**Cyber crime**

Q. What is cyber crime?

A. “Cyber” refers to imaginary space, which is created when the electronic devices communicate, like network of computers.

Cyber crime refers to anything done in the cyber space with a criminal intent. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Cyber crime includes acts such as hacking, uploading obscene content on the Internet, sending obscene e-mails and hacking into a person's e-banking account to withdraw money.

Q. Is there any law that governs cyber crime in India?

A. Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

The act does not define ‘cyber crime’. However, any activities which basically offend human sensibilities would come within its ambit. Child Pornography on the Internet constitutes one serious cyber crime.

Q. What constitutes offence under the IT act?

The act recognizes three kinds of offences which are:

1. Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

2. Hacking with computer system

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack:

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

3. 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.

**Cyber Laws**

1. Regulatory norms in Indian cyberspace

The arrival of the Internet and the World Wide Web made it possible for people to communicate and transact over cyber space. It was a revolutionary step for humanity, but it also created a significant need for the regulation and governance of these activities, a requirement that lead to the creation and implementation of cyber laws across the globe. India became the 12th nation in the world to adopt a cyber law regime during 2000.

The country’s cyber laws are contained in the Information Technology, Act 2000. The Act came into effect following the clearance of the Information Technology Bill 2000 in May 2000 by both the houses of the Parliament. The Bill received the assent of the President Of India in August 2000 (IT Act 2000). The IT Act 2000 aims to provide the legal infrastructure for e-commerce in India. At this juncture, it is relevant to understand what the IT Act 2000 offers and its various perspective.

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.

Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that 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 – rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference The said chapter also details the legal recognition of Digital Signatures.

Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

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 proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

2. Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

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

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

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

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

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

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

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