DATA PROTECTION LEGAL FRAMEWORK: NEED OF HOUR

-by SHREYA SAXENA

B.A. LL. B, 4th YEAR, LLOYD LAW COLLEGE

Data is the life-blood of any business looking to strive and excel today. All organizations from the bakery down the street to banks of the central of the city's financial district are somewhere in the journey to unlocking the value of that data. Collectively there is a massive amount of data constantly being used, stored and processed.

Data is after-all means to an end. A business or an enterprise keep a track of the data of their customers and evaluate their habits according to the likeness and cater it from time to time which as a result helps in satisfaction of the customers. Moreover, it adds value to a business enterprise and builds up the market.

Then there is a flip side of data which implies the fact that data can be helpful in profiling a person. A state can profile a person on the basis of their thinking, viz. political thinking, religious practices or their other habits Thus, in a democratic country it is always essential that data is left to the control of the person whose data it is, namely the 'data principle'.[1] As a matter of fact, the value of data is paramount and no entity or an individual should be allowed to get hold of one's data unless he or she is ready to part with it, besides in case of exceptional circumstances. In current juncture, data and the information assets which people have, the data security and data privacy play a paramount role and thus justifies the fact that our data is in our custody and no one has the right over it.

In the contemporary era, data is first a business strategy, more like itself a business

[1] Section 3(14) of PDPB, 2019 defines "**Data principal**" as *the natural person to whom the personal data referred to in subclause (28);* Section 3(27) of PDPB, 2019 defines "**Person**" as- *(*i) an individual, (ii) a Hindu undivided family, (iii) a company, 5 (iv) a firm, (v) an association of persons or a body of individuals, whether incorporated or not, (vi) the State, and (vii) every artificial judicial person.

today. The ongoing situations have elucidated that how institutions have adopted themselves, become much more virtual and had gone after all the critical data services in serving the nation. This is a true instance of how transformation and digital transformation has laid out in today's world.

Similarly, corporations today have expanded their role beyond the boundary. They have larger ecosystem governing employee's data. Above all, it is all about sharing the information in a secure and an immensely faster way so that the access is available from various data sources by which one can have a quick access to the input.

However, security plays a greater role with increasing number of threats we are witnessing today across the board. The role of data and the necessary laws around it, are now much more paramount and one has to align with it , both for their own and their customer's data safety and hence, it is important that we look at the holistic view of data that how it is going to derive information, various business models and different new ways to access. We have to be vigilant as of how we are exposing out one's data to such mode of access because any amount of compromise here would be highly drastic and can have far-reaching consequences. As a result, we have to balance while connecting people and ensuring risk alignment at the same time. Data is distributed across the edge, the core and the cloud for which we need a strong data protection law, the law that will handle back the data to where it belongs.

Additionally, there exist a 'Third Party Doctrine' which is derived from the legal framework of the United States.[2] The doctrine comprises of two parts: (1) once individuals voluntarily expose matters to third party/public (2) then they assume the risk of unauthorized disclosure. 'Assumption of risk' is a consequence of losing privacy and not the rationale behind the doctrine. The voluntariness is the antecedent. However, to suit the digital aeon, possible modifications to the doctrine were discussed in the recent case law viz. *Thimothy Ivory Carpenter v. USA, 2018.*[3]

[2] U.S. Const. amend. IV.
[3] 585 U.S. 138 (2018), *available at* https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf.

However, in India, in the landmark case of *Justice K.S. Puttaswamy v. UOI*, the Court held, "Privacy recognizes the autonomy of the individual and the right of every person to make essential choices that affect the course of life, which may be infringed through an unauthorized use of such information".[4] It located privacy in dignity by acknowledging the importance of self-determination and personality development.

Lastly, *Puttaswamy* dealt the final blow to the doctrine by recognizing 'purpose limitation', i.e. the reasonable expectation that the information will be utilized only for the purpose for which it was obtained. Thus, it redefined the expectation as allied not to voluntariness but "to the purpose for which the information is obtained". Another is 'content limitation', i.e. only information necessary for the purpose would be collected through lawful and fair means.[5]

Yet, the problem with data storage is that the data will not leak unless there is a human intervention be it by the way of hacking or someone who is manually dealing with data leaks it. Therefore, all several security measures must be intended to ensure to the best that is available. Everyone today has seen Indian market as a big player. Now, when it comes to important analytics which are being done today as, measuring the data centers or the clouds, finally the delivery of these and the consumption of data is happening at the end points which are today in the control of the users. So if a user is generating data at the edge, moving the data across to the distributer code and then to the core or the larger data centers that are in the country, it is a collective responsibility of these organizations to ensure the processing and the storage of data is as per the laws. Some countries have already adopted the measure for instance, GDPR (General Data Protection Regulation) endorsed by European Parliament.

