Data protection and outsourcing industry - A study

By Kumar Mihir

"Scientia Potenti Est- Knowledge is power". The said maxim is apt to describe the primary business model in the 21st century when information is the key to success. With the world outsourcing its essential services to India, there is a growing clamour to ensure protection of the data and other sensitive information passed on and handled by the Indian outsourcing industry. In the factual background of India having emerged as the outsourcing hub and it is more appropriate to evaluate the legal regime for protection of data. As the outsourcing industry is primarily data driven, effective legal provisions for protection of the same are required. India, however, does not have a dedicated statute for the protection of data like the Data Protection Act, 1998 of the United Kingdom and only a few provisions of the Information Technology Act, 2000 deal with protection of data in India.

International obligations

Article 39 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) enjoins the members to make laws to protect data/ information. Article 39 of TRIPS reads as follows:

> *"**Article 39***
>
> *1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.*
>
> *2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:*
>
> *(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
> *(b) has commercial value because it is secret; and*

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

.....”

Despite the above, India, though being a member of WTO, does not have a separate Data Protection Law. The only statute governing the field has been the Information Technology Act, 2000 which has been enacted to give effect to the resolution A/RES/ 51/162 dated 30th January 1997 passed by the General Assembly of United Nations whereby it adopted the Model Law on Electronic Commerce prepared by the United Nations Commission on International Trade Law (UNCITRAL).

Statutory regime & outsourcing industry

The Information Technology Act, 2000 (‘the Act’ for short) came into force on 17-10-2000 vide G.S.R No. 788(E) dated 17-10-2000 and for the first time, legal definition of “Computer”, “Data”, “electronic record”, “Information” *et al* was provided. The said Act gave a legal recognition to the electronic records and digital signatures and in Section 43 thereof provided for damages not exceeding Rs. 1 crore in case of unauthorised access, download or copying or damage to data etc. Chapter IX of the Act provided for penalty and adjudication and Chapter XI (Sections 63 to 78) provided for criminal liability in cases of tampering, hacking, publishing or transmitting obscene material, misrepresentation etc.

However, the provisions of the Information Technology Act, 2000 were not adequate and the need for more stringent data protection measures was felt. The Information Technology (Amendment) Act, 2008 was enacted which came into force on 27-10-2009. The said amending Act brought in the concepts like cyber security in the statute book and widened the scope of digital signatures by replacing the words “electronic signature”. The amending Act also provided for secure electronic signatures and enjoined the Central Government to prescribe security procedures and practices for securing electronic records and signatures (Sections 15-16). It also removed the cap of Rs. 1 crore as earlier provided under Section 43 for damage to computer and computer systems and for unauthorised downloading/ copying of data. Section 43A was introduced providing for compensation to be paid in case a body corporate fails to protect the data. Section 46 of the Act prescribes that the person affected has to approach the adjudicating officer appointed under Section 46 of the Act in case the claim for injury or damage does not exceed Rs. 5 crore and the civil court if the claim

exceeds Rs. 5 crore. The amending Act also brought/ introduced several new provisions relating to offences such as identity theft, receiving stolen computer resource/ device, cheating, violation of privacy, cyber terrorism, pornography (Section 66A-F & 67A-C). Intermediaries are under obligation to protect the data/information and penalty has been prescribed for disclosure of information of information in breach of lawful contract (Section 72A).

Post-amendments, India for the first time got statutory provisions dealing with data protection. The Ministry of Communications and Information Technology vide Notification No. GSR 313 (E) dated 11th April 2011 made the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the said rules). The said rules define personal sensitive data or information besides laying down reasonable security practices and requiring every body corporate receiving or delaing with information to provide a privacy policy. Disclosure related restrictions have also been placed under these rules.

A press note dated 24th August 2011 clarified that the said rules are applicable to the body corporate or any person located within India. The press note further provides that any body corporate providing services relating to collection or handling of sensitive personal data or information under contractual obligation with any other legal entity located within India or outside is not subject to requirements of Rules 5 & 6 as mentioned hereinabove. A body corporate providing services to the provider of information under a contractual obligation directly with them however has to comply with Rules 5 & 6. The said press note also clarifies that privacy policy mentioned in Rule 4 relates to the body corporate and is not with respect to any particular obligation under the contract. The press note at the end provides that the consent mentioned in Rule 5 includes consent given by any mode of electronic communication.

