Submitted on: 26th September 2013
Accepted on: 15th November 2013

Article can be accessed online at http://www.publishingindia.com

DATA PROTECTION LAW IN INDIA: A BUSINESS PERSPECTIVE

Ashutosh Verma*

Abstract *With the increasing use of cyberspace for business operations, regulation of data protection has become a pertinent issue. The Information Technology Act 2002,though originally not intended to cover data protection, filled the legal gap on this aspect for both the individuals and the business entities. The Act has been subjected to amendments to tighten the data protection regime in India. The insertion of Section 43A and the issue of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 aim to protect sensitive personal information and bring the safeguards at par with international standards. The rules put greater responsibility on the corporates to ensure protection of data which is in their possession. Body corporates will have to implement comprehensive security practices and standards for protection of information assets. Information Technology (Intermediaries Guidelines) Rules, 2011 have spelt out the responsibilities of the intermediaries more clearly. However, there is still a long way to bring the entire data protection regime in India at par with global standards.*

Keyword: *Data Protection, IT Act, Data Theft, Sensitive Information, Data Interception*

DATA PROTECTION LAW IN INDIA: A BUSINESS PERSPECTIVE

The cyberspace revolution which significantly made inroads into the trade and commerce in the late nineties brought about a paradigm shift in the business operations. It became a very important medium for undertaking such operations. Cyberspace overrides the restrictive barriers which are present in a physical market. The easy transferability of data and information in cyberspace led to a new kind of business practice called as business process outsourcing (BPO) or off-shoring, wherein personal data of customers were being transferred to countries with low cost of services for processing and handling of such data. India,being a low cost provider of such services benefitted by this as financial, educational, legal, banking, healthcare, marketing, and telecommunication services were outsourced to India (Nair, 2005). However, concerns have been raised by the international business community about the data protection regime in India. Further, the boom in online business operations within India resulted in sharing of personal information by the customers with various sellers and service providers on the internet. Every time a person undertakes an online transaction, he/she is required to provide detailed personal information and then agree to a number of terms and conditions of the contract which are either not fully read or understood by the individual. In addition, financial information relating to bank accounts, debit cards and credit cardsare being disclosed by the individuals in the cyberspace. All this makes it possible to track down the movements of any person as he/she leaves behind an electronic trail on every visit on the internet. Collection of this information in a scattered manner and its subsequent organisation and cross verification leads to preparation of a personal profile of the person without his/her knowledge and consent. This intrusion into privacy due to information technology has left open legal gaps to protect the right of privacy. Further, the convergence of technologies has spawned a different set of issues concerning privacy rights and data protection. Innovative technologies make personal data easily accessible and communicable. This has raised pertinent questions about the protection of the data being shared by the individuals with business entities and the preservation of his/her private information. The law on data protection in India has to address the privacy rights of persons in real and cyber space, freedom of information and right to know of people at large (Desai, 2011). Though there is no right to privacy enshrined in the Constitution of India, it is implied in Article 21 of the Constitution. In the *Kharak Singh v/s State of U.P.* case, the Supreme Court upheld the right of privacy under Article 21 of the Constitution. Thus, the data protection law has to strike a balance between right to know and information and the right to privacy.

Information Technology Act 2002 (ITA), Information Technology Amendment Act 2008, (ITAA) (hereinafter referred to as the Act), various circulars, rules, clarifications notified under this Act mainly deal with data protection in India. According to the Act "*data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being*

* Indian Institute of Forest Management (IIFM), Nehru Nagar Bhopal, Madhya Pradesh, India.
Email: ashutoshverma512@gmail.com

processed or has been processed in a computer system or computer network and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer." 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 (Dalmia, 2012). Data protection is aimed at protecting the informational privacy of individuals, while database protection has an entirely different function, namely protection of the creativity and investment put into the compilation, verification and presentation of databases.

