

DATA PROTECTION IN INDIA

Introduction

India's business, data and knowledge process outsourcing industries have been growing significantly in the last few years. However, various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. Unlike the US or the European Union, India does not have a data protection law.

In the absence of specific legislation, data protection in India is achieved through the enforcement of privacy and property rights. Privacy rights are enforced under the Indian Constitution ("Constitution") and the Information Technology Act, 2000, whereas the Indian Contract Act, 1872, the Copyright Act, 1957, and the Indian Penal Code, 1860, protect property rights.

Data Protection and Privacy Rights

An individual's right to privacy has evolved out of Article 21 of the Constitution and other constitutional provisions protecting fundamental rights. Article 21 of the Constitution provides that no person shall be deprived of life or personal liberty except according to the procedure established by law. The Supreme Court of India has held in a number of cases that the right to privacy is implicit in the right to life and personal liberty guaranteed to Indian citizens. However, constitutional rights can normally be claimed only against the State or State-owned enterprises and not against private individuals or establishments.

The Information Technology Act, 2000 ("IT Act") penalizes "cyber contraventions" (section 43(a) to (h)) and "cyber offences" (sections 65-74). The former category includes gaining unauthorized access and downloading or extracting data stored in computer systems or networks. Such actions may result in civil prosecution. The latter category covers "serious" offences like tampering with computer source code, hacking with an intent to cause damage, and breach of confidentiality and privacy, all of which attract criminal prosecution. The IT Act also prescribes penalties for hacking, which is tampering with a computer's source code and any breach of confidentiality and privacy obligations by a person having powers under the IT Act.

Under the IT Act, a network service provider or an intermediary is liable for any known misuse of third party information or data or for not exercising due diligence to prevent the offence. An “intermediary” is defined as anybody who receives, stores or transmits a particular electronic message on behalf of another person, or who provides any service with respect to that message. Therefore, an Indian Business Process Outsourcing (“BPO”) company may be liable as a “network service provider” because it acts as a service provider and receives and transmits information or data. The IT Act covers offences and contraventions committed outside India as well, irrespective of the offender’s nationality, as long as the computer system or network is located in India.

Confidentiality obligations are limited to officers or persons having powers under the Act and do not extend to private persons. Further, the officer is not liable to compensate the person damaged by the disclosure. Moreover, most of the penalties are in the range of Rs.200,000 to Rs.500,000, which are very insignificant amounts when compared to the gains that a person may make from the crime.

Data Protection and Property Rights

Article 300A of the Constitution ensures the right not to be deprived of property except by authority of the law. However, this right can be claimed only against the State and not against private individuals or employees. Further, the data in question has to be regarded as property.

The Copyright Act, 1957 (“Copyright Act”) protects Intellectual Property rights in literary, dramatic, musical, artistic and cinematographic works. The term “literary work” includes computer databases as well. Therefore, copying a computer database, or copying and distributing a database amounts to infringement of copyright for which civil and criminal remedies can be initiated. However, it is difficult to differentiate between *data* protection and *database* protection under the Copyright Act. Data protection is aimed at protecting the informational privacy of individuals, while database protection has an entirely different function, namely, to protect of the creativity and investment put into the compilation, verification and presentation of databases.

The Indian Penal Code, 1860 (“IPC”) can be used as an effective means to prevent data theft. Offences such as misappropriation of property, theft, or criminal breach of trust attract imprisonment and fine under the IPC. Although the offences of

theft and misappropriation under the IPC only apply to movable property, it has been defined to include corporeal property of “every description,” except land and things permanently attached to the earth. Therefore, computer databases can be protected under the IPC, as they are movable by their very nature, and under the Copyright Act because they are a form of IP.

Further, business entities seek data protection under contract law and common law, by incorporating confidentiality and data protection clauses in contracts.

In the absence of any specific law, BPOs have implemented self-regulatory processes such as the BS 7799 and ISO 17799 standards to standardize information security management and restrict the quantity of data that can be made available to their employees.

Indian BPO outfits are also trying to adhere to US and European regulations. Most Tier I BPO companies have certifications that comply with the Sarbanes Oxley Act, the Safe Harbor Act, the Gramm Leach Bliley Act for financial services, the Fair Debt Collection Practices Act for banking and the Healthcare Insurance Portability and Accountability Act for healthcare.

Proposed Legislative Measures

The Indian government has proposed several amendments to the IT Act, which are likely to be implemented soon. The proposed amendments widen the liability for breach of data protection and negligence in handling sensitive personal information. Additionally, the Government of India, with the help of the Department of Information Technology, is currently working on a holistic law on data protection based on the European Union directive. Further, the government plans to create a “Common Criterion Lab,” backed by the Information Security Technical Development Council, where intensive research in cryptography and product security can be undertaken.

Conclusion

The need for a law on data protection is paramount if India is to sustain investor confidence, especially among foreign entities that send large amounts of data to India for back-office operations. Data protection is essential for outsourcing arrangements that entrust an Indian company with a foreign company’s confidential data or trade secrets, and/or customers’ confidential and personal data.

MAJMUDAR & Co.

INTERNATIONAL LAWYERS

The proposed legislation for data protection will ensure adequate safeguards, and also appoint a regulator to monitor the collected data and its usage.