CHAPTER 2: EXISTING LEGAL FRAMEWORK IN INDIA TO CURB CYBERCRIMES

1. INTRODUCTION

In modern times, legal regulation of Cyberspace is, the most challenging task of the legal machinery of any particular country. The reason is, the legal machinery operating in the physical territory of any particular country is inadequate to regulate this space.

Science and Technology has made this virtual space too near yet too far from the geographical territories of the nations of the World. In other words, physical boundaries are no more the surest way to handle this issue. To put it simply, the world has been shrunk so many times over that it has become a 'Global Village', at least in this seemingly enigmatic space. Understanding the magnitude of the above issue is only a first step towards solving the same. The demands of trade and technology are ever increasing. The more the time taken in addressing the issue, the more would be the perils the world would be facing. 19th century has brought along with it new forms of commission of crimes. Development in the field of Technology has made a way for Internet. Internet is changing the modes of communication very fastly. It is easy to use and cheaper at cost. However, it is unfortunate that this technological change has brought with it many dis-advantages like hacking, credit cards fraud, child pornography etc. What, civilization is now facing is a new form of crime at global level called – cyber crimes. As Internet is decentralised and disregards the geographical boundaries the problem of cyber-crimes has arisen at global level.

If the problem is at a global level, the solution also has to be of a matching proportion. The global body namely, UNCITRAL (United Nations Commission on International Trade Law) rose to the occasion and drafted the model law which supports international contracts through electronic medium. This model law is known as UNCITRAL Model Law on Electronic Commerce, 1996. The General

Assembly of the United Nations by resolution dated the 30th January, 1997 adopted the Model Law on Electronic Commerce and recommended that all States should give favorable consideration to the Model Law when they enact or revise their laws.

Till 1999, India didn't have legislation, to govern Cyberspace. But, e-commerce and allied activities on the Internet have already begun to make permanent impression in the Cyber world. New communication systems and digital technology have made dramatic changes in way we transact business. Use of computers to create, transmit and store information is increasing. Connectivity via the Internet has greatly reduced geographical distances and made communication even more rapid. While activities in this limitless new universe are increasing constantly, laws must be formulated to monitor these activities. Some countries have been rather vigilant and formed some laws governing the net. (India is one of the countries few countries to bring about a cyber legislation. Other nations include Australia, Belgium, Canada, Denmark, Finland, France, Germany, Italy, Japan, Malaysia, Mexico, Peru, Philippines, Poland, Singapore, Sweden, UK, and USA. (Journal of Indian law Institute. Article by Devashish Bharuuka title- Indian Information Tech. Act 2000. Criminal Prosecution made Easy)

The Information Technology Act has been passed to give effect to the UN resolution and to promote efficient delivery of Government services by means of reliable electronic records. At the out set it is worth mentioning that the Act no-where defines cyber crimes, though it does cover some of the cyber offences. The Act is basically E enabling and aims for recognition of digital signatures among other things.

2. OBJECTIVE OF THE ACT

As per the preamble the basic objectives of IT Act are:

- to grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;

- to give legal recognition to Digital Signature for authentication of any information or matter which requires authentication under any law;
- to facilitate electronic filing of documents with Government Departments;
- to facilitate electronic storage of data;
- to facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- to give legal recognition for keeping books of account by Bankers in electronic form.

The first 17 sections of the Act are largely based on Model Law on Electronic Commerce adopted by United Nations Commission on International Trade Law. It contains 94 clauses divided into XIII Chapters. It has four schedules. Schedule-I seeks to amend the Indian Penal Code; Schedule-II seeks to amend the Indian Evidence Act; Schedule-III seeks to amend the Bankers Book Evidence Act; and Schedule-IV seeks to amend the Reserve Bank of India Act. Computer has many advantages in e-commerce, but at the same time it is difficult to shift business from paper to electronic form due to two legal hurdles
(a) Requirements as to writing and
(b) Signature for legal recognition. Many legal provisions assume paper based records and documents and signature on paper.

The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and Company Affairs then vetted this joint draft. After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner must maintain a register to record the names and addresses of all people visiting his

café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cyber crime and to facilitate speedy locating of a cyber criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable. As (late) Mr. Dewang Mehta, Executive Director of the National Association of Software and Service (NASSCOM) said, "it would only result in closing down of all cyber cafés and ultimately deprive people of these facilities." Finally, the IT Ministry in its final draft dropped this suggestion. The Union Cabinet approved the bill on May 13, 2000 and both the houses of Parliament finally passed it by May 17, 2000. The Presidential Assent was finally received in the third week of June 2000. The Act came into effect on 17.10.2000.