REVIEW OF LITERATURE

The concept of data protection in business enterprises was first introduced by ITA which gained prominence over the years on account of the need for more comprehensive legislation for the data protection. There have been studies which have reviewed, commented and made critique of the cyber laws in India. Studies have also been undertaken comparing the Indian laws with their counterparts in other countries. Dalal (2006) evaluated the legal provisions of data protection in India in the light of the TRIPS agreement. The study discussed the various legal provisions and concluded that the existing framework was sufficient and the fear of MNCsabout absence of appropriate framework for data protection was unwarranted. Therefore, any new legislation should incorporate the missing links and should not be such that it may run the risk of being declared unconstitutional. Ardhapurkar*etal.*(2010) have suggested a framework to deal with the data privacy in the legal, technical and political domain. The study observed that ITA and ITAA were more for facilitating e-commerce rather than to handle the challenges arising on account of data mining and cloud computing. The system proposed by them was in keeping with the present challenges and looked at individual privacy from a new perspective.Sumanjeet (2010) examined ITA and ITAA in the perspective of e-commerce. The study aimed at critical reflection of e-commerce issues in the context of existing laws. The study concluded that there should be separate laws for e-commerce in India. Jamil and Khan (2011) evaluated the system and the legal framework of cyber laws in India and also compared it with the similar legal provisions in European Union (EU). The study found that India is far behind EU and it recommended that for sustaining its position as an outsourcing hub, it needed to bring in a legal framework which will assure the international community about the privacy of the data being handled by Indian companies. GargandKuchhal (2013) have discussed the provisions of various laws which directly or indirectly deal with data protection in India. The paper also discussed the impact of these laws on society and made a comparison with the similar laws in U.S. and U.K. The study concluded that all types of data do not have the same utility and importance and therefore categorization of data and their protection based on their category had be incorporated into the statute books. Thus studies have focused on the entire cyber laws rather than the part of the law which deals with data protection. This paper is different as it is focused only on the data protection provisions in the law and evaluates them from the perspective ofcommercial organizations.

DATA PROTECTION IN THE ACT

The objectives as enumerated in the Act areto give legal recognition to the electronic documents, electronic transactions, digital signatures, and to promote e-governance in government administrative system. The original objectives of the Act did not intend to fill legal gaps in data protection. However, in the absence of any other law on data protection and the increasing pressure from the industry as well as civil societies and consumer groups, the subsequent amendments in the Act have mainly focused on the data protection regime in India. The government has for the time being decided not to introduce separate data protectionlegislation but to improve and increase the ambit of this Act to cover its various legal aspects. Therefore, it is expected that this legislation will be subject to frequent amendments and additions so as to keep pace with the rapid changes in technology.

CIVIL LIABILITY FOR DATA THEFT AND DAMAGES TO COMPUTER

Section 43 is the major section which deals with civil liability for damages to computer and data theft. The maximum damages were originally Rs. 1 crore, but the amendment has removed this limit. Any person who engages in the following acts, in relation to a computer, computer system or computer network (includes hardware, software and databases) will be liable to pay compensation to the person who is affected by those acts:

(i). **Unauthorised Access:** If a person actually accesses a computer resource, computer network, without the permission of the owner or in-charge of the system, he/shewill be considered as an unauthorised access. This provision clearly prohibits unauthorised access, without referring to the subsequent outcomes. Thus, unauthorized acts of employees who do not have access to certain level of information, trying to gain information will fall within this provision. Providing assistance to any person to have unauthorised access to any such system which is in contravention of the provisions and the rules and regulations made under this Act will also fall under this category.

(ii). **Unauthorised Data Extraction:** Downloading, copying or extracting any data or database and such acts in relation to data which may be on a removable storage medium, without the permission of the owner or any other person who is in-charge of a computer, computer system or network.This provision can act as a check especially on employees who while leaving the organisation attempt to take confidential information of the company along with them.

(iii). **Spreading Virus:** Acts of contamination by sending sets of computer instructions that are specifically designed to modify, destroy, delete the data or programme or which will usurp the normal operations of the system or network. It includes the acts of sending any instruction, information, data that adversely affects the performance of a computer or which attracts itself to another computer source in the form of a virus.

(iv). **Damages or Disruption:** Acts which destroy, alter, delete, add, modify and disrupt the computer database or any other programme or act which adversely affect the value or utility of such resource or cause physical damage to computer or computer networks.

(v). **Denial of Authorised Access:** An act of denying a person or creating conditions leading to denial to a person access to a system for which he/she has the valid authorization. This includes stealing and changing passwords leading to inaccessibility to the system.

(vi). **Manipulation of Charges for Services:** Any act whereby the charges for a particular service rendered to a person are being levied and recovered from another person who has not been a beneficiary of those services.

