countries though knowing well that the online market extends well beyond the geographical boundaries.

7.5.2 Child Pornography

What has, however, been most disturbing is the increase in child pornography. Child pornography is different from other pornography, and consequently receives more stringent legal treatment. It is distinguished as an issue of child abuse — in its production and/or in the way it is used by pedophiles to desensitise their victims. The growth of the Internet has provided child pornographers with a distribution vehicle which is perceived to be relatively anonymous.

In February 2006, Mark S. Proctor was sentenced by U.S. District Court Judge to a total of 151 months' imprisonment after pleading guilty to possession and distribution of child pornography. Proctor's arrest was part of "Operation Clean-Sweep", an undercover operation initiated by the Miami Electronic Crimes Task Force. A Secret Service agent met Proctor in a 'Preteen' Internet chat room on 'Yahoo'. Proctor, who believed the undercover agent was the parent of a pre-teen girl, engaged the agent in sexually explicit chats about minors and sent the undercover agent images of child pornography. A search warrant of his residence and seizure of his computers revealed additional images of child pornography. Proctor pled guilty.⁴

7.5.3 Indian Law

The issue of cyber pornography has been dealt with in section 67 of the IT Act where publishing of information which is obscene in electronic form has been made an offence. Section 67 reads as under:

67. Publishing of information which is obscene in electronic form.

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

The section provides that any material which is published, or transmitted or caused to be published in the electronic form shall be an offence in the following situations:

- a) The material so published or transmitted is lascivious;
- b) The material appeals to the prurient interest;
- c) If the effect of the material is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

In case one is found committing an offence under section 67, he shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees. It is worth noticing that the obscenity test in section 67 is the same as that in section 292 of the IPC which deals with sale of obscene books, etc.

Other enactments having a bearing on the issue of cyber pornography are Indecent Representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950. Persons dealing in cyber pornography that is accessible to persons under the age of twenty years are also liable to be prosecuted under section 293 of the IPC.

7.5.4 Cyber Crime Convention

The Convention on Cyber Crime has, under Article 9, dealt with child pornography and corresponds to an international trend that seeks to ban child pornography. It defines 'child pornography' as inclusive of such pornographic material that visually depicts:

- a) a minor engaged in sexually explicit conduct;
- b) a person appearing to be a minor engaged in sexually explicit conduct;
- c) realistic images representing a minor engaged in sexually explicit conduct.

The article requires the member countries to adopt laws which establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

- 1) Producing child pornography for the purpose of its distribution through a computer system;
- 2) Offering or making available child pornography through a computer system;
- 3) Distributing or transmitting child pornography through a computer system;
- 4) Procuring child pornography through a computer system for oneself or for another person;
- 5) Possessing child pornography in a computer system or on a computer-data storage medium.

- c) Anonymity: The cyber stalker can easily use an identity mask thereby safeguarding his real identity.
- d) Geographical location: In online cyber stalking the cyber stalker can be geographically located anywhere.
- e) Ease of indirect harassment: The cyber stalker does not directly harass his victim. Rather, he would post such comments on a common discussion board that would prompt the other users to send messages to the victim under a misconceived notion.

Conventional Crimes
Through Computer

In the first successful prosecution under California's new cyber stalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized of being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999.⁵

Similar problem arose in *State of Tamil Nadu v Suhar Katti*,⁶ where a family friend who wanted to marry a widow, on her refusal, started posting online messages in her name as if she is soliciting. These messages resulted in annoying phone calls. On a police complaint made in February 2004, the accused was traced, put to trial and was ultimately found guilty of offences under sections 469, 509 of the Indian Penal Code and section 67 of the IT Act.

7.6.2 Indian Law

Chapter 22 of the Indian Penal Code deals with criminal intimidation, insult and annoyance. Section 503 provides that whoever threatens another with any injury to his person, reputation or property, or to the person or reputation of anyone in whom that person is interested, with intent to cause alarm to that person, or to cause that person to do any act which he is not legally bound to do, or to omit to do any act which that person is legally entitled to do, as the means of avoiding the execution of such threat, such person commits criminal intimidation. Cyber stalking in effect is committing criminal intimidation with the help of computers. The offender might be causing alarm by sending messages via the Internet to the victim threatening injury to him, his property or reputation. The computer is merely used as a tool for committing the offence or rather improving upon the act of committing the offence and to be able to more effectively threaten his victim. The anonymity over the Internet gives the offender a suitable shield to commit the offence without being easily detected. However, the end-result being the same, cyber stalking is merely criminal intimidation under section 503 of the IPC.