3. SOME IMPORTANT HIGHLIGHTS OF THE IT ACT

- Data, electronic forms and electronic records get legal recognition. They are now admissible in evidence just like paper-based documents.
- The Act gives legal recognition to the system of digital signatures. Digital signature performs the duty of a regular signature. Government will prescribe rules for affixing digital signature.
- Applications and documents can be filed with Government in electronic form.Government can publish gazette in electronic form.
- The Bill creates regularly authorities like- Controller and Certifying Authorities. They are empowered to deal with various issues associated with E-Commerce transactions.
- Government to form Cyber Regulations Advisory Committee to give policy guidelines to the Government and the controller.
- Various computer crimes are defined and penalties provided for infringement of Cyber laws. Hacking with computer system is an offence punishable with imprisonment upto 3 years and with fine upto Rs 2 lacs.
- Government will appoint Adjudicating Officers to enquire into computer crimes and award compensation. Government will establish a Cyber Regulation Appellate Tribunal to hear appeals against orders passed by Adjudicating Officers.

- Controller and Adjudicating Officers are empowered to compound the offences against the Act.
- Police officer not below the rank of DSP can conduct raids and arrest people without warrant for suspected cyber crimes.

4. IMPORTANT PROVISIONS OF THE IT ACT

The Act is arranged in 13 Chapters comprising of 93 Sections along with Four Schedules.

Preamble

The Preamble to the Act states that it aims at providing 'legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and aims at facilitating electronic filing of documents with the Government agencies.

Further, the Act extends to the whole of India including the State of Jammu and Kashmir. As per S.1 cl. (2) of the Act, it also applies to any offence or contravention committed under the Act outside India by any person. However this is subject to the provisions contained in section 75 of the Act. On account of development of World Wide web sites, it was necessary to extend the application of this act to offences committees outside India. It seems that our Indian Legislature wants to give this Act the effect of "LONG ARM STATUTE" – the way it is there in USA, where-by the courts of the respective states can assume jurisdiction over non-resident defendant, subject to the satisfaction of the stipulated conditions based on "purposeful availment" and "minimum contacts".

However, the Act shall not apply to the following

-Negotiable Instruments

-Power of Attorneys

-Trusts

-Wills and other testamentary dispositions

-Contracts for sale or conveyance of immovable property

-Any class of documents or transactions notified by the Union Government.

The General Assembly of the United Nations had adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in its General Assembly Resolution A/RES/51/162 dated January 30, 1997. The Indian Act is in keeping with this resolution that recommended that member nations of the UN enact and modify their laws according to the Model Law. Thus with the enactment of this Act, Internet transactions will now be recognized, on-line contracts will be enforceable and e-mails will be legally acknowledged. It will tremendously augment domestic as well as international trade and commerce.

Legitimacy and Use of Digital Signatures

The Act has adopted the Public Key Infrastructure (PKI) for securing electronic transactions. As per Section 2(1)(p) of the Act, a digital signature means an authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the other provisions of the Act. Thus a subscriber can validate an electronic record by affixing his digital signature. (Digital signature is a digest of the message that is further encrypted for added privacy and security. In the electronic world digital signatures replaces conventional signatures). A private key is used to create a digital signature whereas a public key is used to verify the digital signature and electronic record. They both are unique for each subscriber and together form a functioning key pair.

Section 5 provides that when any information or other matter needs to be authenticated by the signature of a person, the same can be authenticated by means of the digital signature affixed in a manner prescribed by the Central

Government. Under Section 10, the Central Government has powers to make rules prescribing the type of digital signature, the manner in which it shall be affixed, the procedure to identify the person affixing the signature, the maintenance of integrity, security and confidentiality of electronic records or payments and rules regarding any other appropriate matters.

Furthermore, these digital signatures are to be authenticated by Certifying Authorities (CAs) appointed under the Act. These authorities would inter alia; have the license to issue Digital Signature Certificates (DSCs). The applicant must have a private key that can create a digital signature. This private key and the public key listed on the DSC must form the functioning key pair.

Writing requirements

Section 4 of the Act states that when under any particular law, if any information is to be provided in writing or typewritten or printed form, then notwithstanding that law, the same information can be provided in electronic form, which can also be accessed for any future reference.

This non-obstinate provision indicates that the legal recognition of electronic records is an exception to the legal requirement of a paper document in writing. The Parliament intended carefully to provide that the submission of electronic record by any person may not be rejected, therefore, it has taken care to enact that in spite of a requirement under any law for submission of a document in writing or in the typewritten or printed form, a person can submit the document in electronic form. No civil, criminal or revenue court or the department of government would deny the acceptance of electronic records. This will make it possible to enter into legally binding contracts on-line.

Attribution, Acknowledgement and Dispatch of Electronic Records

Chapter IV of the Act explicates the manner in which electronic records are to be attributed, acknowledged and dispatched. These provisions play a very important role while entering into agreements electronically.