Data that is being generated from devices goes to the body called 'data fiduciary'[6]

[4] K. S. Puttaswamy and Anr. v. Union of India and Ors., AIR 2015 SC 3081, para. 113, 85.
[5] Quoted by Justice Dr D Y Chandrachud in the case of K. S. Puttaswamy and Anr. v. Union of India and Ors., AIR 2015 SC 3081, para. 66, 184.
[6] S.3(13) of Personal Data Protection Bill (PDPB), 2019 defines "Data Fiduciary" *as 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*.

which is generally responsible for the data and the bill itself lays down the obligations and certain transparency and accountability measures undertaken by data fiduciaries.[7] At the same time, the threat actors are also easing their play by attacking the most sensitive and impactful industries be it healthcare, retail, medical supplies, as in whole of the livelihood of people. These services are absolutely critical to be protected especially the data which is now being produced for instance under health-sector, the clinical laboratories which carries a lot of critical and sensitive data processing. Therein lies the people processed technology norms that has to be taken care of according to the present legal framework regarding data privacy. Moreover, the organisation or the concerned departments in the country should be able to bounce back their business, able to trace the threat and limit the damage.

Coming to the approach that government and the government bodies have adopted for ensuring data protection and recovery, the two departments have already shot the gun earlier. One being the Reserve Bank of India (RBI), which clearly stated even before the recent amendment i.e. PDPB came into picture that, all payments data needs to be stored in systems located in India. It further clarified that while there is no bar on overseas processing of strictly domestic transactions, the data shall be brought back to India within one business day or twenty-four hours of payment processing and be stored locally here. It also mentioned the inclusive content of 'data' that is to be mandatorily stored in India and further said that the data stored should include end-to-end transaction details and information pertaining to payment or settlement transactions.

The other entity that dealt with it was TRAI, i.e. Telecom Regulatory Authority of India, which emphasized on all the mobile data which is transacted or collected with the mobile companies to remain within the country. It further accentuates on ensuring end-to-end security that is essential for any mobile financial services (MFS) with powerful transaction management. MFSSP i.e., Mobile Financial Services Secure Platform secures all communication between the mobile front-end to the

[7] PDPB, 2019.

back-end financial processing and back office cluster. The Secure Mobile Financial Service Platform go far beyond standard telecom security safeguarding data using various factors sc.[8]:

- Strong two-factor authentication.
- Data classified and ciphered separately.
- Secure execution environment and non-repudiation assurance.
- Derived Unique Key Per Transaction (DUKPT) standard for additional protection.
- Secure OTP (One Time Password) generation and validation using the HSM.
- Anti-phishing mechanisms.

It is very difficult for the law to define what is the security measure. It can only impart us to keep our data secure, proportional to the technical knowledge which advances with time. Therefore, we have to keep pace with technological advancements making sure latest available technology is built in and around the data and its security depending upon the type of data being used. People sometimes follow the 'NIST' framework which actually goes to save and identify, protect, detect, respond and recover. Nowadays, lot of people are increasingly emphasizing on the recovery assets. It has all to do with what extent one can afford the SNA or to what extent it is impactful. Also, one must have the copy of the data moving to cloud which is equally important.

Furthermore, there is a tool rather an index that can measure the maturity of data protection strategies and access the relative preparedness of a business in a country, termed as the “Global Data Protection Index'. It is a report by a third party called 'Vanson Bourne' which did an independent research and classified several organizations based on the confidentiality, and further elaborated on cloud and multi-cloud data protection strategies.[9] The rate of incident with regard to data unavailability and company data loss which is an extreme situation, has gone up

[8] https://trai.gov.in/sites/default/files/10gemalto.pdf.
[9] Global Data Protection Index 2020 Snapshot.

since last year as exhibited by various studies.

India has yet not enacted a specific legislation on data protection. However, the Indian legislature did amend the Information Technology Act, 2000 ("IT Act") to include Section 43A and Section 72A, which accord a right to compensation for improper disclosure of personal information, whereby the IT Rules have incorporated Section 43A of the Act and provide for minimum standards on collection, disclosure and transfer of personal information, defined as "any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person." It further substantiates that all body corporates need to devise a 'privacy policy' for dealing with personal information (including sensitive personal data or information).

CONCLUSION

In this data protection arena today, more and more efforts are taken and there are chances that data will be subjected to strict norms from a processing viewpoint and one must continue to comply with the law and work accordingly. The Personal Data Protection Bill of 2019 (PDPB) although, supersedes Section 43A of IT Act, 2000, it is a comprehensive law and proposes to protect 'personal data' and 'sensitive personal data' as laid out in the bill.[10] It inter alia, prescribes the manner in which the personal data is to be collected, processed, used, disclosed, stored and transferred. However, these days data processor may also seek getting the data insured which is a new concept but can be certainly looked upon.

In the framework of data protection laws, as far as consumer's fundamental right of privacy is taken care of by an appropriate law, ergo, the rest will fall into place.

***

[10]S.3(28) and S.3(36) of PDPB,2019.