7.7.1 Indian Law

The Public Gambling Act, 1867 prohibits gambling. Section 3 of the Act imposes a fine on the person opening a common gaming-house for others. However, it is also worth noting that the Act presumes a physical place where gambling will take place. The interpretation clause of the Act defined 'common gaming-house' as any house, walled enclosure, room or place in which card, dice, tables or other instruments of gaming are kept or used for the profit or gain of the person owning, occupying, using or keeping such place.

Relevant provisions of the IPC dealing with cheating, criminal misappropriation or criminal breach of trust could be applied in cases of online gambling. However, there is no direct law on this point.

7.8 ONLINE SALE OF ILLEGAL ARTICLES

There are certain articles like drugs, guns, pirated software or music that might not be permitted to be sold under the law of a particular country. However, those who would want to sell such articles find Internet a safe zone to open up online shops. There are specific concerns with regard to increase in online sale of drugs. A simple Internet search will turn up dozens of Web sites that let anyone order drug-of-choice for home-delivery.

The sale of illegal articles on the Internet is also one of those computer crimes where the computer is merely a tool to commit the crime. The traditional crime is already not permissible under various statutes. However, it is being committed by using computer and through the Internet where one gets a better and bigger market along with the benefit of anonymity.

In December 2004, the CEO of Bazee.com was arrested in connection with sale of a CD with objectionable material 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 by the Delhi High Court.⁸ 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.

7.8.1 Indian Law

Under the Indian law, many articles are prohibited for sale. For instance, with regard to sale of arms and ammunition, section 7 of the Arms Act, 1959 specifically prohibits sale of any prohibited arms or prohibited ammunition by any person. Section 9B of the Indian Explosive Act, 1884 makes sale of any explosive an offence if it is done in contravention of the rules. Likewise, section 8 of the Narcotic Drugs and Psychotropic Substances Act, 1985 prohibits sale or purchase of any narcotic drug or psychotropic substance. As regards drugs, sections 18, 27, 27A, 28B and 33I of the Drugs and Cosmetics Act, 1940 prohibit sale of certain drugs or cosmetics. Similarly the sale of banned animal products would be covered under the Wild Life (Protection) Act, 1972. Dealing illegally in antiques is covered by the Antiques and Art Treasures Act, 1972.

Therefore, as far as the issue of legality of sale of any article on the Internet is concerned, it would be governed by a specific statute. Merely because it is being sold through the Internet would not change the character of sale and would still be within the ambit of the prohibitory provision of the enactment.

7.9 SUMMARY

This unit discusses the crimes enumerated in the IPC which can be committed with the aid of the Information Communication Technology (ICT) with more ease and some times with more impunity.

Defamation law – aims at protecting the reputation of the injured person and giving him the right to sue if his reputation is damaged. If a defamatory statement is published on the website, it may have more quantitative and qualitative impact as compared to the publication in a newspaper etc. for instance e-mailing a defamatory statement to a large number of persons or posting it on a discussion board or newsgroups of a profession e.g. lawyers etc. may prove to be very injurious.

Similarly, corporate cyber smearing i.e. injurious or defamatory statement about a company or its officials may be more harmful than the other medium of publication.

Forgery – forgery is a creation of a document which the person knows to be not genuine and yet he projects it to be genuine. With the use of the desk top publishing system, laser and ink-jet printers, colour copier, image scanner etc forged documents such as birth certificates, passports etc can be made and it is more difficult to test the genuineness of such documents.

Pornography – means writings, pictures and films which are sexually exciting. Pornographic material on the Internet can be accessed by any one any where in the world in privacy and without feeling shame irrespective of whether the law of such country permits it or not.

The most disturbing aspect is the increase in the child pornography.

Cyber stalking/harassment – stalking means to follow quietly and secretly. It refers to the use of Internet, e-mail and other communication devices harass or intimidate etc. with a bit expertise in hacking, a person may have access to the personal information stored in the computer and use in stalking and while doing it, he may conceal his identity also.

Gambling – online gambling websites can be operated from the country where it is not illegal. In such types of virtual casinos, it is not necessary to be present in the country from where the site is being operated. A person can be engaged in gambling while sitting in his home even if it is illegal in his country.

