CYBER CRIME AND INFORMATION TECHNOLOGY ACT 2000 ~ AN OVERVIEW ~

Nikhil A. Gupta,
2nd Jt. CJJD & JMFC, Newasa, Dist. : Ahmednagar
guptanikhil1@rediff.com

Abstract : This paper highlights the importance of computer in human life. It elaborates the concept of Cyber Crime. It discusses the provisions of Information Technology Act, 2000 along with the sweeping changes brought in by The Amendment Act of 2008. An attempt is been made to discuss the silent features of the amendment Act of 2008. In this paper the important provisions of Information Technology Act are discussed. The offences and penalties prescribed in the Act are discussed in tabular form to understand its nature, punishment and its bailability.
Keywords – Cyber crime, Computer, Information Technology Act, Digital Signature, Electronic Signature, E-Governance.

I INTRODCTION

The Term 'Cyber Crime' needs no introduction in today's E-world. In this world, where everything is available at a click, crimes are also been committed at a click. Cyber Crime thus is the darker side of technology. It is a Crime where the computer is either a tool or a target. The term WWW which stands for World Wide Web has now become **World Wide Worry** because of mushroom growth in cyber crimes.

Crime in a developing nation is a hindrance to its development. It not only adversely affects all the members of the society but it also pulls down the economic growth of the country. Computer Technology provided a boost to the human life. It made the life of human being easier and comfortable. It not only added speed to the life of human being, but it also added accuracy and efficiency. But this computer was exploited by the criminals. This illegal use of computers for commission of crime leads to Cyber Crime. To combat Cyber Crime India got armed herself with The Information Technology Act 2000. This act got drastically amended in year 2008. The Amended Information Technology Act is not only effective than the previous Act it is more powerful and stringent than the previous one.

II IMPACT OF COMPUTER ON HUMAN LIFE

Change is the rule of universe. Nothing in this world is static and technology is providing a pace to this change. The highlight of this era is e-governance. That means the government is available to its citizens at just a click. A farmer is not required to the village officer for obtaining his property extract, its available online to him. The long queues for paying bills are becoming history, people are preferring to pay bills online. E-commerce is becoming a part of business. Shopping on internet through e-commerce website is becoming a trend. Telegram technology has already said good bye to the World, because mobile is available in every pocket.

The impact of globalization and computerisation is phenomenal. It is an era when now we can dream of a paperless world. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

III CYBER CRIME

Cyber Crime is the darker side of technology. The term '**Cyber Crime'** finds no mention either in The Information Technology Act 2000 or in any legislation of the Country. Cyber Crime is not different than the traditional crime. The only difference is that in Cyber Crime the computer technology is involved. This can be explained by following instance;

Traditional **Theft** : A thief enters in B's house and **steals** an object kept in the house.

Hacking : A Cyber Criminal sitting in his own house, through his computer hacks the computer of B and **steals** the data saved in B's computer without physically touching the computer or entering in B's house.

Hence Cyber Crime is a Computer related crime. The I.T. Act, 2000 defines the terms access in computer network in **section 2(a),** computer in **section 2(i)**, computer network in **section (2j)**, data in **section 2(0)** and information in **section 2(v)**. These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime. In a cyber crime, computer or the data are the target or the object of offence or a tool in committing some other offence. The definition of term computer elaborates that computer is not only the computer or laptop on our tables, as per the definition computer means any electronic, magnetic, optical or other high speed data processing devise of system which performs logical, arithmetic and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. Thus the definition is much wider to include mobile phones, automatic washing machines, micro wave ovens etc...

IV PREAMBLE OF INFORMATION TECHNOLOGY ACT

The Preamble of the I. T. Act reflects the objectives with which The Government of India enacted The Act. The objectives of the Act are;

1. To provide 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,
2. To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000. The I. T. Act got President assent on 9th June 2000 and it was made effective from 17th October 2000. By adopting this Cyber Legislation India became the 12th Nation in the world to adopt a Cyber Law regime during 2000.