Section 11 states that an electronic record shall be attributed to the originator as if it was sent by him or by a person authorised on his behalf or by an information system programmed to operated on behalf of the originator.
As per Section 12, the addressee may acknowledge the receipt of the electronic record either in a particular manner or form as desired by the originator and in the absence of such requirement, by communication of the acknowledgement to the addresses or by any conduct that would sufficiently constitute acknowledgement. Normally if the originator has stated that the electronic record will be binding only on receipt of the acknowledgement, then unless such acknowledgement is received, the record is not binding. However, if the acknowledgement is not received within the stipulated time period or in the absence of the time period, within a reasonable time, the originator may notify the addressee to send the acknowledgement, failing which the electronic record will be treated as never been sent. Section 13 specifies that an electronic record is said to have been dispatched the moment it leaves the computer resource of the originator and said to be received the moment it enters the computer resource of the addressee.

Utility of electronic records and digital signatures in Government Audits Agencies

According to the provisions of the Act, any forms or applications that have to be filed with the appropriated Government office or authorities can be filed or any license, permit or sanction can be issued by the Government in an electronic form. Similarly, the receipt or payment of money can also take place electronically.

Moreover, any documents or records that need to be retained for a specific period may be retained in an electronic form provided the document or record is easily accessible in the same format as it was generated, sent or received or in another format that accurately represents the same information that was originally sent or received. The details of the origin, destination, date and time of the dispatch or receipt of the record must also be available in the electronic record.

Furthermore, when any law, rule, regulation or byelaw has to be published in the Official Gazette of the Government, the same can be published in electronic form. If the same are published in printed and electronic form, the date of such publication will be the date on which it is first published. However, the above-mentioned provisions do not give a right to anybody to compel any Ministry or Department of the Government to use electronic means to accept, issue, create, retain and preserve any document or execute any monetary transaction. Nevertheless, if these electronic methods are utilized, the Government will definitely save a lot of money on paper.

Regulation of Certifying Authorities (CAs)

A CA is a person who has been granted a license to issue digital signature certificates. These CAs are to be supervised by the Controller of CAs appointed by the Central Government. Deputy or Assistant Controllers may also assist the Controller. The Controller will normally regulate and monitor the activities of the CAs and lay down the procedure of their conduct. The Controller has the power to grant and renew licenses to applicants to issue DSCs and at the same time has the power to even suspend such a license (S.25) if the terms of the license or the provisions of the Act are breached. The CAs has to follow certain prescribed rules and procedures and must comply with the provisions of the Act (S.30).

Issuance, Suspension and Revocation of Digital Signature Certificates (DSCs)

As per Section 35, any interested person shall make an application to the Certifying Authorities for a Digital Signature Certificate (DSC). The application shall be accompanied by filing fees not exceeding Rs. 25,000 and a certification practice statement or in the absence of such statement; any other statement containing such particulars as may be prescribed by the regulations. After scrutinizing the application, the CA may either grant the DSC or reject the application furnishing reasons in writing for the same.

While issuing the DSC, the CA must, ensure that the applicant holds a private key which is capable of creating a digital signature and corresponds to the public key to be listed on the DSC. Both of them together should form a

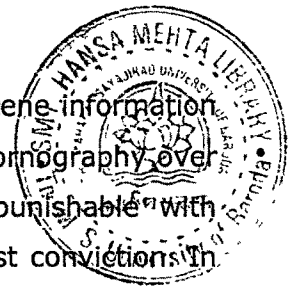
functioning key pair. The CA also has the power to suspend the DSC in public interest on the request of the subscriber listed in the DSC or any person authorized on behalf of the subscriber. However, the subscriber must be given an opportunity to be heard if the DSC is to be suspended for a period exceeding fifteen days. The CA shall communicate the suspension to the subscriber.

There are two cases in which the DSC can be revoked.
Firstly, as per Section 38 (1), it may be revoked either on the request or death of the subscriber or when the subscriber is a firm or company, on the dissolution of the firm or winding up of the company.
Secondly, according to Section 38(2), the CA may *suo moto* revoke it if some material fact in the DSC is false or has been concealed by the subscriber or the requirements for issue of the DSC are not fulfilled or the subscriber has been declared insolvent or dead. A notice of suspension or revocation of the DSC must be published by the CA in a repository specified in the DSC.

Penalties for Computer Crimes

Chapter IX of the Act contains 5 sections dealing with penalties and adjudication. As per the Act, civil liability and stringent criminal penalties may be imposed on any person who causes damage to a computer or computer system. The offender would be liable to pay compensation not exceeding Rs. 1 Crore (10 million) for gaining unauthorized access to a computer or computer system, damaging it, introducing a virus in the system, denying access to an authorized person or assisting any person in any of the above activities. (S.43)
Furthermore, the Act also defines specific penalties for violation of its provisions or of any rules or regulations made there under. However, if any person contravenes any rules or regulations framed under the Act for which no specific penalty is prescribed, he will be liable to pay compensation not exceeding Rs. 25,000 (S.45).

