Overview of Data Protection Laws in India

Often confused with trade secrets and confidentiality, privacy refers to the use and disclosure of personal information and is only applicable to information specific to individuals. Since personal information is a manifestation of an individual personality, the Indian courts including the Supreme Court of India, have recognised that the right to privacy it as an integral part of the right to life and personal liberty[1], which is a fundamental right guaranteed to every individual under the Constitution of India. As such, the right to privacy has been given paramount importance by the Indian judiciary and can only be fettered with for compelling reasons such as, security of the state and public interest.

Legal Framework:

Presently, there is no specific legislation with dealing with privacy and data protection. The protection of privacy and data can be derived from various laws pertaining to information technology, intellectual property, crimes and contractual relations.

a. *Information Technology Act, 2000(**"IT Act"**)*

The IT Act provides for safeguard against certain of breaches in relation to data from computer systems. The said Act contains provisions to prevent the unauthorized use of computers, computer systems and data stored therein.

The section creates personal liability for illegal or unauthorized use of computers, computer systems and data stored therein. However, the said section is silent on the liability of internet service providers or network service providers, as well as entities handling data. As a result, the entities responsible for safe distribution and processing of data like the vendors and outsourcing service providers are out of the purview of this section.

The liability of the entities is further diluted in Section 79 by providing the criteria of "knowledge" and "best efforts" before determining the quantum of penalties. This means that the network service provider or an outsourcing service provider would not be liable for the breach of any third party data made available by him if he proves that the offence or contravention was committed without his knowledge, or that he had exercised all due diligence to prevent the commission of such offence or contravention. It may be noted that if there is any alleged violation of the IT Act by a company, its key employees (managers and directors) are made personally liable for intentional or negligent act resulting in the violation of the IT Act.

---

[1] *Kharak Singh Vs. State of U.P (AIR 1963 SC 1295; Govind Vs. State of M.P. (AIR 1975 SC 1375; R. Rajagopal Vs. State of Tamil Nadu ([1994] 6 SCC 632); People's Union of Civil Liberties (PUCL) Vs. Union of India (AIR 1997 SC 568); Distt. Registrar and Collector, Hyderabad Vs. Canara Bank (AIR 2005 SC 186)*

With regard to damages available in the event of a breach of data privacy under the said Act, the maximum penalty for illegal and unauthorized use of computer data is approximately $222,000/-. The law makes no differentiation based on the 'intentionality' of the unauthorized breach, and no criminal penalties are associated with the breach. Section 65 offers protection against intentional or knowing destruction, alteration, or concealment of computer source code while Section 66 makes alteration or deletion or destruction of any information residing in a computer an offence. Both sections 65 and 66 are punishable with criminal penalties including imprisonment up to 3 years or a monetary penalty of up to $440,000/-.

b. *Indian Penal Code*

The Indian Criminal law does not specifically address breaches of data privacy. Under the Indian Penal Code, liability for such breaches must be inferred from related crimes. For instance, Section 403 of the India Penal Code imposes criminal penalty for dishonest misappropriation or conversion of "movable property"[2] for one's own use.

c. *Intellectual Property Laws*

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offence. Section 63B of the Indian Copyright Act provides that any person who knowingly makes use on a computer of an infringing copy of computer program shall be punishable for a minimum period of six months and a maximum of three years in prison. Fines in the minimum amount of approximately $1,250, up to a maximum of approximately $5,000 may be levied for second or subsequent convictions- imprisonment for a minimum term of one year, with a maximum of three years, and fines between $2,500 and $5,000.

It is pertinent to mention here that the Indian courts recognise copyright in databases. It has been held that compilation of list of clients/customers developed by a person by devoting time, money, labour and skill amounts to "literary work" wherein the author has a copyright under the Copyright Act. As such if any infringement occurs with respect to data bases, the outsourcing parent entity may have recourse under the Copyright Act also.

d. *Credit Information Companies Regulation Act, 2005("CICRA")*

As per the CICRA, the credit information pertaining to individuals in India have to be collected as per privacy norms enunciated in the CICRA regulation. Entities collecting the data and maintaining the same have been made liable for any possible leak or alteration of this data. Based on Fair Credit Reporting Act and Graham Leach Bliley Act, the CICRA has created a strict framework for information pertaining to

[2] Movable property has been defined as property which is not attached to anything and is not a land.

credit and finances of the individuals and companies in India. The Regulations under CICRA which provide for strict data privacy principles have recently been notified by the Reserve Bank of India.