V SILENT FEATURES OF INFORMATION TECHNOLOGY ACT

The silent features of the Act are;

- The Act gives legal recognition of Electronic Documents.
- The Act gives legal recognition of Digital Signatures.
- It describes and elaborates Offenses, penalties and Contraventions.
- It gives outline of the Justice Dispensation Systems for cyber crimes.
- The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.
- The said Act also proposed to amend to; The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 etc...

VI SCHEME OF THE INFORMATION TECHNOLOGY ACT

The I. T. Act is spread in total **13 chapters**. There are total **90 sections,** the last four sections namely sections 91 to 94 in the I. T. Act 2000 dealt with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted. The I. T. Act commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition. Chapter 2 deals with authentication of electronic records, digital signatures, electronic signatures etc. Thereafter elaborate procedures for certifying authorities (for digital certificates as per IT Act -2000 and since replaced by electronic signatures in the ITAA -2008) are been provided. Chapter XI deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act. Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.

The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

VII APPLICATION OF THE INFORMATION TECHNOLOGY ACT

As per Section 1 of The I. T. Act, the Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. As

per sub clause (4) of Section 1, Nothing in this Act shall apply to documents or transactions specified in First Schedule. As per this first schedule following are the documents or transactions to which the Act shall not Apply;

1. Negotiable Instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
2. A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
3. A trust as defined in section 3 of the Indian Trusts Act, 1882;
4. A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
5. Any contract for the sale or conveyance of immovable property or any interest in such property;
6. Any such class of documents or transactions as may be notified by the Central Government

VIII DEFINATIONS

The I. T. Act, 2000 provides for following definition;

TABLE I

Section 2(a)	Access		**Section 2(r)**	Electronic Form
Section 2(b)	Addressee		**Section 2(s)**	Electronic Gazette
Section 2(c)	Adjudicating Officer		**Section 2(t)**	Electronic Record
Section 2(d)	Affixing		**Section 2(ta)**	Electronic Signature
Section 2(e)	Appropriate Authority		**Section 2(tb)**	Electronic Signature Certificate
Section 2(f)	Asymmetric Crypto System		**Section 2(u)**	Function
Section 2(g)	Certifying Authority		**Section 2(ua)**	Indian Computer Emergency Response Team
Section 2(h)	Certification Practice Statement		**Section 2(v)**	Information
Section 2(ha)	Communication Device		**Section 2(w)**	Intermediary
Section 2(i)	Computer		**Section 2(x)**	Key Pair
Section 2(j)	Computer Network		**Section 2(y)**	Law
Section 2(k)	Computer Resource		**Section 2(z)**	Licence
Section 2(l)	Computer System		**Section 2(za)**	Originator
Section 2(m)	Controller		**Section 2(zb)**	Prescribed
Section 2(n)	Cyber Appellate Tribunal		**Section 2(zc)**	Private key
Section 2(na)	Cyber Café		**Section 2(zd)**	Public key
Section 2(nb)	Cyber Security		**Section 2(ze)**	Secure system
Section 2(o)	Data		**Section 2(zf)**	Security procedure
Section 2(p)	Digital Signature		**Section 2(zg)**	Subscriber
Section 2(q)	Digital Signature Certificate		**Section 2(zh)**	Verify

VIII AMENDMENT BROUGHT IN THE I. T. ACT BY AMENDMENT ACT OF 2008

Cyber Crime is a technology related offence. Technology is never static. It keeps on changing and getting better and better. At the same time Cyber Criminals are exploiting this advanced technology to discover sophisticated ways of committing crime. The Information Technology Act is the saviour in the nation to combat cyber crimes. Thus as the criminals are keeping pace with the advancement in technology, it is equally important for the Law to keep itself update with the recent trends in commission of crime and advancement in technology. With the same intention the Amendment Act of 2008 brought sweeping changes in the old I. T. Act. To overcome the lacuna of old I. T. Act, many bodies, teams of technical experts and advisory groups were construed. They studied the cyber legislations in other foreign countries and recent trend in cyber crime scenario. Their recommendations were scrutinized and the Parliament of India came up with Information Technology Amendment Act 2008. It was placed in the Parliament and passed without much debate. This Amendment Act got the nod of President 05th February 2009. The Amendments were made effective on 27th October 2009.