Moreover, any person who intentionally or knowingly tampers with computer source documents would be penalized with imprisonment upto three years or a fine of upto Rs. 2 lakhs or both. In simpler terminology, hacking is made punishable (S.65).



The Act also disallows the publishing and dissemination of obscene information and material. The introduction of this provision should curtail pornography over the net. Any person who disobeys this provision will be punishable with imprisonment of two years and a fine of Rs. 25,000 for the first convictions. In the event of a subsequent conviction, the imprisonment is five years and the fine doubles to Rs. 50,000 (S.67).

The Controller has the power to issue directions for complying with the provisions of the Act (S.68). Failure to comply with his directions is punishable. Moreover, the interference with 'protected systems' or the reluctance to assist a Government Agency to intercept information in order to protect state sovereignty and security is also made punishable.

The adjudicating court also has the powers to confiscate any computer, computer system, floppies, compact disks, tape drives or any accessories in relation to which any provisions of the Act are being violated. No penalty or confiscation made under this Act will affect the imposition of any other punishment under any other law in force. If penalties that are imposed under the Act are not paid, they will be recovered, as arrears of land revenue and the license or DSC shall be suspended till the penalty is paid.

Adjudicating Officers

The Central Government shall appoint an officer not below the rank of Director to the Government of India or equivalent officer of the State Government as an adjudicating officer to adjudicate upon any inquiry in connection with the contravention of the Act (S.46 (1). Such officer must have the legal and judicial experience as may be prescribed by the Central Government in that behalf.

The Adjudicating Officer must give the accused person an opportunity to be heard and after being satisfied that he has violated the law, penalize him according to the provisions of the Act. While adjudicating, he shall have certain powers of a Civil Court.

Cyber Regulations Appellate Tribunal (CRAT)

A Cyber Regulations Appellate Tribunal (CRAT) is to be set up for appeals from the order of any adjudicating officer. Every appeal must be filed within a period of forty-five days from the date on which the person aggrieved receives a copy of the order made by the adjudicating officer. The appeal must be the appropriate form and accompanied by the prescribed fee. An appeal may be allowed after the expiry of forty-five days if 'sufficient cause' is shown (S.57). The appeal filed before the Cyber Appellate Tribunal shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal. The CRAT shall also have certain powers of a civil court.

As per Section 61, no court shall have the jurisdiction to entertain any matter that can be decided by the adjudicating officer or the CRAT. However, a provision has been made to appeal from the decision of the CRAT to the High Court within sixty days of the date of communication of the order or decision of the CRAT. The stipulated period may be extended if sufficient cause is shown. The appeal may be made on either any question of law or question of fact arising from the order.

Police Powers

A police officer not below the rank of deputy superintendent of police has the power to enter any public place and arrest any person without a warrant if he believes that a cyber crime has been or is about to be committed. This provision may not turn to be very effective for the simple reason that most of the cyber crimes are committed from private places such as one's own home or office. Cyber-cafes and public places are rarely used for cyber crimes. However, if the Act did give the police department powers to enter people's houses without search warrants, it would amount to an invasion of the right to privacy and create uproar. Keeping this in mind, the Legislature has tried to balance this provision so as to serve the ends of justice and at the same time, avoid any chaos (S.80).

On being arrested, the accused person must, without any unnecessary delay, be taken or sent to the magistrate having jurisdiction or to the officer-in-charge of a police station. The provisions of the Code of Criminal Procedure, 1973 shall apply in relation to any entry, search or arrest made by the police officer.

Network Service Providers not liable in certain cases

To quote Section 78, it states:

"For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention."

"Explanation. —For the purposes of this section, —

(a) 'Network service provider' means an intermediary;

(b) 'third party information' means any information dealt with by a network service provider in his capacity as an intermediary."

Thus a plain reading of the section indicates that if the network service provider is unable to prove its innocence or ignorance, it will be held liable for the crime.

Cyber Regulations Advisory Committee (CRAC)

The Act also provides that as soon as it is enacted and it comes into force, the Central Government shall constitute the CRAC. The CRAC will assist the Central Government as well as the Controller of CAs to form rules and regulations consistent with the provisions of the Act. The Controller will notify these regulations in the Official Gazette after consultation with the CRAC and the Central Government.

Amendments

With the introduction of the IT Act certain amendments are to be carried out in the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. These amendments will try and make these existing codes Internet compatible.

Section 91 stipulates that the Indian Penal Code shall be amended in the manner specified in the First Schedule of the Act. Through this Schedule read with the Section as many as 17 amendments have been carried out in the Indian Penal Code.

Electronic records have been recognised as documents and appropriate changes have been incorporated in defining offences relating to fraud, forgery, falsification of documents etc. Section 92 stipulates that the Indian Evidence Act 1872 shall be amended in the manner specified in the Second Schedule of the Act. Through this Schedule read with the Section as many as 16 amendments have been carried out in the Indian Evidence Act.

