Cyber laws in India

The 21st Century Indian Legal System deals with the following Cyber Laws:-

Information Technology (IT) Act, 2000

With a projected 730 million in 2020, India ranks third in the number of Internet users after the US and China, clocking a compound annual growth rate of 44 per cent over the past few years. It also figures among the top five countries to be affected by cybercrime. Laws against cybercrimes in India have been laid down in the Information Technology (IT) Act 2000. They are as follows:

Hacking and Data Theft: Sections 439 (h) and 66 of the IT Act punish various exercises going from hacking into a computer organize, information burglary, presenting and spreading infections through computer systems, harming computers or computer systems or computer programs, disturbing any PC or PC framework or PC arrange, denying an approved individual access to a PC or PC organize, harming or pulverizing data dwelling in a computer and so on. The greatest discipline for the above offenses is detainment of up to 3 years or a fine or Rs. 5,00,000 or both.

Tampering with Computer Source Document: Section 65 of the IT Act provides punishment for tampering with computer source documents and says that any person who knowingly or intentionally conceals, destroys or changes or intentionally or knowingly causes another to conceal, destroy, or change any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) used for a computer, computer programme, computer system or computer network, when the source code is required to be kept or maintained by law for the nonce effective, shall be punishable with imprisonment for up to 3 years or with a fine which can reach Rs. 3,00,000 or with both.

Receipt of Stolen Property: Section 66B of the IT Act provides punishment for untrustworthy accepting any stolen PC asset or communication device. This segment necessitates that the individual accepting the stolen property should have done so untrustworthy or ought to have motivation to accept that it was taken property. The discipline for this offense under Section 66B of the IT Act is detainment of up to 3 years or a fine of up to Rs. 1,00,000 or both.

Identity Theft and Cheating by Personation: Section 66C of the IT Act provides punishment for identity theft and provides that anyone fraudulently or deceivingly making use of the electronic signature, password or any other special identifying feature of some other person shall be imprisoned for a term which may extend to 3 years and shall also be liable to fine which may extend to Rs. 1,00,000.

Section 66D of the IT Act provides punishment for ‘cheating by personation by using computer resource’ and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment for a term which may extend to 3 years and fine which may extend to Rs. 1,00,000.

Violation of Privacy: Section 66E of the IT Act provides punishment for violation of privacy and provides that any person who intentionally or knowingly captures, publishes or transmits private images of a person without his or her consent thereby violating the privacy of that person, shall be punished with imprisonment of upto 3 years or with fine not exceeding Rs. 2,00,000 or with both.

Obscenity: Sections 67, 67A and 67B of the IT Act provides punishment for publishing or transmitting, in electronic form: (a) obscene things (b) material containing sexually explicit content, etc.; and (c) material containing children in sexually explicit act, etc. The punishment given for an offence under section 67 of the IT Act is, on the first conviction, imprisoned for a term which may extend to 3 years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in a subsequent conviction, imprisoned for a term which may extend to 5 years with fine which may extend to Rs. 10,00,000. The punishment led down for offences under sections 67A and 67B of the IT Act is on first conviction, imprisoned for a term which may extend to 5 years with fine which may extend to Rs. 10,00,000 and in case of second conviction, imprisoned for a term which may extend to 7 years with fine which may extend to Rs. 10,00,000.

Cyber Terrorism: Section 66F of the IT Act provides punishment for cyber terrorism. Whoever, with an intention to threaten the integrity, security or sovereignty of India or to strike terror in the people, denies access to computer resources to a person who is authorised to do so, or tries to access computer sources without authorisation, or causes the introduction of any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it’s likely to do so thereby cause damage or disruption of supplies or services essential to the lifetime of the community or adversely affect critical information infrastructure, is guilty of ‘cyber terrorism’. Whoever knowingly penetrates a computer resource without authorisation and then obtains access to information, data or electronic database that is restricted for the safety of the State or foreign relations, or get access to such information which if leaked would cause great harm to the sovereignty, integrity and public relations in India is also guilty of ‘cyber terrorism’.

Email Spoofing: Email spoofing refers to email that seems to originate from one source but is sent from another source. Email spoofing can also lead to monetary damage.

