Data Protection Laws in India

Data Protection refers to the set of privacy laws, policies and procedures that aim to minimise intrusion into one's privacy caused by the collection, storage and dissemination of personal data.

Personal data generally refers to the information or data which relate to a person who can be identified from that information or data whether collected by any Government or any private organization or an agency.

India presently does not have any express legislation governing data protection or privacy. However, the relevant laws in India dealing with data protection are the Information Technology Act, 2000 and the (Indian) Contract Act, 1872. A codified law on the subject of data protection is likely to be introduced in India in the near future.

The (Indian) Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

Under section 43A of the (Indian) Information Technology Act, 2000, a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. It is important to note that there is no upper limit specified for the compensation that can be claimed by the affected party in such circumstances.

The primary objectives of the IT Act, 2000 are:

- Granting legal recognition to all transactions done through electronic data exchange, other means of electronic communication or e-commerce in place of the earlier paper-based communication.
- Providing legal recognition to digital signatures for the authentication of any information or matters requiring authentication.
- Facilitating the electronic filing of documents with different Government departments and also agencies.
- Facilitating the electronic storage of data
- Providing legal sanction and also facilitating the electronic transfer of funds between banks and financial institutions.
- Granting legal recognition to bankers for keeping the books of accounts in an electronic form. Further, this is granted under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

Features of the Information Technology Act, 2000

a. All electronic contracts made through secure electronic channels are legally valid.
b. Legal recognition for digital signatures.
c. Security measures for electronic records and also digital signatures are in place
d. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

e. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

f. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

g. Digital Signatures will use an asymmetric cryptosystem and also a hash function

h. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.

i. The Act applies to offences or contraventions committed outside India

j. Senior police officers and other officers can enter any public place and search and arrest without warrant

k. Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

The Government has notified the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. The Rules only deals with protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to:-

- Passwords;
- Financial information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information.

The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, the body corporate may be held liable to pay damages to the person so affected.

Under section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000

It is to be noted that s 69 of the Act, which is an exception to the general rule of maintenance of privacy and secrecy of the information, provides that where the Government is satisfied that it is necessary in the interest of:

- the 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,

It may by order, direct any agency of the appropriate 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**. This section empowers the Government to intercept, monitor or decrypt any information including *information of personal nature* in any computer resource.

Where the information is such that it ought to be divulged in public interest, the Government may require disclosure of such information. Information relating to anti-national activities which are against national security, breaches of the law or statutory duty or fraud may come under this category.

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.

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, 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 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.