As discussed above in the topic relating to Legal Recognition of Electronic Records, Section 65B has been added as a new Section in Evidence Act, which stipulates admission of electronic records as evidence. Section 85A has been added as a new Section in the Evidence Act, which creates presumption in favour of electronic agreements. Similarly, Section 85B has been added as a new Section in the Evidence Act which creates a presumption in favour of electronic records by stating that the Court shall presume unless the contrary is proved that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

Section 93 stipulates that the Bankers Books Evidence Act 1891 shall be amended in the manner specified in the third Schedule of the Act. Through this Schedule two amendments have been carried out in the Bankers Books Evidence Act, which is discussed in a separate topic below. Section 94 stipulates that the Reserve Bank of India Act, 1934 shall be amended in the manner specified in the Fourth Schedule of the Act and one amendment has been carried out which provides for regulation of fund transfer through electronic means.

5. LEGAL ISSUES INVOLVED IN THE IT ACT

Nothing is perfect in this world. Not even the persons who legislate. Therefore it would not at all be feasible to expect that the laws enacted will be absolutely perfect, without any lacunas.

- Section 67 of the IT Act intends to punish any person who publishes or transmits or causes to be published in the electronic from any material which is lascivious or appeals to the prurient interests 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. The title of the section is "Publishing of Information which is obscene in the electronic form".

  The case-law relating to the offence of obscenity under section 292 and 294 of the Indian Penal Code would provide guidance as to determine whether a particular act of a person is obscene or not. However, obscenity is a question of fact to be decided by the court in each case. In general it may be said that is a publication is detrimental to public morals and is calculated to produce pernicious effect in depraving the minds of persons into whose hands it may come, it will be treated as an obscene publication. The motive behind the publication is immaterial if publication itself is obscene, judged by the above-mentioned criteria. However what is treated as 'obscene' in India is certainly not likely to be treated as obscene in some countries, especially Western Countries. Culture, educational, social and other conditions are not the same in all countries. Section 1 and S.75 of the IT Act, deal with the applicability of the Act and section 1(2) specifically states that the Act applies to any offence or contravention there under committed outside India by any person. Accordingly, the IT Act is also applicable to the offences committed outside India. But it is difficult to imagine how a publication which is not obscene in USA but is obscene in India will be made punishable and by what procedure.

Further, the whole object of eliminating obscene content would be defeated if the Act of "accessing" such material is not punishable but merely its publication, since publication is almost always in the foreign soil and also legal under the laws of several countries. (AIR 2000, "The Information Technology Act 2000 by Abhijit Sen page no.215)

- Section 43 of the act deals with 'Penalty for damage to computer, computer system, etc'. It provides for compensation to the aggrieved party not exceeding one crore rupees. This provision for payment of compensation in terms of money only may not have deterrent effect upon the wrongdoers. In order to have deterrent effect what is further required is a provision for imprisonment along with fine payable by the accused. Under section 44 of the act, provision is made for penalty for failure to furnish information, return etc. and the penalty prescribed under the section is payment of penalty not exceeding 10,000 rupees for every day during which failure continues. No provision for imprisonment is prescribed under S.44 of the Act. Even Section 45, which deals with residuary penalty for the violation of any rules or regulations (for which no penalty has been separately provided), imposes liability to pay compensation not exceeding 25,000 rupees, but it omits to provide for imprisonment of the accused who is found guilty.

  The general view is that when punishment only by way of fine is provided the rigors of the law is reduced to a considerable extent because in modern times payment of fine is not perceived as punishment. Therefore it is submitted that under all the three sections i.e. S.43, 44, and 45 punishment by way of imprisonment must be provided.

- Section 46 deals with appointment of officer not below the rank of Director to Government of India to be an Adjudicating Officer for holding an inquiry. However there is no provision about what technical qualifications the concern authority must possess.

- Section 49 of the Act deals with the composition of Cyber Regulation appellant Tribunal. It provides that a Cyber Appellate Tribunal shall consist of one person only, referred to as the Presiding Officer of the Cyber Appellate Tribunal to be appointed, by notification, by the Central Government. Regarding the qualification for appointment as Presiding Officer of the Cyber Appellate Tribunal, section 50 puts forth that either he is, or has been, or is qualified to be, a judge of a high court, or is, or has been, a member of the Indian Legal Service and is holding or has held a post in Grade I of that service for at least three years.
  What seems to be objectionable over here is the qualification as well as the composition of the Tribunal. It is submitted that the position would be somewhat better if the Tribunal consists of one presiding officer and three-member i.e. a total of four people. One of the members exclusively from the field of I.T. One out of the remaining two (leaving aside the presiding officer) strictly from legal / judicial background and the third having experience of both I.T. & legal field. Further while appointing the presiding officer every endeavor should be made to select a person who has some background of I.T. as well.