Indian Penal Code (IPC) On Cybercrimes

- Sec 503 – Sending of threatening messages by emails.
- Sec 499 – Sending defamatory messages by emails
- Sec 463 – Forgery of electronic records
- Sec 420 – Bogus websites, cyber frauds
- Sec 463 – Email spoofing
- Sec 383 – Web- jacking
- Sec 500 – Email abuse
- Sec 292 – Pornography
- Sec 354D – Cyber Stalking
- Internet Time Thief – It is nothing but a way of cheating, where the web is a tool for committing this crime. This will note the usage by an unauthorized person of the web hours purchased for by another person. This type of cyber crime was unheard until the victim reported it. This offence is usually covered under IPC and also the Indian Telegraph Act.
- Web Jacking – The term is coined from "web hijacking". Once a website is web jacked the owner of the site tend to lose all control over it. The person getting such kind of an access is called a hacker who may even alter or destroy any information on that site.
- Salami Attack – This is basically associated with finance and thus the most victims of this crime are the financial institutions. This attack features a unique quality that the alteration is so insignificant that during a single case it might go completely unnoticed. E.g. a bank employee inserts a program whereby a meagre sum of Rs 3 is deducted from customers account. Such a small amount will not be noticeable at all. However, due 90 such mergers from all the account holders collect huge amounts. This is purely a criminal breach of contract.
- Email Bombing – Email bombing means sending a huge number of mails to the victims as a result of which their account or mail server crashes. The victims of email bombing can vary from individuals to companies and even the email service provider. This is one kind of mischief, where the account or server is subject to destruction.
- Virus Attack – Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or by deleting it. They merely make functional copies of themselves and do that repeatedly until they eat up all the available space on a computer's memory. This is one kind of trespass in conventional crime. Though it is purely a cyber crime, it covers under the Indian Penal code.

These are the offences, which are subject to the Indian Penal code and without the general principles of criminal law and specially Indian Penal Code; cyber law cannot work in India. However, the nature of offences changes, the base of the crime is quite the same. Therefore, IPC is having wider scope even in conventional crime and cybercrime in India.

Cyber Crimes Under Special Acts

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms under Arms Act

Other cyber laws in India

Apart from The Information Technology Act 2000 and Indian Penal Code 1860, there are various other laws relating to cyber crime in India. There are many civil laws as well as Tort laws related to the same. They are as follows:

- Common law (governed by the general principles of law)
- The Information Technology (Amendment) Act, 2008 and 2009
- The Information Technology (Removal of difficulties) Order, 2002
- The Information Technology (Certifying Authorities) Rules, 2000
- The Information Technology (Certifying Authorities) Regulations, 2001
- The Information Technology (Securities Procedure) Rules, 2004
- The Bankers` Book Evidence Act, 1891
- The Reserve Bank of India Act, 1934
- Various laws relating to IPRs

Measures to curb cyber crimes under cyber laws and cyber ethics

The main objective of the technology is to provide a sense of security to the users. But nowadays, with the improvement of technology due to cyber crimes and ethics, day-to-day activities have become much more easier and user friendly. It has led to a harsh world of security threats at the same time by agencies like hackers, crackers etc. Hence a number of information technology methods have come up to curb such destructive and dangerous activities to achieve the real objective of such improved technology, i.e., to provide a sense of security to the users. Some measures to curb cyber crimes via cyber law and ethics are as follows:

• Synchronised passwords

Passwords are meant for one`s security. The password synchronised on the card changes after every 30-60 seconds which makes it valid for one-time log-on sessions only. Other methods providing security are fingerprint identification, signature, voice, retinal identification and biometric recognition etc to impute password and pass phrases.

- Encryption

This is an important tool to protect data in transit. Plain content (readable) can hence be changed over to cipher text (coded language) by this technique and the beneficiary of the information can decode it by changing over it into plain content again by utilizing private key. With the exception of the beneficiary whose holder of the private key unscramble the information, nobody can access sensitive data.

The data in travel, as well as the data put away on PC, can be secured by utilizing Conventional cryptography technique. Regular issue lies during the appropriation of keys as anybody who catches it or captures it can make the entire object of encryption to stop. Open key cryptography was one answer for this where the open key could be known to the entire world however the private key was just known to the recipient, it is extremely hard to get a private key from an open public key.

- Firewalls

It divides between the framework and potential interlopers or intruders to shield the arranged archives from spilled or got to. It would just give the information to stream access PCs which in this way are perceived and confirmed by one's framework. Therefore, it just allows access to the framework to ones previously registered with the PC.

- Digital signatures

Advanced or Digital Signature made by utilizing methods for cryptography by pplying algorithms. This has its unmistakable use in the matter of banking where client's mark is accordingly distinguished by utilizing this technique.

Conclusion

The effects of cybercrimes are growing at an alarming rate in this 21st century. Cybercrime, hacking, 'cyber-ethics' etc. is an addition to the crimes in today's era. Hence, we'd like to evolve a 'cyber-jurisprudence' on the basis of which we will evaluate and criticize 'cyber-ethics'. The right to freedom of belief, thought and expression is considered as one of the basic principles of our constitution. The freedom of press additionally guarantees the right provided by our constitution.

There are likewise issues of protection when classified data is caught or unveiled, legitimately or something else. Universally, both administrative and non-state entertainers take part in digital violations, including secret activities, money related robbery, and different cross-fringe wrongdoings. Action crossing universal fringes and including the interests of in any event one country's state along these lines now and then alluded to as digital government assistance.

The advancement of technology has made man hooked into the Internet for all his needs. The Internet has given man quick access to everything while sitting in one place. Social networking, online shopping, storing data, gaming, online studying, online jobs, every