Data Loss and Cyber Laws

Introduction: Data is increasingly becoming the most sought after asset these days. It has become the nerve centre in any industry and technology and data are together the driving force at the backbone of any organisation in today's networked world. Such is the technology penetration in every walk of life today, that if you want to be the Number One, you don't have to be the leader in the domain but have to the top in technology, data integration and related information systems. The Number One cab operator does not own a single taxi, and so does the top autorickshaw operator not own a single autorickshaw. The top retailer does not store any grocery item and the top caterer does not cook a single food item! All these are the in the top slot not because of their strength in the domain but because of their strength in data movement across a network and precisely data integration based info systems.

Data keeps moving over a wide area of network sometimes across various nations too, gets stored in some place, processed elsewhere, and accessed from somewhere else by the user ultimately in his mobile or desktop. With such ubiquity, it is quite natural that protection of data and its security are real causes of concern, especially from a legal perspective. In India, we had been coping just a solitary legislation Information Technology Act, 2000 and its later revision called the IT Amendment Act 2008 to deal with the entire gamut of data theft, cyber crimes and all computer or network based offences.

The Amendment Act had a powerful section 43-A, which dealt with the civil liability for companies dealing with sensitive data of individuals and provided for judicial powers to levy hefty penalty for contravention and breach of the provisions (ie data theft or unauthroised access or transmission of data). In fact, the IT Act or the Amendment Act did not define cyber crimes, nor did it describe the various cyber crimes. Other than the civil liability of data theft, the Acts dealt with the criminal offences of data theft, unauthorised access of data, transmission of obscene messages in a network, id theft and other such offences.

Personal Data and its Security: As per the section 43-A of the Amendment Act, penalty may be levied for breach and theft of "personal and sensitive data" of individuals and others at the hands of "body corporates" not following "reasonable security practices". Using the three phrases as cited here, the Act fixed the responsibility of firms (body

corporates) handling data. Subsequently, the rules relating to what constitute personal data were framed and notified by the Ministry of IT during April 2011, and bank data, card related data, health related information and sexual orientation related data were all included in it.

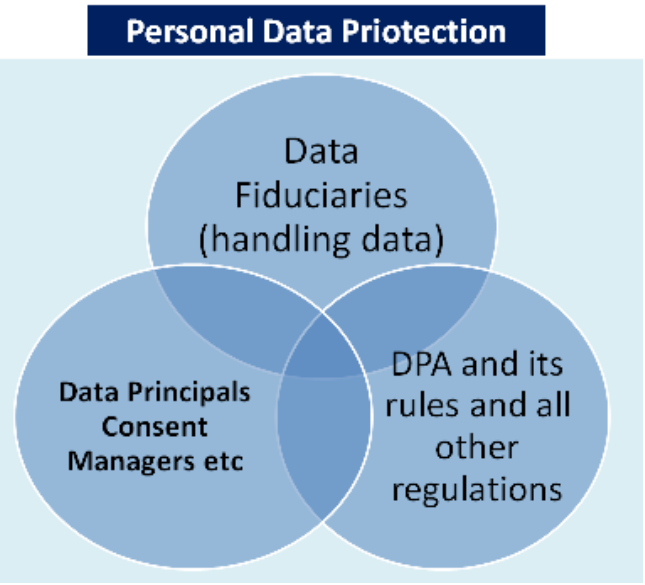
In this backdrop, in the famous Puttaswamy case, the Hon'ble Supreme Court declared in August 2017 that 'privacy is a fundamental right'. Other than the IT Acts cited above, there was no data protection law or any law regulating the data in a network or in internet has been in vogue in India, by whatever name. Need for a legislation to protect data and to ensure privacy of data of individuals has always been felt in India, more particularly after the apex court verdict cited above and an Act was being discussed for quite some time.

