DATA PROTECTION LAWS IN INDIA

Data Protection refers to the set of privacy laws, policies and procedures that aim to minimize 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.

The Constitution of India does not patently grant the fundamental right to privacy. However, the Courts have read the right to privacy into the other existing fundamental rights, i.e., freedom of speech and expression under Article 19(1) (a) and right to life and personal liberty under Article 21 of the Constitution of India. However, these Fundamental Rights under the Constitution of India are subject to reasonable restrictions given under Article 19(2) of the Constitution that may be imposed by the State.

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.

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 INR 5,00,000 (Approx. US$ 10750).

As of now, the issue of data protection is generally governed by the contractual relationship between the parties, and the parties are free to enter into contracts to determine their relationship defining the terms personal data, personal sensitive data, data which may not be transferred out of or to India and mode of handling of the same.

It is to be noted that section 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.

Grounds on which Government can interfere with Data

Under Section 69 of the IT Act, the Controller, appointed by the Government, can direct a subscriber to extend facilities to decrypt, intercept and monitor information, If the Controller under the IT Act is 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, direct any agency of the Government to intercept any information transmitted through 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.
**Penalty for Damage to Computer, Computer Systems, etc. under the IT Act**

Section 43 of the IT Act, imposes a penalty of INR 10 million inter alia, for downloading data without consent. The same penalty would be imposed upon a person who, inter alia, introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

**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 INR 200,000, or with both.

**Computer related offences**

Earlier, the IT Act under Section 66 defined the term ‘hacking’ and provided penalty for the same. However, the term ‘hacking’ has now been deleted by the introduction of the IT Amendment Act, 2008. The substituted Section 66 now reads as “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 five lakh rupees 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 INR 100,000, or with both.

**Recent amendments as introduced by the IT Amendment Act, 2008**
A new section 10A has been 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.
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

Article By

Vijay Pal Dalmia, Advocate
Delhi High Court & Supreme Court of India

Partner & Head of Intellectual Property Laws Division, Vaish Associates Advocates, New Delhi, India

© 2011. All rights reserved with Vaish Associates Advocates, IPR & IT Laws Practice Division
Flat # 903, Indra Prakash Building, 21, Barakhambha Road, New Delhi 110001 (India)

The content of this article is intended to provide a general guide to the subject matter. Specialist professional advice should be sought about your specific circumstances. The views expressed in this article are solely of the authors of this article.

Specific Questions relating to this article should be addressed directly to the author.