- S. 46. deals with Power to Adjudicate – It says -
  (1) for the purposes of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under the Central Government shall, subject to the provision of sub-section (3), appoint any officer not below the
  rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in manner prescribed by the Central Government.
  2) * * *
  3) No person shall be appointed as an adjudicating officers unless he possess such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government
  4) * * *
  5) * * *

A joint reading of sub-section 1) and 3) makes it clear that the Act prescribes that no person should be appointed as an "Adjudicating Officer" unless he possess such experience in Information Technology and legal or judicial experience as may be prescribed by the Government. It would not be below the rank of a Director to the Government of India or an equivalent officer of the State Government.

At this juncture it becomes important to have look at the pecuniary jurisdiction provided to the Adjudicating Officer under this Act. In the present legislations financial penalty imposed by this Act is highest i.e. up to on corer rupees (S.43). This indeed is a praiseworthy attempt to bring at least some relief to the aggrieved.

The Adjudicating Officer has powers to dispense punishment of up to 10 years of imprisonment and up to one corer of financial penalty based on his findings. Those who say that the powers vested to the Police Authorities under this Act as "Draconian" should consider the possibility of misuse of powers by one of the many adjudicating officers who may be operating under the system. Not withstanding the possibility of an appeal, the damage that a dishonest or an inefficient adjudicating officer may inflict on innocent Netizens, Network manager, cyber cafe owners, ISPs, or IT companies could be deliberating. The Act does not specify any checks and balances to prevent misuse of the powers of the adjudicating officers. On the other hand, section 84 provides protection from legal action to the adjudicating officer for acts done in good faith. These provisions are quite loose and vague. Further these provision need to be reviewed and a proper system for appointment, periodical review, transfer, and removal of the adjudicating officer need to be provided.

One of the solutions to this problem is to see that all enquires will be held in the presence of an "Expert watch-dog Committee" consisting of at least three members with requisite knowledge of law and information technology and persons of integrity. This committee can be drawn from a pool of talented persons created for the purpose with the assistance of the Cyber Regulation Advisory Committee. The member of this committee should record their comments independently in a confidential

report to such authority which can be referred to in the event of necessity and when an appeal being heard.

- According to section 82, which deals with Deemed Public Servants, all officers of the Cyber Regulation Appellate Tribunal and the Office of the Controller would be deemed as "Public Servants under section 21 of Indian Penal Code. This clause does not include the Adjudicating officer. It is submitted that the public servant definition should be linked to the definition in the "Prevention of Corruption Act" and not with Indian Penal Code. This change may help to put more check on any misuse of powers.

- Moreover, though the statute is supposedly a 'long arm statute', it does not indicate the powers of the adjudicating officers when a person commits a cyber crime or violates any provisions of the law from outside India. Several practical difficulties may also arise in importing the cyber criminal to India. The Act does not lay down any provisions whereby extradition treaties can be formed with countries where the cyber criminal is located. Therefore, the extra-territorial scope of the Act may be difficult to achieve

- Regulation of intellectual property rights, particularly copyright on the Internet is an ever-growing problem. The Act does not discuss the implications of any copyright violations over the net. It has no provisions to penalize copyright infringers, commonly known as "pirates" for their activities over the net. Internet piracy is a major problem has not been tackled by this Act. No amendments have been proposed to the Copyright Act of India.

- Under Section 80 of the Act, police officers not below the rank of Deputy Superintendent of Police authorised by the Central Government have been given wide powers to search and arrest persons without warrant who has committed or reasonably suspected to have committed or about to commit any offence under the act. These powers seem to be very

wide, and hence, there should be a monitoring mechanism to ensure that no excesses are committed.

- Under the act various provisions are made for imprisonment and fine, but the Act fails to provide which concerned judicial authority i.e. court can impose such imprisonment and fine. If we take a short look to Criminal Procedure Code, then section 6 of the Code deals with the different kinds of the courts such as Judicial Magistrate First Class, Metropolitan Magistrate, and Court of Sessions etc. Further Criminal Procedure Code also provides for the jurisdictional powers that such courts possesses,
  - High court and the court of sessions can pass any sentence of imprisonment and fine. (however, death sentence passed by the sessions court shall be subject to the confirmation of the High Court)
  - Chief Judicial Magistrate can pass any sentence authorised by law except the sentence of death or imprisonment for life or imprisonment for term not exceeding 7 years.
  - Judicial Magistrate First class can pass sentence not exceeding 3 years or fine not exceeding 5000 rupees or both.
  - Court of Magistrate of Second class can impose sentence for not exceeding 1 year and fine not exceeding 1000 rupees or with both.

  Now let us take a look to section 66 of the IT Act, which deals with 'Hacking with Computer System'. The section says "whoever commits hacking shall be punished with imprisonment upto three years and fine which may extend upto 2 lakh rupees or with both. Now, if the case is tried by JMFC court the offender can be sentenced upto 3 years, but the court cannot impose penalty by way of fine for more than 5000 rupees. Thus the act fails to provide necessary provisions for the concerned authority that can try a case and impose necessary imprisonment and fine.

