Data Protection and Liability

Rajnish Kumar
National Academy of Indian Railways, Vadodara

DATA PROTECTION LAWS IN INDIA

India presently does not have any direct legislation governing data protection or privacy. However, the relevant laws in India dealing with data protection are the Information Technology Act, 2000 and the Contract Act, 1872.

The 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.

Grounds on which Government can interfere with Data

Section 69 of the IT 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.

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.

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 lakh, 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 there under, 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 100,000, or with both.

Recent amendments as introduced by the IT Amendment Act, 2008

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 72A – Punishment for Disclosure of information in breach of lawful contract

Section 43-A primarily deals with compensation for negligence in implementing and maintaining reasonable security practices and procedures in relation to sensitive personal data or information ("SPDI"). 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.

Section 72-A deals with personal information and provides punishment for disclosure of information in breach of lawful contract or without the information provider's consent. Under this section, 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 lakh.

On 13 April 2011, the Ministry of Communications and Information Technology(MCIT), Government of India, notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules).

Further, on 24 August 2011, the MCIT released a press note (Press Note) which clarified a number of provisions of the Rules. Amongst others, the Press Note clarified that the Rules relate to SPDI and are applicable to body corporate (i.e. organization) or any person located in India.

The Press Note exempts outsourcing companies in India from the provisions of collection and disclosure, as set out under the Rules.

Essentially, SPDI consists of the following:

- ***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.***

Section 43-A of the Act defines 'reasonable security practices and procedures' to mean security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force.

The rules now stipulate that the requirement of 'Reasonable Security Practices and Procedures' will be satisfied if a body corporate has implemented such security practices and standards

and have comprehensive documented information security programmes and policies that are commensurate with the information assets being protected.

The Rules also set out that International Standards(IS / ISO / IEC 27001) is one such standard (Standards) which could be implemented by a body corporate. If any industry association, etc are following standards other than IS / ISO / IEC 27001 for data protection, they need to get their codes approved and notified by the Central Government.

The Rules provide that a body corporate should obtain prior consent from the information provider regarding purpose of usage of the SPDI. The information should be collected only if required for a lawful purpose connected with functioning of the body corporate and if collection of such information is necessary.

The Rules require that a body corporate handling SPDI shall provide a privacy policy. Such privacy policy shall contain the prescribed details such as type of information collected, purpose for collection of information, disclosure policy, security practices and procedures followed, etc. The privacy policy is required to be made available to information providers and is required to be clearly published on website of the body corporate.

According to the Rules, a body corporate is required to designate a Grievance Officer to address grievances of its information providers and should publish the name and contact details of such Grievance Officer on its website. The Grievance Officer is required to redress the grievances within one month.

With this in background, it will now be evident that PROTECTION of Data is responsibility of the organizations and adequate attention must be accorded to the issue by the Head of Institution.

References:

Mali, Prashant., CYBER LAW & CYBER CRIMES, Snowwhite Publications, Mumbai, India, 2012

http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

http://deity.gov.in/content/information-technology-act

http://www.cyberlawsindia.net/

http://www.asianlaws.org/index.php#.U0PJY6iSyBI

Contact:

rajnishkumar@nair.railnet.gov.in
rajnishkumar1971@gmail.com

Updated till April 2014

Disclaimer: The information has been collected from several sources and is only for reference.