Data Privacy and Big Data

V. Rajendran
Chairman, Digital Security Association of India, Chennai. Email: rajcyberlaw@gmail.com

Introduction:

Big Data is being discussed in detail elsewhere in this issue from various angles. This article focuses on the security concerns in Big Data, especially in the emerging scenario of Big Data Analytics and the Data being stored in various places including what is interestingly called 'the cloud' ie across a network server, and studying such a scenario in the backdrop of the Personal Data Protection Act (expected to be passed in India in a month or two).

Data Security and the Legal position:

The Information Technology Act, 2000 was notified in India on 17th October 2000 and has been in vogue since then. Subsequently, it was amended by IT Amendment Act 2008 effective from 27 October 2009. One of the powerful sections of the 2008 Amendment Act was its Section 43-A which provided for data protection especially the legal responsibility of corporates while dealing with the personal and sensitive data of public. The section uses the words "body corporate", "reasonable security practices" and "sensitive and personal data", signifying that the critical data relating to individuals which are collected, saved and processed or used by companies should be handled with utmost care and that they would be liable for breach and contravention if they do not adopt reasonable information security practices for data protection. In short, this section is for the civil liability of those handling data.

The Act in other sections speaks about the criminal liability of data theft, crimes related to electronically publishing objectionable data over the internet and other related cyber crimes. Besides these criminal offences, the Act also has a provision for due diligence thereby, those intermediaries handling data if they take adequate care, and if still some data theft occurs, would be protected in case they take proper care subject to the exceptions and other guidelines stated therein. After the Amendment Act, 2008, IT Rules were framed in April 2011 which described the phrases in Section 43-A cited above. Though these rules cannot be taken to be a definition of sensitive personal information, these rules may be taken as a description of what constitutes such information, in an inclusive manner and hence are not exhaustive.

In this backdrop, we have to look at the landmark judgement in the Puttaswamy case [Justice K.S.Puttaswamy, (Retd) vs Union Of India, Writ Petition (Civil) No.494 of 2012] delivered by the Supreme Court on 26 September, 2018, which holds that the right to privacy is a fundamental constitutional right. Having said that, it has become all the more interesting what exactly should come under the definition of 'privacy' which of course does include the related concepts 'personal data' or 'data privacy' as well. Though privacy has not been defined, it is still considered very significant in social and legal circles, especially after the proposed legislation on Personal Data Protection, being discussed in India, and expected to be passed in April 2020 as an Act.

The process of Personal Data Protection Act started with the submission of the draft bill by the Srikrishna Commission in July 2018 to the IT Ministry, soon after which it was also available in the public domain. Before the bill could be passed as an Act, the tenure of the Lok Sabha was over. Fortunately in the next Lok Sabha, the same Law Minister assumed charge and everyone hoped that the bill will see the light of day as an Act. As of now (19 Feb 2020), it has been referred to a Joint Panel of Lok Sabha and Rajya Sabha and public comments have been sought on the same.

The bill assumes significance in our study of security concerns in the big data environment especially with large volume of data being stored, processed, communicated and made available in various parts of the world in various networks and at various times too. The proposed Act speaks about the concepts of localisation, responsibility of stake holders in the context of data being processed outside India, the role and responsibility of the various parties associated with data processing and related activities like the data principal, data protection officers etc.

The proposed Act consisting of 98 sections divided into XIV chapters and two schedules seeks to provide for protection of personal data of individuals, create a framework for processing such personal data, and establishes a Data Protection Authority (DPA) for the purpose. Like Reserve Bank of India (the banking regulator) and TRAI (the telecom regulator), the DPA as proposed in the Act is going to be an all-India body presumably with technological, legal and other expert members on the Board and many regional or zonal offices, regulating and controlling the data protection arena. DPA will also be the judicial authority to handle cases of contraventions in the area of data protection and its breach, providing the required redress mechanism with enormous powers to levy penalty to those responsible for not protecting the data.

Personal Data means the data which is identifiable, a personal trait, characteristic or an attribute and Data Principal is the natural person to whom the personal data relates. Information such as financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, caste or tribe, religious or political belief are all included as sensitive personal data.

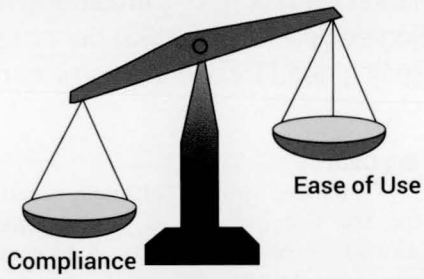
Data Principal, as per the Act, is vested with rights such as Right to confirmation and access the data and a Right to correction in the data if

anything false or objectionable is found and a right to seek erasure of the data through the regulator DPA. Besides, he also has a right to data portability and a right to be forgotten. This right ie the right to be forgotten is something new introduced in the Act. In the context of big data, one has to study carefully the impact of all these, which forms part of "big data" being handled or processed by firms and entities including government departments.

Big Data and bigger processing:

"Data Fiduciary" is defined as any person, including the State, a company, or any entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data. Therefore, it may be safely concluded that data fiduciary may have to deal with, most often, what is known as 'big data'. All the security related controls as enshrined in the Act, should be in place for any entity dealing with or processing big data ie a data fiduciary. There are some mandated obligations on the part of the fiduciaries to comply with. In the context of big data processing, cloud storage and remote processing, these provisions are quite significant, maybe somewhat difficult to comply with in today's ambiguous environment of techno-legal issues involved in cross-border and global processing of data.

The Act speaks about 'harm' to data and also 'significant harm'. In the area of big data analytics, when data moves from one server to another or is processed in various places, these concepts assume enormous significance, since the DPA is vested with powers to levy penalty in the event of contravention and the nature of harm caused to the data, in any technological process at the fiduciary level or elsewhere too. Probably, compliance of all the regulations of the Act may be even at the cost of ease of use, which is an issue, the stake holders may have to address.



Security concerns localised: To have a better control on the data whatever the nature of data and wherever the same is processed, the Act envisages localisation of data. Sensitive personal data may be processed outside India for specific purposes with the data principal's express consent but are to be stored only in India. Data which are to be notified by the government as Critical personal data are to be processed only in India. Besides, data audit has been mandated. To address the security concerns of data principals and to give them a comfort feeling that the rules would be strictly complied with by the stake holders, the DPA has been vested with powers too to levy a penalty of maximum 4% of global turnover of the corporates (or other entities) in the case of any breach and contravention. The localisation rules may evoke much criticisms too, since most of the big data and cloud storage now move across in a global network, across nations with the data principals not even knowing where his/her data moves and where and how it is processed and what his redress remedies are, in the event of any data loss.

To provide an ease of use, for big data users with larger volumes of data involving huge technological process, the Bill provides for a Consent Manager. A consent manager is a third party expected to possess a reasonable amount of techno-legal know-how and will express the consent or otherwise on behalf of the data principal to the DPA or a Data Processing Officer, who will represent the fiduciary to the DPA. Perhaps, tech-savvy chartered accountants and lawyers and other big data analysts have good opportunities waiting for them from corporates!

Of course, there are quite a few exceptions and exemptions inasmuch as the Bill provides for processing without a consent in the event of emergency, national sovereignty and other such exigencies. ■

About the Author

V. Rajendran is an M.A. B.L. M.Com with CAIIB. A certified cyber forensic examiner from IDRBT, Hyderabad and a CeISB from Indian Institute of Banking and Finance, CISP from STQC, Govt of India, a Diploma holder in IT Law and a lead auditor in ISMS (ISO 27001).

Worked for over three decades in Indian Overseas Bank, including 15 years in I.T. Department, in domains like Core Banking Solution, Info System Security, IS Audit etc. Was instrumental in drafting the Information System Security Policy and other related policies of the bank. After quitting the bank in 2008, started practice as an advocate mainly handling cyber crime and banking security related cases and as a consultant on banking law, practice and technology. Has contributed articles in various academic and professional journals like Indian Banker, CSI Communications etc and appeared in electronic and print media on subjects like ATM frauds, cyber crimes and cyber laws. Has authored the book on "IT Security" for bankers and "Cyber Crimes and Fraud Management in Banks" both published by Indian Institute of Banking and Finance, Mumbai. .

A Guest Faculty in the Indian Institute of Banking and Finance and an invited speaker on cyber crimes, banking laws etc in various Universities and academic institutions including the Police Training Academy, industry bodies like CII, FICCI etc and training colleges of various public sector and private sector banks. Past President of Cyber Society of India and currently the Chairman of Digital Security Association of India.