Overview of Existing Data Protection Laws in India, and the Proposed Data Privacy Bill

15 November 2019 | by Sushmita Haldar

Tags: Halder & Associates India Financial and corporate

It won't be wrong to say that data is the new oil. Gone are the days when one kept information written in hard copy and secured by lock and key, with guards protecting 24x7. Now information is power, and we all want it at our fingertips.

Technology and cyber net have allowed us access to information from any corner of the earth, through smart phones, computers and countless other access methods. The problem is when you open the door to access information in the virtual world, many unwanted elements may also use the opportunity to steal and abuse your data.

Supreme Court of India: In 2018, the Supreme Court of India has held that the right to privacy is a fundamental right flowing from the right to life and personal liberty (**Puttaswamy v Union of India**). The sphere of privacy includes a right to protect one's identity.

This right recognizes the fact that all information about a person is fundamentally her own, and she is free to communicate or retain it for herself. This core of informational privacy, thus, is a right to autonomy and self-determination in respect of one's personal data.

Duty of Care: The common law principle of "duty of care" also imposes an obligation on individual accessing data, a certain duty of care. Duty of care is owed by one party to another where there is a reasonably foreseeability that an act or omission by one party may cause injury to another party. Extending this principle to the virtual world, given the foreseeable risk of a data breach, the entity (i) possessing, (ii) dealing or (iii) handling data, owes a duty of care to safeguard the data in its custody. If there is a breach resulting in injury and damage to the data owner, then the entity could be held liable.

Applicable Legislatures: In India, the primary legislation governing information security is the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**Data Protection Rules**").

The IT Act Imposes obligation on the entity that possesses, deals or handles any "Sensitive Personal Information" to "maintain reasonable security" to protect such information. Currently, the law only refers to maintaining security with respect to "Sensitive Personal Information". Sensitive Personal Information is defined very narrowly to mean information relating to password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information and details related to the above. The limited definition has raised many concerns, as it does not include information such as ethical and religious belief, sex life etc.

The Data Protection Rules further details out the obligation of an entity dealing with data. These include obligation to maintain privacy and disclosure policy, obtain consent from the provider of "sensitive personal data" for collecting and using the data, provide the data owner the right to review and correct the data or withdraw consent, obtain prior

permission before disclosure of data to any third party (except for Government agencies mandated under the law).

The IT Act penalizes a body corporate who fails to maintain reasonable security practices and procedures to pay damages by way of compensation to the data owner/person so affected. Further, under the IT Act, a person may be punished with imprisonment for a term of up to three years, or/and with a fine of up to five lakh rupees for disclosure of information in breach of lawful contract.

Although the IT Act is applicable to all body corporates, it is not applicable to the Government. Further, there has been delays in appointments of the adjudicatory mechanisms created under the IT Act. The existing law and the executive have failed to successfully implement the checks and balances provided in the law to ensure data security.

In view of the Supreme Court decision and also to keep aligned/step/abreast with the law across globe, especially the EU General Data Protection Regulation ("**EU GDPR**"), a draft Personal Data Protection Bill, 2018 ("**Privacy Bill**") has been submitted to the Government of India and is awaiting legislative approval.

EU GDPR: GDPR has been implemented to ensure that uniform data security law is applicable to all EU members. Further, GDPR has an extra-territorial jurisdiction and is applicable to an entity not located in the EU, if such entity is to (a) offer free or paid goods or services to EU residents, or (b) monitor the behavior of EU residents. However, such applicability requires active participation from the service provider, such as the use of a language or a currency generally used in EU States, possibility of ordering goods and services in that language, or the mentioning of customers or users who are in the EU. However, there is no clear guidance on how GDPR is to be implemented outside EU States. EU will likely use the principles of jurisdiction under international law to implement GDPR outside EU.

Data Privacy Bill: The Privacy Bill will regulate the processing of personal data by government and private entities incorporated in India and abroad, if they systematically deal with data owner within the territory of India. Thus granting extra-territorial jurisdiction to the domestic law. The new bill covers both sensitive personal data and personal data, and have expended the definitions. It imposes specific obligations with respect to both types of data. These include, among others, the right of the data owner to obtain a summary of their personal data, the right to seek correction of data, transfer data to any other entity and right to restrict disclosure of personal data where such information has served the purpose, or was made contrary to law.

Any breach of law could lead to a penalty, which may extend up to 15 crore rupees or 4% of the entity's total worldwide turnover of the preceding financial year, whichever is higher.

Way forward: In this age of internet, data privacy and data security have never been more important and more challenging than ever. To achieve this end, law and law enforcement agencies have an important role to play. However, before the law is enacted, the Government needs to put in place the relevant implementation mechanism to ensure that the law is not without teeth.

One of the major reasons identified for data breach is lack of awareness. Therefore, continuous training of individuals dealing with data will play an important role to ensure data security.

In addition, contract negotiation will also play an important role, especially as most of the services are often outsourced by entities. There is a need to not only conduct proper due diligence on the entities dealing with data, but also include protective contractual provisions such a specific notice provision and indemnity clause with respect to breach of data security.

By Sushmita Haldar, Counsel at Halder & Associates, Advocates, India.
sushmita.haldar@halderassociates.com; www.halderassociates.com

Related articles

- Offshore Wind Power in India: Where do we stand!!!
- India's policy on FDI in multi-brand retail trade
- India - 2013 Overview
- Clasis Law hires new Mumbai head from Juris Corp
- JSA opens Ahmedabad office in the New Year

© Euromoney Institutional Investor PLC 2019
Registered Office: 8 Bouverie Street, London EC4Y 8AX, United Kingdom