Impact on industry & compliances required

In view of the above provisions, the BPO companies in India have been enjoined to protect the sensitive personal data or information as available with and dealt by them and in case of any failure on their part which may cause wrongful loss or wrongful gain to any person, they shall be liable to pay damages by way of compensation to the person affected. The said rules of 2011 prescribe that a BPO company located in India shall have to comply with the provisions of the same and provide a privacy policy for handling sensitive personal data or

information having the requisite details and such policy has to be published on the website of such BPO companies. If the data is being handled, collected, processed by any other person on behalf of the company, in such case, the policy may be displayed either on the website of such other person or of the company and the same would be sufficient.

In case the BPO is an independent entity and is providing services relating to collection, storage, dealing or handling of sensitive personal information or data under a contractual obligation with any other legal entity or company, then consent from provider of information is not required while collecting the information or while disclosing the same. In other words, as stated above, such a BPO Company shall not be subject to the requirements of Rules 5 & 6 of the said rules of 2011. However, in case of any back office of a company providing services to the provider of information under a direct contract, Rules 5 & 6 of the said rules shall be applicable and the said company shall be liable to obtain the consent even when the provider of information is outside India. Thus a company dealing directly with the provider of information shall have to seek written consent from the provider while collecting the information and inform the said provider about the purpose for which such is being collected. The company shall also have to designate a grievance officer to address the grievances of the provider of information. Such a company shall also require prior permission of the provider before disclosing the information to a third party except in cases when such disclosure has expressly been agreed to in the contract between the company and the provider or where the disclosure is necessary for compliance of a legal obligation or where the government agencies request such information .

The outsourcing companies have been barred from transferring data and sensitive information to any other body which does not have the same level of data protection as is present in India. The outsourcing companies have also been enjoined to comply with the reasonable security practices and procedures such as international standard IS/ISO/IEC 27001 on “Information Technology - Security Techniques - Information Security Management System - requirements” or any other best practices approved by the Central Government.

It may be added herein that the companies operating in India shall have to carry out regular audits to ensure compliance with the rules as any violation of the same would entail an action under the Information Technology Act, 2000 as amended.

Areas of concern

The Information Technology Act, 2000, as amended, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the press note dated 24th August 2011 read together, provide the legal framework for data protection in India. However, there are certain concerns that the above statutory provisions have failed to address in an effective manner.

- The first concern is that the rules do not require any consent to be taken from the person to whom the information relates to and only the consent of the "provider" of information has been deemed sufficient. This may lead to misuse of information when the provider and, the person to whom the information relates to, are different. In such a case, even if the company having information has taken consent of the provider, the person affected may sue the said company for compensation under Section 43A of the IT Act.
- The unfettered access that the government agencies may have to sensitive information is another cause of concern as it would amount to an infringement of the right to privacy of an individual. It may be noted that the rules do not mandate the government agencies to obtain a warrant in order to access sensitive information but a written request alone has been provided for. Further, it is not clear as to whether the said rule applies to the government agencies constituted and operating under the Indian laws or whether the same also applies to government agencies operating under other jurisdictions.
- The bar on transfer of information to other countries which do not have the same level of data protection measures may also hamper the outsourcing industry in India. Such bar would mean that the outsourcing companies cannot send the data to their employers, employees or other offices located in different jurisdictions which do not have the same level of data protection and the same may lead to loss of business opportunities.
- The adjudication procedure provided under Section 46 of the Act lays down that claims for compensation upto Rs. 5 crore shall be dealt by the adjudication officer and claims for more than Rs. 5 crore would be decided by competent civil courts. However, the civil courts in India may not be equipped to handle such claims due to poor infrastructure, lengthy dockets, huge pendency of cases etc.

Conclusion

The Government of India had introduced the Personal Data Protection Bill, 2006 in the Rajya Sabha on 8th December, 2006 with a view to provide a dedicated statute for protection of personal data and information of an individual collected for a particular purpose by one organization and, to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent[1]. However, the bill was allowed to lapse and instead, the Information Technology Act, 2000 was amended to provide certain measures for data protection in India which may allay the fears of misuse of data / information being dealt with by the outsourcing industry or the IT Sector or in e-commerce. However, with the ever changing technology and increase in the volume of data being processed, the need for a dedicated statute for data protection may be felt again after some time and the Government of the day may be compelled to enact the same.

(The author is a Consultant, Corporate Division, Lakshmikumaran & Sridharan)

[1] http://164.100.24.219/BillsTexts/RSBillTexts/asintroduced/XCI_2006.pdf (13.10.2011)