6. APPLICIBALITY OF PROVISIONS OF INDIAN PENAL CODE AND LAW OF TORTS TO CYBERCRIMES

Apart for Information Technology Act 2000, there are other legislations, which indirectly apply to cybercrimes. They include Law of Torts, Indian Penal Code and Contract Act. We will briefly discuss some of the provisions of these enactments, which indirectly deal with cybercrimes. We may apply these provisions in cases where IT Act is silent over the particular issue.

Provisions of Law of Torts applicable to cybercrimes

The law of Torts is mainly the product of judicial decisions. The courts in England have generally shown a favorable attitude towards recognition of an action in novel situations or even recognizing new torts, whenever the changing conditions so demanded. The legislature too have played a significant role in the development of this branch of law by defining liability in various situations, where either some unjustness was caused by the decisions of the courts or the social justice demanded an intervention by the legislature. We have applied the principles of English law to Indian situations in many cases. Tort is a civil wrong for which unliquidated damages are awarded. The difference between tort and crime is that, tort is less serious whereas crime is more serious because it affects the interests of the society at large. Crimes are public wrong. Crimes like Defamation, Fraud, Negligence, and liability for Mis-statements fall in the category of torts.

Defamation is injury to the reputation of the person. A mans reputation is his property and if possible, more valuable than other property. The essentials of the defamation include that, - a). the words must be defamatory, b). they must refer to the plaintiff and c). they must be published. Internet makes us more vulnerable. The reason is, messages, which are sent by one person, can be read by another person also. For example, messages in the chat rooms can be seen by the world at large. They are publication to the whole world. Any such statement by one person in the chat room, may lead him to the commission of the offence of defamation if it affects the reputation of another

person. Apart from this, the messages sent through e-mail are also not secure. They can be easily tampered with. Information Technology Act 2000-doesnot deal with the offence of defamation. In such circumstances we have to depend on the provisions laid down in law of torts. The two most important points are, the statement must refer to the plaintiff and secondly, it must be published. Here publication means making the defamatory matter known to some person other than the person defamed. In case of Internet, if the statements made are such which can affect the reputation of the person and if they are made in such a fashion that it will be known to some person other than the person defamed. However cases in which the statements made are true or are fair comment will not fall within the definition of defamation.

Another tort is, a wrong of deceit. Internet gives freedom of speech and expression. At the same time it opens door for every one to do business. There are examples whereby persons are defrauded due to faulty advertisements on the Internet. The nature of the Internet is such that make us more vulnerable to such wrongs. The person who pays on-line doesn't know, where the payee is located (i.e. in which part of world). What if the person is defrauded on Internet? IT Act does not deal with this issue and therefore we have to rely much on the Law of Torts, and Indian Penal Code. Fraud means willfully making of false statement with intent to induce the plaintiff to act upon it and is actionable when the plaintiff suffers damage by acting upon the same. However we must understood that offences that take place on-line are crimes and not purely civil wrongs and therefore the provisions of Indian Penal Code will be applicable. The term "Fraud" has not been defined in the IT Act 2000 and therefore we have to go back to Indian Penal Code and Indian Contract Act. As per the IPC, a person is said to do a thing fraudulently if he dose that thing with the intent to de-fraud but not otherwise. (S. 25 of IPC). The "defraud" involves two elements; i.e. deceit and injury to the person deceived. As per section 17 of the Indian Contract Act 1972: "Fraud" means and includes any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:

- the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;
- the active concealment of a fact by one having knowledge or belief of the fact;
- a promise made without any intention of performing it;
- any other act fitted to deceive; any such act or omission as the law specifically declares to be fraudulent

This definition of "fraud" in the law of contract applies to civil and contractual relations between the parties and has no application to criminal law. Therefore, in India, S. 415 of IPC, which deals with 'cheating', will be applicable. It says: "Whoever by deceiving any person, fraudulently or dishonestly induces the person so deceived any property to any person, or to consent that any person shall retain any property, or intentionally induces that any person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to cheat".

Apart from this cybercrimes like Hacking, Launching a virus may also fall in the definition of 'Negligence'. Further, the maxim 'res ispa loquitur' can also be made applicable. The maxim says that, when the act explains only one thing and that is that the accident could not ordinarily occur unless the defendant had been negligent the law raises a presumption of negligence on the part of defendant. In case such it will be sufficient for the plaintiff to prove accident and nothing more. Cyber crimes like Hacking and Launching of virus requires some 'positive act' and 'intention' on the part of defendant. Such cases may also be brought under this heading.