CRIMINAL LIABILITY FOR DATA THEFT AND UNAUTHORISED DATA DISCLOSURE

All acts mentioned above and referred to in Section 43, are criminal offences if the person engages in those acts dishonestly or fraudulently as per the meaning assigned to these two words within the relevant section of the Indian Penal Code. It is punishable with imprisonment uptothree years or with fine which may extend upto Rs. 2 lakhs or with both. Other acts relating to data theft which entail criminal liability and subject to the same punishment are:

(i). **Theft and damage to source code: A**n act of stealing, concealing, destroying, altering or causing another person to engage in such acts for a computer source code with an intention to cause damage to it. Computer source code means the listing of programmes, computer commands, design layout and programme analysis of computer resource in any form. While this section provides for compensation in case of damages to source code, it also entails criminal liability. Any tampering by any such acts mentioned above of a computer source code which is required to be maintained by law for the time being in force, is a criminal offence.

(ii). **Identity Theft:** If any person dishonestly or fraudulently uses the password, login name or any other code which is peculiar for identity, or the electronic signatures, it is a criminal offence under Chapter IX of the Act.

(ii). **Receiving Stolen Computer Resources:**An act of dishonestly or fraudulently receiving stolen computer resource or communication device.

(iv). **Breach of Confidentiality and Privacy:** Unless provided under this Act or any other law in force, a person who by virtue of the powers conferred under this Act and its rules, obtains electronic records, books, register, correspondence or other material, discloses such records without the consent of the person concerned shall be liable to imprisonment which may extend upto two years or with fine which may be upto one lakh rupee or with both.

(v). **Disclosure of information in breach of lawful contract:** Any person including an intermediary who has secured access to any information which is personal in nature, discloses it without obtaining the consent of the concerned person knowing fully well that it is going to cause wrongful loss or gain or such disclosure is in breach of the contract entered into with such person attracts criminal liability under the Act.

OBLIGATION OF CORPORATES FOR PROTECTION OF DATA

The legal position in respect of this can be analysed by a reading of Section 43A along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter referred to as rules). Section 43A inserted by the amendment in 2008 has imposed greater responsibility on the corporates to ensure protection of data which is in their possession.According to this section, if any body corporate which is dealing or handling sensitive personal information fails to implement reasonable security procedures leading to a loss or damage to a person, then such body corporate will be liable to pay damages as compensation to the person affected by such acts. The rules deal and elaborate this section in terms of operationalisation by following:

(i). **Definition of Sensitive Personal Data or Information:** The rules define "*personal information means any information that relates to a natural person, which either directly or indirectly in combination with*

other information available or likely to be available with a body corporate is capable of identifying such person." The sensitive data is indicated as including password, financial information, physical and mental health, medical records, biometric information, and any other information obtained under a lawful contract. However, information under public domain or which is required to be furnished under the Right to Information Act will not be part of personal information.

(ii). **Policy on Privacy and Disclosure of Information:** The body corporate will have to draft a document which should incorporate clear statements of its practices and policieson type of personal information collected, disclosure of sensitive information and reasonable security procedures. The policy will have to be brought to the notice of every person with whom the body corporate is entering into a contract and from whom the personal information is being collected.

(iii). **Consent for Collection of Information:** Prior consent in writing must be obtained from the person from whom the body corporate intends to collect personal information. Further, such information should be collected for a lawful purpose and such collection should be necessary to achieve that purpose.

(iv). **Awareness of Collection Process:** The body corporate will have to take appropriate steps to ensure that while collecting information, the person must have knowledge about the fact that information is being collected, the purpose of its collection and the name of the agency which is receiving the information and will retain the information in future.

(v). **Retention of Information:** The body corporate will be able to retain the information till the purpose of collection has been achieved. Further, if there is any law which prescribes the time limit in relation to the information collected, then the same must also be complied with by the body corporate.

(vi). **Right of Access and Correction:** Persons providing information will always have access to the information for review and to bring to notice any deficiencies and inaccuracies in the information. The body corporate will be under an obligation to rectify the errors, inaccuracies brought to its notice by the provider of information. The body corporate cannot be held responsible for the authenticity of the personal information.