Online illegal sale of articles – such as drugs, arms, pirated copies of software's etc. Internet provides a bigger market and privacy to the seller. Through online shopping, these goods can be sold even if their sale is prohibited by law.

7.10 TERMINAL QUESTIONS

- 1) Discuss how the information and communication technology have added new dimensions to many of the technology neutral offences as defined in the Indian Penal Code of 1860.

7.11 ANSWERS AND HINTS

- 1) Every individual has a private right to protect his reputation. Every individual has a right to its own personal space and he would not want others to interfere in that 'space'. However, a public right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India makes enforcement of our private right a challenge. A delicate balance has to be maintained. The law of defamation has been designed to protect the reputation of an injured person and provide such balance between private and public rights by giving him the right to sue for damages. Defamation comprises of both libel (defamation by means of writing) and slander (defamation by speaking).

Quantitative impact of Cyber Defamation

Quantitatively, a comment defaming a person can be sent to a large number of persons through e-mail by a click of the mouse. Much easier would be to publish on a discussion board known to be visited by thousands of persons every day.

Qualitative impact of Cyber Defamation

Qualitatively, the impact of an online comment defaming a person would again depend upon the fact as to where it has been published. Putting a defaming message in specific a newsgroups (for example, a lawyer's group in case one wants to defame a lawyer) would necessarily have a more effective negative impact on the reputation of the person being defamed rather putting the same on a ladies' kitty party group.

- 2) Forgery is creation of a document which one knows is not genuine and yet projects the same as if it is genuine. In common parlance, it is used more in terms of affixing somebody else's signature on a document. Digital forgery implies making use of digital technology to forge a document. Desktop publishing systems, colour laser and ink-jet printers, colour copiers, and image scanners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.
- 3) Pornography literally means, "Writings, pictures or films designed to be sexually exciting". Developing, distributing and propagating the same over the Internet is termed as cyber pornography. This would include pornographic Web sites, pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, photos, writings, etc. In recent times, there have been innumerable instances of promotion of pornography through the use of computers. Information technology has made it much easier to create and distribute pornographic materials through the Internet;

Cyber Crimes and Torts

such materials can be transmitted all over the world in a matter of seconds. The geographical restrictions, which hitherto prevented, to a certain extent, foreign publications to enter into local territories, have disappeared.

- 4) To stalk is to follow quietly and secretly. Cyber stalking is an electronic extension of stalking. The electronic medium is used to pursue, harass or contact another in an unsolicited fashion. The term is used to refer to the use of the Internet, e-mail, or other electronic communication devices to stalk another person. .

Preferred mode of harassment

Five reasons why cyber stalking today is a preferred mode of harassment are:

- a) Ease of communication
- b) Access to personal information: With a bit hacking expertise, one might easily be able to access personal information of a person which would help in further harassment.
- c) Anonymity: The cyber stalker can easily use an identity mask thereby safeguarding his real identity.
- d) Geographical location: In online cyber stalking the cyber stalker can be geographically located anywhere.
- e) Ease of indirect harassment: The cyber stalker does not directly harass his victim. Rather, he would post such comments on a common discussion board that would prompt the other users to send messages to the victim under a misconceived notion.

Internet knows no boundaries. Communication has begun faster and easier. It has become easy to conceal his identity and commit offences. Internet gives access to a large number of persons irrespective of geographical boundaries through e-mail, newsgroups, online shopping etc.

Study the offences discussed in the unit and see how ICT has provided the technology which can be used in the commission of these offences.

7.12 REFERENCES AND SUGGESTED READINGS

- 1. Sharon Walsh. Washington Post Staff Writer. "14 Charged in Internet Betting. The Washington Post". <<http://www.washingtonpost.com/wp-srv/national/longterm/intgambling/stories/charged.htm>>.
- 2. Judgment delivered by Ld. Additional Chief Metropolitan Magistrate. Egmore on 05.11.2004.

3. <<http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>>.
4. 6 No. 6 Cyber Crime Law Reporter 6 <<http://www.usdoj.gov/usao/fls/060210-03.html>>.
5. S. 2(1)(t).- 'electronic record' means, data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.
6. S. 2(1)(d).- 'affixing digital signature', with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
7. <<http://www.legalservicesindia.com/articles/defcy.htm>>.
8. Suit no. 1279 of 2001, Delhi High Court.