Provisions of Indian Penal Code applicable to cybercrimes

Before the IT Act 2000 was enacted the provisions of IPC were applicable. At the outset it must be mentioned that, the IT Act 2000 is basically E enabling (i.e. enabling e-commerce). Though it does discuss and define some of the cybercrimes, it is not exhaustive of all the cybercrimes. In fact, the IT Act nowhere defines cybercrimes. So in cases where the IT Act is silent regarding the cyber offences the relevant provisions of IPC will be applicable. Here it must be understood that, for proving the criminal liability both actus reus and mens rea is required. In cases of cybercrimes, both are present. Since

commencement of cybercrimes requires good knowledge of intricacies of computer, the person concern that commits the cybercrime is well aware of the consequences of his act. We will now discuss some of the provisions of IPC, which may be applicable to cybercrime.

Fraud on the Internet is big business. It constitutes about one-third of the cybercrimes. 'Fraud' has not been defined in the IT Act and therefore we have to back to the provisions of IPC. According to the IPC a person is said to do a thing fraudulently if he does that thing with the intent to defraud but not otherwise (S-25 of IPC). However for the purpose of cyber fraud, the more appropriate word would be 'cheating' which is defined in S-415 of IPC. The essentials of offence of cheating are: - 1). A representation is made by a person, which is false, and which he knows is false 2). The false representation is made with a dishonest intention. 3). The person deceived is induced to deliver any property or to do or omit to do something. The punishment is imprisonment that may extend upto one year or with fine, or with both. Apart for this section 416 of IPC also provides for 'cheating by personation'. Since, the nature of the Internet facilitates netizens to interact without meeting each other physically, cheating by personation becomes easier. Apart for these S-405 and 406 relating to Criminal breach of trust, S-463/465 regarding Forgery, S-477A regarding Falsification of accounts are also attracted. These offences are relevant in the cyber world, which by its nature permits the commission of these offences.

Launching of Virus is also a big threat. It makes net insecure. Apart from S-43 of the IT Act which deals with launching if virus, there is one provision in IPC which may also be applicable here. S-425 of the IPC, which deals with the offence of 'mischief'. The act of launching of virus and other computer contaminants, would also amount to the criminal offence of 'mischief'. If the essentials of 'mischief' are satisfied it would be an offence too.

Cyber defamation and e-mail abuse is rampant on net. The common meaning of defamation is injury done to the reputation of a person. Defamation is criminal offence under the IPC (S-499). The essentials are: 1). Making an

imputation concerning any person. 2). The imputation is made with the intention of causing harm to such person. 3). The imputation is made by words, which are rather spoken or intended to be read, or by signs or by visible representation. Anonymity on the Internet together with speed and global access at low cost have provided an opportunity to criminal netizens to threaten and intimidate others, which is punishable under IPC (S-503). Criminal intimidation by anonymous communication – concealing the name, which is rampant on net, is also punishable under S- 507 of IPC.

Thus, in cases where the IT Act is silent, relevant provisions of the Indian Penal Code, Law of Torts will be applicable to curb the cyber crimes.

7. CONCLUSION

The IT Act is a comprehensive piece of legislation, which aims at policing some of the activities over the Internet. The fundamental approach of the Act is towards validating and legalizing electronic and on-line transactions. Business transaction costs will be curtailed and transaction volumes will multiply. Computer and Cyber Crimes will hopefully be curbed and offenders will be strictly penalized. Policing these crimes is extremely necessary. At the same time the police officers who occupy large powers under the IT Act must also be educated in computers and Internet. This would help them in executing their powers effectively and efficiently.

But in order to curb computer crimes, the police alone cannot make all the difference. Awareness regarding these cyber laws must be created. Private and Non Government organizations must play an active role in communicating this message to the masses. Moreover, the judiciary will also have to play a proactive role in adjudicating cyber trials. A large part of the judiciary is probably unaware of cyber laws and their implications. They must themselves study the laws carefully and effectively enforce them. Co-ordination amongst the organizations, police and judiciary will definitely create some impact and minimize the crime rate. However, the working and implementation of this law will depend greatly on the rules and regulations that will be formed by the

Government and other authorities constituted under the Act. The Act is only a skeletal figure, while it is the rules and regulations that will form the fleshy content.

This Act is not the end but only a beginning to a plethora of legislation that still needs to be formed. It leaves various issues untouched, some of them relating to intellectual property rights, data protection and taxation. No concrete regulations have also been formulated for cross border issues. These issues are of immense importance and the Parliament must speedily frame laws to govern them. While legislation will always be lacking behind as time and technology progress, the Parliament must ensure that it keeps amending the law and enacting new laws to keep pace with ever-changing standards. At the same time, Indian law must be consonant with international standards that are prescribed and that may be prescribed in the future. This is essential if we desire to effectively regulate this boundless world.

India is amongst few of the countries in the world, which have any legal framework for e-commerce and e-governance. Indian industry projections indicate that business transactions over the net would cross Rs. 2500 crore (Rs.25 Billion) by 2002. The correct and honest implementation of this Act would definitely be a boon to the Indian InfoTech Sector. The Act has been passed at a time when the Internet population in India is low and therefore it is hoped that implementing the law should not be very difficult.