(vii). **Right of Refusal:** The information provider will always be given an option to provide or refuse to provide the personal information sought by the body corporate. The person availing the services of body corporate will have the right to withdraw his/her consent in writing which was given earlier. In such cases, body corporate can refuse to provide services or discontinue providing the services, if the consent was withdrawn subsequently.

(viii). **Grievance Redressal Mechanism:** In case there is any grievance of information provider in relation to information processing, the same must be addressed by the body corporate in an expeditious manner, but not more than one month from the receipt of the communication from the person. There will a designated Grievance Officer who will handle these issues and his/her details must be available on the website of the body corporate.

(ix). **Disclosure to Third Parties:** Disclosure of personal information to third parties is possible only if the consent of the provider has been taken or if this clause has been specifically inserted in the contract. However, there is an exception for obtaining the consent, in case the information is sought by the government agencies. The agencies will ask for the information in writing and will also specify the purpose for which information is being sought. The agencies may seek information for identity verification or for detection and prevention of cyber incidents or crimes. Further, information will have to be disclosed where an order for the same has been issued under any law for the time being in force. The third party receiving the information will be under an obligation not to disclose it further to anybody.

(x). **Transfer of Information:** A body corporate may if required for the performance of contract or on obtaining the consent of the information provider, transfer information to a third party in or outside India which has the same level of security for data protection as provided in these rules.

(xi). **Reasonable Security Practices and Procedures:** Body corporate will have to implement appropriate security practices and standards for protection of information assets. It will have to develop a comprehensive document containing information security programmes and policies which deal with all the aspects of security arrangements. The security standards may be such as thebest practices of data protection developed by any industry association and approved by the central government. The rules specifically mention International Standard IS/ISO/ IEC 27001 on Information Technology – Security Techniques – Information Security Management System-Requirements as one such standard. Body corporates which follow the standard mentioned above or the best practices developed by their industry association shall be deemed to have complied with this provision. The security practices will have to be audited at least once a year. In case the body corporate is negligent in implementing these security procedures and any concerned person suffers a wrongful loss due

to this, he/she can claim compensation by approaching the adjudicating authority or the civil court respectively depending on whether the compensation claimed is above or below Rs. 5 crore.

The rules were aimed at plugging in the loopholes in data protection, but lead to some major concerns of the industry. The government in order to clarify the concerns of the industry issued a press note on 24 August 2011, clarifying some of these issues or concerns. The important highlights of this press note are:

(i). The rules are applicable to sensitive personal data or information whereas originally the terms 'information', 'personal information' and 'sensitive data and information' were used in the same sense creating confusion that it was applicable to all the three terms.

(ii). The second clarification is regarding the entities to which it is applicable. The press note clarifies that it applies to any body corporate or any person who is located within India. Thus, if the person is located in India, the location of the computer resource being whether in India or abroad is immaterial. If the computer resource is in India, but the body corporate is located outside India, then the rules will not be applicable in such cases. The term provider of information could mean individuals providing information as well as entities that collect individual information and pass on to others, however, it will be referring to only individuals.

(iii). The rules will be applicable only where the service provider is directly providing service to the persons under a contractual obligation. Thus, body corporates which are in possession of sensitive information on account of passing of information by another body corporate which entered into contract with information provider will be exempted from these provisions.

OBLIGATIONS OF INTERMEDIARIES FOR DATA HANDLING

The term intermediary is defined as any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes service providers for telecom, network, internet, web hosting, search engines, online payment sites, online auction sites, online market places and cyber cafes. The Act provides that intermediary, who has provided communication link or hosted information or data of a third party will not be liable in case the role of intermediary is limited to providing communication system on which information is stored, hosted or transmitted. Secondly the liability will not arise if the intermediary does not select the receiver of transmission or does not select or modify the information contained in transmission. Further, the intermediary should follow the guidelines prescribed by central government and follow the due diligence procedures. An intermediary is liable if it has, in any way, conspired in the commission of the unlawful act. The responsibilities of intermediaries have been more clearly spelt out in the Information Technology (Intermediaries Guidelines) Rules, 2011. According to this rule, the intermediary on its own knowledge or on account of communication received from a person aggrieved by the information stored, published or hosted shall take immediate steps in consultation with the user or owner of the information to disable such information. The time limit set out for disabling is 36 hours and such records or information will have to be preserved for a minimum of 90days.

