

Information Technology Act 2000-a Critique

M. Sivananda Reddy, *SP Cyber crimes*

Information Technology Act, 2000 was passed by the Parliament in the year 2000. The main objective of the law makers was to facilitate e-commerce. At that point of time i.e., 1998-1999, when the I.T. Act was prepared, the incidence of Cyber Crimes in India was negligible and they did not visualize computer related crimes that would arise in future and the issue of crimes related to computers did not receive much emphasis. Cyber Crimes are increasing in geometric progression in the U.S.A. and other developed countries, causing loss of billions of dollars to business establishments. In the next five years, it is predicted that in the U.S.A., more than 90% of crime will be related to computers or internet and India is going to witness a similar situation with some time lag. In India, there are (3) Sections of the Information Technology Act 2000-a which are specifically relevant to Cyber Crimes viz., (1) Sec.65, (2) Sec.66 and (3) Sec.67 of I.T.Act 2000.

1) Section 65: 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 computer, computer programme, 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.

2) Section 66: 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 values or utility or affects it injuriously by any means, commits hacking (2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

3) Section 67: Publishing of information, which is obscene in electronic form:

Whoever published 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 two 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.

During the implementation of Information Technology Act at the field level, some of the problems faced are discussed below:

- 1) U/S 78 of IT Act, the I.O. should not be below the rank of a D.S.P. This Sec. should be modified so that SIs and above can be IOs, provided they have skills in computers (i.e., B.Sc. Computers, BCA/MCA or B.Tech.). At the field level we do not have D.Ss.P. who have knowledge of computers where as we have many SIs qualified in computer sciences. Rank can not be a criteria for investigation of Cyber Crimes. This clause restricting lower ranks from investigation is mainly due to archaic thinking, wherein, higher ranks are made mandatory for investigation of sensitive crimes such as Dowry Deaths, SC/ST Atrocities, Offences U/ POTA, COCA etc.,
- 2) Online frauds making purchases through stolen credit cards, promising employment, promising delivery of goods at throw away prices and disappearing after receiving funds, prostitution in the guise of escorts, etc., are not covered.
- 3) U/s 80 of IT Act, Police Officer has the power to search & seize in a public place without a warrant. For Search & Seizure in private places, a warrant is required which is time consuming and confidentiality is compromised. As in the case of public places, search & seizure in private places should be allowed without warrant with a letter of authorisation from the concerned unit head.
- 4) Many cases have been reported wherein online purchases were made using credit card Nos. which were acquired illegally by the accused. Such offences are called Identity thefts and no law exists at present to tackle this problem.
- 5) Spamming is not an offence under IT Act 2000 in India. This has become a menace in USA and anti-spamming laws need to be passed.
- 6) Rules to be framed for regulating Cyber Cafes, ISPs, etc.,

To make our country safe from Cyber Crimes, we need to have necessary checks at vulnerable areas. Most of the crime committed is through internet media and we need to have checks, controls in this sphere.

Gateways are main entry points to the country for all internet communications. Filters to screen pornographic material / terrorist related communications should be installed.

ISPs provide internet connection to the customers mostly through cables laid exclusively or using existing telephone lines. They should install devices that can collect and store data regarding access details of customers. Nowadays ISPs are subleasing to cable operators who are not bound by license conditions unlike an ISP. They should be regulated & ISPs should be made responsible for providing log details of cable operators under them Filters to be installed for checking transmission of pornographic material or terrorist related communications. All Gateways / ISPs having an out bound capacity greater than 2 mbps are required to allot an A.C. Room with telephone and monitoring equipment to facilitate monitoring as per conditions of the license.

Cyber Cafes are unique to India and with them, we have certain peculiar problems which need to be tackled. Cyber Cafes offer anonymity and hence are the preferred places for illegal acts, hence rules should be made for maintaining registers in which full details of users (ID Card / Driving License etc) are noted and photographs of users should be taken through web cameras and stored on hard disc for 3 months. Children less than 18 years should not be allowed into Cyber Cafes etc., Temporary internet files / cookies are generally deleted every day by internet café owners, they should be preserved for 30 days at least. Cyber Cafes should be made liable for any offence committed through their Cafes if they do not follow the rules so framed.

All Govt. and Quasi Govt. Agencies should indicate the computers which they want to be declared as protected and communicate to the central government. All Companies / Govt. Organisations having computers should have basic security measures such as fire walls. Such security measures should be made mandatory and no complaint should be entertained for security breaches if these minimum security measures are not installed. (It is like leaving a house wide open without locking the front door etc., and blaming burglars or intruders for theft / loss.) All organisations should have an agreement with their employees making each employee responsible for any unauthorized access made through the system allotted to them. They should install necessary software packages to track their employees access details and action taken for access beyond their authorization. These measures are already being implemented by a few companies but it should be made mandatory for all.

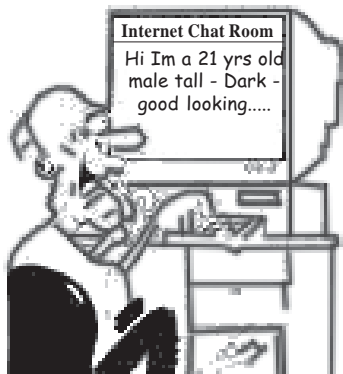
Unlike other acts which are static and do not require frequent modifications, IT Act is dynamic and would require modifications with technological advances. A Committee consisting of Chief of NASSCOM, Law Secretary, IT Secretary and CBI Chief and few business heads should meet regularly once in 3 / 6 months to review existing provisions and suggest necessary changes to Parliament. Unless the act is modified regularly, it would become archaic and obsolete and the best enforcement agencies will be helpless. India has vast resources of man power

in IT field and for fully exploiting global IT related trade / commerce our country should be recognized as a secure place by outsiders only than can we expect commerce to grow. This can happen if our law is not archaic and Enforcement Agencies are well equipped and skills

updated regularly. India should also take a lead in UN to frame international treaty / convention so that the problem of geography / territorial jurisdiction of the accused is not a hindrance for implementing law.



Don't come here. Just visit the website, e-mail, the complaints online and



“Liar chatting on the internet”

“The strictest law often causes the most serious wrong”.

- Cicero (106BC-43BC)