Lecture- 23

Information Technology Act, 2000

The Information Technology Act, 2000 (hereinafter referred to as the "IT Act") is an act 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 alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies.

Grounds on which Government can interfere with Data

Under section 69 of the IT Act, any person, authorised by the Government or any of its officer specially authorised by the Government, if satisfied that it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, for reasons to be recorded in writing, by order, can direct any agency of the Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. The scope of section 69 of the IT Act includes both interception and monitoring along with decryption for the purpose of investigation of cyber-crimes. The Government has also notified the *Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009*, under the above section.

The Government has also notified the *Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009*, under section 69A of the IT Act, which deals with the blocking of websites. The Government has blocked the access of various websites.

Penalty for Damage to Computer, Computer Systems, etc. under the IT Act

Section 43 of the IT Act, imposes a penalty without prescribing any upper limit, doing any of the following acts:

1. accesses or secures access to such computer, computer system or computer network;
2. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
7. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
9. steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Tampering with Computer Source Documents as provided for under the IT Act, 2000

Section 65 of the IT Act lays down that whoever knowingly or intentionally conceals, destroys, or alters any computer source code used for a 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 Rs 2,00,000 (approx. US$3,000), or with both.

Computer related offences

Section 66 provides that if any person, dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to Rs 5,00,000 (approx. US$ 8,000)) or with both.

Penalty for Breach of Confidentiality and Privacy

Section 72 of the IT Act provides for penalty for breach of confidentiality and privacy. The Section provides that any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000, (approx. US$ 3,000) or with both.

Amendments as introduced by the IT Amendment Act, 2008

Section 10A was inserted in the IT Act which deals with the validity of contracts formed through electronic means which lays down that contracts formed through electronic means "shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose".

The following important sections have been substituted and inserted by the IT Amendment Act, 2008:

1. Section 43A – Compensation for failure to protect data.
2. Section 66 – Computer Related Offences
3. Section 66A – Punishment for sending offensive messages through communication service, etc. (This provision had been struck down by the Hon'ble Supreme Court as unconstitutional on 24th March 2015 in Shreya Singhal vs. Union of India)
4. Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device.
5. Section 66C – Punishment for identity theft.
6. Section 66D – Punishment for cheating by personation by using computer resource.
7. Section 66E – Punishment for violation for privacy.
8. Section 66F – Punishment for cyber terrorism.
9. Section 67 – Punishment for publishing or transmitting obscene material in electronic form.
10. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.
11. Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form.

12. Section 67C – Preservation and Retention of information by intermediaries.

13. Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.

14. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource.

15. Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

16. Section 72A – Punishment for disclosure of information in breach of lawful contract.

17. Section 79 – Exemption from liability of intermediary in certain cases.

18. Section 84A –Modes or methods for encryption.

19. Section 84B –Punishment for abetment of offences.

20. Section 84C –Punishment for attempt to commit offences.