POWERS OF GOVERNMENT FOR DATA INTERCEPTION AND DISCLOSURE

Section 69 along with its amended Section 69A and B empower the government and its agencies to intercept, monitor, decrypt any information stored, communicated through any computer resource under certain circumstances. The Indian Telegraph Act of 1885 empowered the government to do phone tapping in case of the public interest or emergency. However, this section is far more intrusive as it enables the government agency to comply with certain procedures and then it is possible to listen to phone calls, read SMS or emails and monitor the websites visited by a person. The nodal agency i.e., Indian Computer Emergency Response Team will be exercising these powers. The central or state government may authorise any of its officers for interception, monitoring and decryption of information if it satisfied that it is necessary to do so in the interest of sovereignty or integrity of India, defense of India, security of the state or for public order. The government may in order to identify, analyse or prevent the spread of any virus, monitor and collect traffic data or information from any computer resource. The owner or the intermediary of the computer resource shall be required to provide all the necessary assistance and facilities to have online access to such traffic data or information. Any person who refuses to provide such assistance incurs criminal liability with prison term upto three years or with fine or with both.

CONCLUSION

Privacy and data protection are important issues that need to be addressed today as information technology assumes greater importance in personal, professional and commercial spheres (Udapudi and Ghosh, 2012). The data protection legislation in India still falls short of European Union (EU)

Data Protection Directive 95/46/EC or safe harbor policy. The provisions are very specific to the documents and records in electronic form. There is no separate classification of the parties as data provider, data processor, data controller and data user. The Act also needs to contain provisions for third country transfer of data. Data protection is used in a very limited sense in the Act and a regulatory framework which is broad enough to cover all the aspects needs to be established. Further, all the aspects on data protection should be brought at par with global standards so that there is no need to provide for elaborate terms and conditions in the contracts between the foreign parties and the data processing Indian parties. There is no difference between data at rest and data in transit as far as the level of encryption is concerned (DSCI, 2010). The issue of implementing standard security procedures will be subject to wide scrutiny especially on account of the cloud computing scenario become more popular wherein data is being stored and processed on remote servers rather than on local servers (IIBF, 2011). Issues on responsibility and the kind of agreements between the information owner and custodians will have to be clarified in coming times. Thus, the data protection legislation will have to keep pace with the evolving technology to keep it relevant and up-to-date.

REFERENCES

Ardhapurkar, S., Srivastava, T., Sharma, S., Chaurasiya, V., & Vaish, A. (2010). Privacy and data protection in cyberspace in Indian environment. *International Journal of Engineering, Science & Technology*, *2*(5), 942-951.

Dalal, P. (2006). Data protection law in India: The TRIPS perspective. *Journal of Intellectual Property Rights*,*11*(3), 125-131.

Dalmia, V. P. (2012). *Data Protection Laws in India.* Retrieved fromhttp://www.vaishlaw.com/article/information_technology_laws/data_protection_laws_in_india.pdf?articleid=100324

Desai, N. (2011). *Technology Law Analysis.* Retrieved fromhttp://www.nishithdesai.com/New_Hotline/IT/IT%20Hotline_final_aug%2026.htm

DSCI (2010). Information Technology Act, 2000 & Information Technology (Amendment) Act 2008, Frequently Asked Questions, Data Security Council of India, New Delhi.

IIBF (2011). Cyber Laws in India. Retrieved fromhttp://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

Garg, A. K., & Kuchhal, S. (2013). Data protection laws in India: A comparative study. *Indian Journal of Applied Research, 3*(1), 75-76.

Jamil, D., & Khan, M. N. A. (2011). Data protection act in India compared to the European union countries. *International Journal of Electrical & Computer Sciences*, *11*(6), 16-20.

Kharak Singh v State of U.P.AIR 1963 SC 1295.

Nair, L. R. (2005). Does India need a separate data protection law. *World Data Protection Report, 5*(12), December.

Sumanjeet (2010). The State of e-commerce Laws in India: A Review of Information Technology Act. *International Journal of Law & Management*, *52*(4), 265-282.

Udapudi , S. V., & Ghosh, B. (2012). The information technology act of India: A Critique.*Zenith International Journal of Business Economics and Management Research, 2*(5), 182-194.