IX HIGHLIGHTS OF THE AMENDMENT ACT, 2008

The newly amendment Act came with following highlights;

- It focuses on privacy issues.
- It focuses on Information Security.
- It came with surveillance on Cyber Cases.
- The Concept of Digital Signature was elaborated.
- It clarified reasonable security practices for corporate.
- Role of Intermediaries were focuses.

- It came with the Indian Computer Emergency Response Team.
- New faces of Cyber Crime were added.
- Powers were given to Inspector to investigate cyber crimes as against only to DSP.
- Severe Punishments and fine were added.

X DIGITAL SIGNATURE TO ELECTRONIC SIGNATURE

The term '***Digital Signature***' was defined in the old I. T. Act, 2000. This term was replaced by '***Electronic Signature***' by the amending Act of I. T. Act, 2008. Certainly the concept of Electronic Signature is much wider than term Digital Signature. Section 3 of the Act provides for authentication of Electronic Records by affixing his Digital Signature. It shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. By the Amendment Act of 2008 Section 3(A) was embedded in the Act. The newly added provision provides for authentication of electronic record by electronic signature or electronic authentication technique which is, considered reliable and may be specified in the second schedule. Sub Clause (2) provides the circumstances in which the electronic signature or electronic authentication technique shall be considered reliable.

According to the **United Nations Commission on International Trade Law (UNCITRAL)** electronic authentication and signature methods may be classified into the following categories;

1. Those based on the knowledge of the used or the recipient i.e passwords, personal identification numbers (PINs) etc…
2. Those bases on the physical features of the user i.e. biometrics.
3. Those based on the possession of an object by the user i.e. codes or other information stored on a magnetic card.
4. Types of authentication and signature methods that, without falling under any of the above categories might also be used to indicate the originator of an electronic communication (Such as a facsimile of a handwritten signature, or a name typed at the bottom of an electronic message).

According to the UNCITRAL MODEL LAW on Electronic Signatures, technologies currently in use include;

1. Digital Signature within a public key infrastructure (PKI)
2. Biometric Device.
3. PINs
4. Passwords
5. Scanned handwritten signature
6. Signature by Digital Pen
7. Clickable "OK" or "I Accept" or "I Agree" click boxes [1]

XI ELECTRONIC GOVERNANCE

In this era of computer where every word is getting prefixed by word '**E**', Government of India is also not lacking behind and to provide its services to the citizens at their finger tips the Government is also turning in E-Governance. E-Governance is nothing but providing Government Services cheaper, faster and efficiently to the citizens through internet and computer. The Information Technology Act, 2000 gives recognition to the Electronic Governance. Chapter III, Section 4 to Section 10-A, of the Act provides for the provisions regarding Electronic Governance. Section 4 and 5 gives Legal Recognition to electronic records and electronic signatures. Section 6 of the Act authenticates use of electronic record and electronic signatures in Government and its agencies.

The aim electronic government is to ensure transparency in Government. It also makes the Government accessible to the citizen residing in the most remote village of the country.

X OFFFENCES AND PENALITIES

Section 65 to Section 74 describes for offences and prescribes penalties for the offences. To understand each of them, they are arranged in tabular form in Table 2. As per Section 77-B of the Act, the offences punishable with imprisonment of three years and above shall be Cognizable. The offences punishable with imprisonment of three years shall be Bailable. After the amendment of 2008, the power to investigate the offence under this Act is with a Police Officer not below the rank of Inspector as per Section 78 of he Act.