Industry Initiative:

In India, the efforts at complying with the demands of adhering to privacy laws have originated mainly from the private sector rather than the Government. In the absence of a specific legislation, the Indian software and outsourcing industry has been taking initiatives on its own that would provide comfort to the foreign clients and vendors.

The National Association of Service & Software Companies ("**NASSCOM**") is India's national information technology trade group and has been the driving force behind many private sector efforts to improve data security. For example, NASSCOM has created a National Skills Registry which is a centralized database of employees of the IT services and BPO companies. This database is for verification (with independent background checks) of the human resources within the industry. Further, a self regulatory organisation has been launched which will establish, monitor and enforce privacy and data protection standards for India's business process outsourcing ("**BPO**") industry. The organisation has already completed its initial round of funding and the final rollout phase including industry membership is underway.

Additionally, many BPO service providers in India have engaged in voluntary self-regulation and adopted stringent security measures to reduce the risks of misuse of non-public personal data. To reduce the risks of misuse of non-public personal data, the BPO companies in India have adopted one or more of the following stringent security measures:

- Posting of armed guards outside office premises.
- Restricting entry by requiring microchip-embedded swipe cards.
- Prohibiting bags and briefcases in the work area.
- Making provisions that computers in workstations have no printers or devices for removable storage.
- Banning or restricting agents or visitors from carrying mobile phones to the production floor.
- Forbidding phone calls to and from either family or friends in employee workstations.
- Disallowing image capturing devices like cell phones, scanners or photocopiers.
- Restricting or prohibiting internet and e-mail access at workstations and inside most BPO companies.
- Encryption of key information, such as passwords and, thus, s unseen by employees.
- Monitoring employees via closed-circuit television.

The aforesaid protections to tighten security are an attempt by the Indian industry to ease customer concerns over theft of private information.

Offshoring Data and Contractual Obligations:

India, only being an off-shoring destination, the process of data collection, seeking consent of the customers/employees regarding the data, etc. is carried out in India. As such, safe harbor principles and AICPA principles may not apply on the Indian leg of the operations insomuch so that the data collection is not being done by the Indian entities.

While entering into contracts, the off-shoring vendors imbibe terms and specific conditions in their contracts for data protection in line with the Graham-Leach Bliley Act, Health Insurance Portability and Accountability Act[3], Fair and Accurate Credit Transactions Act, etc. Typically, these vendor agreements stipulate how the information can be disclosed and provide for implementation of administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the data provided to the vendors.

Enforcement:

With respect to the personal and financial data being misappropriated by the employees or any other persons while the data is in possession of the Indian vendors, Indian legislation recognizes copyright in database[4] and as such, the foreign entity may take legal action against the infringer. Since the Supreme Court of India recognises privacy under right to life, the person whose personal data has been leaked may also take legal recourse against the alleged culprit.

Conclusion:

The lack of a comprehensive legislation pertaining to privacy and data protection has been a matter of concern. This concern has been particularly expressed by foreign companies that are doing business in India and are transmitting confidential data into the country.

Even though the data protection laws are not specifically laid down in any statute as yet, the Indian industry as well as the have begun the process of sensitising the Government and the masses regarding the importance of privacy. Further, with regulators like the Reserve Bank of India providing for strict privacy norms in certain areas, it seems that India is taking a huge step towards privacy norms. It is being felt by all concerned that a dedicated data protection law would give further impetus to not only the outsourcing industry but to the Foreign Direct Investment Policy at large.

Manjula Chawla
Corporate Lawyer, India
manjulachawla@vsnl.com

[3] HIPAA requires that a "Covered Entity" have appropriate administrative, technical and physical safeguards in place to protect the privacy of protected health information. Covered Entities must contractually obligate business associates to protect health information through Business Associate Agreements.

[4] Recognised in Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber 61(1995)DLT6