Justice Srikrishna Committee, also known as the Data Protection Committee submitted its report in July 2018 with a draft of an Act for Personal Data Protection. The same could not be passed as an Act in the previous Lok Sabha. It has now been placed in the Parliament, referred to an Expert Panel of MPs and is expected to be passed as an Act in a few weeks (maybe in April 2020). This Act is being widely discussed and debated now and data privacy is being looked at with its all implications on the corporate arena as well the ramifications to individuals.

Though privacy has not been defined in the Bill, related concepts like 'personal data', 'Sensitive Personal Data' have all been defined. Personal Data is a simpler term signifying an identifiable personal trait, characteristic or an attribute whereas 'Sensitive Personal Data' refers to information such as financial data, health data, official identifier, biometric data, genetic data, details about sex life etc. More responsibility has been fixed for the stake holders in the case of Sensitive Personal Data.

'Data Principals' means the natural persons to whom the personal data relates. "Data fiduciary" means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data. A Data Principal is vested with rights such as i) Right to confirmation and access the data, ii) a Right to correction in the data if the same is incorrectly saved or displayed or processed, iii) a Right for data portability and iv) a Right to be forgotten. The last one here viz the Right to be forgotten is something new in the Indian legal parlance (though the General Data Protection Regulations of the UK effective from

May 2018 and legislations in quite a few other nations have such provisions).



The proposed Act consisting of 98 sections, seeks to create a framework for processing such personal data, and establishes a Data Protection Authority (DPA) for the purpose. DPA is will be a regulator like the banking regulator Reserve Bank of India and the telecom regulator TRAI and is expected to be a separate entity (organisation) with branches pan India, with technology experts, legal pundits and data security professionals on the management. DPA will also be vested with judicial powers to handle cases of contraventions in the area of data protection, to levy penalty and it is proposed that penalty can be as high as 4% of the global turnover.

"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. Data fiduciaries are expected to comply with the strict controls envisioned in the proposed Act, which is a significant step especially now that, data gets generated in one part of the globe, is processed in another country, gets communicated and displayed somewhere else. It would be interesting to note the ramificaitons of these responsibilities and how the industry especially the data integrators, cloud storage firms and all intermediaries are going to comply with the regulations applicable for data fiduciaries.

There are restrictions on processing of data abroad ie the concept of localisation is being intrdouced. 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. Though RBI has already given isntructions to banks on data localisation to comply with, now the proposed PDP Act is expected to have a look at sectoral controls, thereby controlling the various industries dealing with data like telecom, banking, software, BPOs health, insurance etc. Data Protection Impact Assessment is enforced for those fiduciaries

notified as significant data fiduciaries, based on criteria like volume of data processed, turnover of fiduciary etc. Privacy by design is another new concept in the proposed legislation, meaning that the information system security policy of fiduciaries should be transparent, be available at the website and customised for the particular data principals.

The concept of "anonymisation" is another new area in the proposed Act. It may be defined as an irreversible process of transforming or converting personal data to a form in which a data principal (ie the person whom the data relates to) cannot be identified, as per the standards of irreversibility that are to be specified by the DPA. Standards and norms relating to anonymisation are all yet to be finalized and perhaps in the days to come, technology gurus will discuss and debate over this issue. Similarly, to save the data principals from the technicalities of data and maybe the technological ambiguities or glitches, a consent manager is being envisaged, who will represent the data principal and is supposed to have a reasonable knowledge of technology and law associated with data protection. Perhpaps in the days to come, tech-savvy professionals and maybe chartered accountants and other techno-legal experts will have a good opportunity in getting hired by big firms dealing with enormous data with such appointment expected to facilitate better compliance. Ease of use and compliance with the proposed rules are to be balanced properly to ensure a smoother e-governance and data protection in the industry and to gurad against what the proposed Act calls ‘significant harm’ to data.

Of course, there are ample provisions in the proposed Act to take care of exigencies like law and order situations, national sovereignty, criminal investigation process, judicial orders etc when disclosure of the data will have precedence over security and protection of data. In sum, let us wait for the Act to be passed, to be notified, for the DPA to be set up and all the other rules to be framed gradually. Until such time, maybe we have to continue with our path of ‘unsecured or unprotected data’.