TABLE II

Section	Offence	Punishment	Bailability & Congizability

[1] : Rohas Nagpal : E-commer Legal Issues

Section 65	Tampering with Computer Source Code	Imprisonment upto 3 years or fine upto Rs. 2 lacks	Offence is Bailable, Cognizable and triable by Court of JMFC.
Section 66	Computer Related Offences	Imprisonment upto 3 years or fine upto Rs. 5 lacks	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-A	Sending offensive messages through Communication service, etc...	Imprisonment upto 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment upto 3 years and/or fine upto Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-C	Identity Theft	Imprisonment of either description upto 3 years and/or fine upt Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-D	Cheating by Personation by using computer resource	Imprisonment of either description upto 3 years and /or fine upto Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-E	Violation of Privacy	Imprisonment upto 3 years and /or fine upto Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
Section 67	Publishing or transmitting obscene material in electronic form	On first Conviction imprisonment upto 3 ears and/or fine upto Rs. 5 lakh On Subsequent Conviction imprisonment upto 5 years and/or fine upto Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
Section 67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment upto 5 ears and/or fine upto Rs. 10 lakh On Subsequent Conviction imprisonment upto 7 years and/or fine upto Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
Section 67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description upto 5 years and/or fine upto Rs. 10 lakh On Subsequent Conviction imprisonment of either description upto 7 years and/or fine upto Rs. 10 lakh	Offence is Non Bailable, Cognizable and triable by Court of JMFC
Section 67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment upto 3 years and fine	Offence is Bailable, Cognizable.
Section 68	Failure to comply with the directions given by Controller	Imprisonment upto 2 years and/or fine upto Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
Section 69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment upto 7 years and fine	Offence is Non-Bailable, Cognizable.
Section 69-A	Failure of the intermediary to comply with the direction issued for blocking	Imprisonment upto 7 years and fine	Offence is Non-Bailable, Cognizable.

	for public access of any information through any computer resource		
Section 69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment upto 3 years and fine	Offence is Bailable, Cognizable.
Section 70	Any person who secures acess or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description upto 10 years and fine	Offence is Non-Bailable, Cognizable.
Section 70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres etc.. who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment upto 1 year and/or fine upto Rs. 1 lakh	Offence is Bailable, Non-Cognizable
Section 71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment upto 2 years and/ or fine upto Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
Section 72	Breach of Confidentiality and privacy	Imprisonment upto 2 years and/or fine upto Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
Section 72-A	Disclosure of information in breach of lawful contract	Imprisonment upto 3 years and/or fine upto Rs. 5 lakh.	Offence is Cognizable, Bailable
Section 73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment upto 2 years and/or fine upto Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
Section 74	Publication for fraudulent purpose	Imprisonment upto 2 years and/or fine upt Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

XI COMPOUNDING OF OFFFENCES

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if;

1. The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
2. Offence affects the socio economic conditions of the country; OR
3. Offence has been committed against a child below the age of 18 years; OR
4. Offence has been committed against a woman.

The person accused of an offence under this Act may file an application for compounding in the Court in which offence is pending for trial and the provisions of Sections 265-B and 265-C of Cr. P. C. Shall apply.

XII CONCLUSION

The Information Technology Act is the sole savior to combat cyber crime in nature. Though offences where computer is either tool or target also falls under the Indian Penal Code and other legislation of the Nation, but this Act is a special act to tackle the problem of Cyber Crime. The Act was sharpend by the Amendment Act of 2008, yet the Act is still in its budding stage. There is grave underreporting of cyber crimes in the nation. Cyber Crime is committed every now and then, but is hardly reported. The cases of cyber crime that reaches to the Court of Law are therefore very few. There are practical difficulties in collecting, storing and appreciating Digital Evidence. Thus the Act has miles to go and promises to keep of the victim of cyber crimes. To conclude I would quote the words of noted cyber law expert in the nation and Supreme Court advocate Mr. Pavan Duggal, "***While the lawmakers have to be complemented for their admirable work removing various deficiencies in the Indian Cyberlaw and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyberlaw a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals,***

with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; ….. a legislation which makes a majority of cybercrimes stipulated under the IT Act as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world……"