BIG DATA – EVOLUTION OF INDIAN DATA PROTECTION LAWS

By Nishith Desai[1]

"The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data"[2]. Indeed India's aspirations to be a knowledge economy coupled with the very real issues faced in cases of data being transferred to and processed in India particularly by the services sector has made it necessary for India to craft a clearly thought out policy in respect of data protection.

Historically, the concept of data protection and privacy were not addressed specifically in any Indian legislation. In the absence of a specific legislation, the Supreme Court of India has in a number of decisions recognized the "right to privacy" as a subset of the larger "right to life and personal liberty" under Article 21 of the Constitution of India[3]. However a right under the Constitution can be exercised only against any government action. Non-state initiated violations of privacy may be dealt with under principles of torts such as defamation, trespass and breach of confidence, as applicable.

The Information Technology Act, 2000 ("**IT Act**") is the only legislation which has attempted to address the issue of data protection. There are two basic elements of data protection under the IT Act.

- The first concerns negligence in maintaining reasonable security practices and procedures to safeguard specific items of information classified as sensitive personal data or information which can identify a natural person ("**SPDI**")[4] where such negligence results in wrongful loss or wrongful gain to any person. The Government has in 2011 introduced certain rules ("**India Data Protection Rules**") under the IT Act which, read along with Section 43A, which set out the

[1] Nishith Desai is Nishith Desai is the founder of Nishith Desai Associates, a leading international law firm with offices in India, Singapore and Palo Alto (US).

[2] Preface to *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[3] Kharak Singh v State of UP, AIR 1963 SC 1295; People's Union of Civil Liberties v. the Union of India, (1997) 1 SCC 318

[4] SPDI is defined as sensitive personal data or information which can identify a natural person consisting of (i) passwords, (ii) financial information such as Bank Account or credit card or debit card or other payment instrument details, (iii) physical, physiological and mental health conditions, (iv) sexual orientation, (v) medical records and history, (vi) biometric information

compliances which need to be observed by an entity which collects or stores or otherwise deals with SPDI.

- The second element is in relation to intentional disclosure of any personal information of any person that is capable of identifying such person, including any SPDI ("**Personal Information**") which has been collected under a contractual relationship.

On analysis of various other laws and guidelines dealing with data protection, it appears that there is a commonality of purpose for most laws and guidelines dealing with data protection

The Organisation for Economic Co-operation and Development's ("**OECD**") Guidelines OnThe Protection Of Privacy And The Transborder Flow Of Personal Data came out in 1980 ("**OECD Privacy Guidelines**"). The OECD Guidelines set out eight principles which act as minimum guidelines to be applied by OECD member countries in relation to "*personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties*[5]*"* **[emphasis supplied].** Some of the pertinent guidelines set out in the OECD Privacy Guidelines are

- **Collection Limitation Principle** which states that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
- **Data Quality Principle** which states that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Use Limitation Principle** which states that personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: (a) with the consent of the data subject; or (b) by the authority of law.

The Indian Data Protection Rules do seem to imbibe the spirit of the OECD Guidelines in a number of ways. For instance, the Indian Data Protection Rules have specific provisions which mandate that the collection of SPDI should be for specific purpose and that the SPDI should only be used for such purpose.

[5] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

In the European Union, Directive 1995/46/EC [6] ("**EU Directive**") provides for guidelines to be implemented by the European states for the processing of personal data and free movement of personal data within the European Union. The EU Directive does contain provisions which mandate obtaining of consent from the data subjects which is a similar feature under the India Data Protection Rules. One important aspect of the EU Directive is that it provides for a mechanism of notification to a Supervisory Authority appointed by each of the EU member states for the processing of personal data – the India Data Protection Rules do not provide for such an office which will supervise activities relating to data processing. In effect the India Data Protection Rules prescribe more self compliance – though liability does get attracted in some cases as we have discussed in the preceding paragraphs. Another interesting feature of the EU Directive is the creation of **special categories of data** which include highly sensitive data (such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs) which are subject to increased checks and balances for processing. Here it is interesting to note that SPDI which is dealt with in the Indian Data Protection Rules form a limited exhaustive list and do not cover a wide range of data which may be perceived to be sensitive.

To conclude, since the entire ecosystem in terms of global data sharing is constantly evolving, the recently introduced Indian Data Protection Rules would be tested in light of variant business models and newer age technologies. Also, with the passage of time, it would be interesting to observe the implementation of these rules along with the development of judicial precedents on the same.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML