VOLUME 4 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DATA PROTECTION REGIME IN INDIAN LEGAL SYSTEM

- Palak Priyadarshini[1]

• Introduction

The Previous chapter has equipped the researcher with a very broad understanding ofthe different approaches adopted by the European Union, the United States and the United Kingdom towards protection of Personal Data. Before getting into the discussions about the optimality of a certain Data Protection Model in India, it would be necessary to have a thorough review of the existing data protection legislations in India. The sole objective of the discussions in this chapter is to strike gather the best possible understanding of the stateof Data Protection in India.

The world is becoming more and more intensely digitalized by each passing day and India is no exception to the phenomena. With billions of people all over the world communicating with each other through the transmission of information through digital mediums a huge volume of data is generated all over the world[2]. The new found digital mediums of communications including the social media intermediaries such as the WhatsApp, Facebook, Twitter and other platforms have an extensive outreach amongst a huge chunk of population. With the availability of cheaper internet and broader connectivity, the more than 53% of the Indian population has an online presence.

Further, the use of online payment applications such as the Paytm and Google pay have got an extensive presence in the Indian economy. The use of these apps by the citizens has added to the enormous amount of data that is involved in the digitals sphere. However, the progress in technology has also armed both the public and private sector entities to get access to the personal data of the individuals, store them and process them within a matter of moments.

[1] Student at Amity Law School, Amity University, Noida

[2]Mandavia, M., 2020. *India Has Second Highest Number Of Internet Users After China: Report*.[online] The Economic Times.

A surge in the internet users also indicates that a lot of personal and financial data is usually involved in these transactions. The immense popularity of these applications amongst the Indian users, make India a hotbed of digital transmissions. It must be noted that these mobile applications that offer various kinds of services to the uses such as online chatting, digital transactions, online shopping, cab service etc. do store and process a huge volume ofthe personal data of the individuals. The evolution of a digital economy with the Data atits centre-stage can be amply traced in the following excerpt:

Something as simple as hailing a taxi now involves the use of a mobile application which collects and uses various types of data, such as the user's financial information, her real-time location, and information concerning her previous trips. Data is fundamentallytransforming the way individuals do business, how they communicate, and how they make their decisions. Businesses are now building vast databases of consumer preferences and behaviour. Information can be compressed, sorted, manipulated, discovered and interpretedas never before, and can thus be more easilytrans formed into useful knowledge.

Along with the collection and processing of the personal data, the process more oftenthan not involves storage and transmission of the personal data. With the advancement of technology, the storage and processing of personal data has become extremely viable option economically and technically as well. These phenomena ensure that thedata aggregators not only collect bit also store the personal data of the individuals which can beused to make the individual profiles of the users, of course for a more efficient functioningof the applications. The creation of customized user profiles helps the service providers to reduce the transaction time and make the services moreefficient. The online aggregators and the e-commerce companies make use of the online history of the users to suggest the products that the users may be interested in buying[321]. To be precise, the use of data can have a great impact on the way things work in the digitalized world and every entity, whether be it the private sector or the public sector, does strive to get the maximum outputthrough the data of their users. Use of data for analyzing the locations of people living in aparticular area may be used to improved traffic conditions, the analysis of health data of the patients may help the researchers come up with a better diagnosis procedure, the analysis of the demography and economic condition of the individuals can be of great helpto the government in framing policies and targeted delivery of socially beneficial policies.The processing of data can also be of great help to the financial regulators in detecting fraudsand the law enforcement agencies prevent crimes. There has been an increasing trend among the law enforcement authorities to use

drone cameras and using more complex methods of surveillance with the help of the internet and sophisticated technologies of the personal data of the individuals possesses a great threat to the informational privacy at the same time. An increasingly prevalent use of the internet has thrown open a plethora concerns related to the possibility of data breaches. With government being the largest processor of personal data in India, it becomes extremely important to have a law in place that would regulate the entire affair of collection, storage and processing of the data and put in place necessary safeguards. However, the threat to the informational privacy in India, just like the entire world is not something that has just loomed up, it is just that the threat has become much more larger with the advent of digitalization.

- **The Information Technology Act, 2000**

The Indian Information Technology Act 2000 ("Act") was a based on the Model Lawon Electronic Commerce adopted by the United Nations Commission on International Trade Law the suggestion was that all States intending to enact a law for the impugned purpose, give favourable consideration to the said Model Law when they enact or revise their laws,in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. As noted earlier, the scheme of dataprotection laws in India was initially hinged at the affairs related to the off-shoring businesses and the information technology sector. It was the result of the void in the existing laws in India that there were several instances of data theft and amidst growing international pressure, India came up with the Information Technology Act, 2000 toregulate the flow of data in the country. Even to this date, the IT Act remains the most foundation of the several Indian laws aimed at securing a society conducive to the cause of data protection. The boost in the technological sector marked the beginning of a data drivenculture in India and it was through the problems outlined above are regulated primarily bythe IT Act. The Act has been amended several times till now in order to tackle the ever- evolving challenges posed to the security of data with the advancement of technology. This section shall deal with the existing provisions of the Act in order to analyze the existing framework for data protection in India.

The IT Act adopts a conventional e-commerce-oriented definition of the term "data" under its scheme. The emphasis on computer and other forms of memory storages implies the initial legislative intent behind the provision. It should also be noted that the restricted meaning of term data has undergone considerable changes in the wake of subsequent provisions

"(o) 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnet ic oroptical storage media, punched cards, punched tapes) or stored internally in the memory of the computer."

The scope of the IT Act appears to be confined to the e-commerce activities and the primefocus of the definition of data in the Indian law was to further the cause of internet governance in the information technology sector. This proposition may be appreciated fromthe fact that the concept of data protection was far away from the Indian conception of privacy and informational self determination. The fact that there is any law in existence in India can be attributed to the subsequent amendments that were brought in the IT Act. The two most notable pillars of the data protection scheme in the country are Section 43Aand Section 72A of the Act.

The scheme of data protection in India can be broadly classified under two categories, viz. the Cyber Contraventions and the Cyber offences. While, the Cyber Contraventions, are in the nature of civil wrongs the Cyber offences, as the name suggests are more severe in nature and attract penal consequences. The first post for an insight intothe provisions of a statutory law in India saw its dawn in the form of Section 43 A of the IT Act and the provision seeks to impose a liability upon the companies that fail to processthe data in a negligent manner without taking reasonable safeguards and security procedures.[338] Violations of the provisions of the section falls within the ambit of cyber contravention. The term contravention is notably very restricted in its extent and it includesall the unwarranted inference in the informational privacy of the individual through an unauthorized intrusion into the data stored in computer or computer network.

The bulwark of codified Indian data protection law lies in the Chapter IX of the IT Act. The Section 43 of the Information Technology Act, 2000 provides for the liability of the data controller in case there is a breach.

43A Compensation for failure to protect data. -Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns,controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person,such body corporate

shall be liable to pay damages by way of compensation to the person so affected. Explanation. - For the purposes of this section, -

- "body corporate" means any company and includes a firm, sole proprietorship orother association of individuals engaged in commercial or professional activities;
- "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force andin theabsence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;
- "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

As implicit from the text of the provision, the Section purports to impose penalties upon those body corporates dealing, possessing and handling the sensitive data and fail to maintain and implement reasonable security measures and as a result of which there is a wrongful gain or a wrongful loss to a person, the said body corporate shall be liable to pay damages to the affected person. The meaning of wrongful gain has to be construed in accordance with the definition in the Indian Penal Code.

As can be inferred from the bare reading of the section, the liabilities will arise out only against the body corporates, that is to say companies, corporations, proprietorships and the other sections of group of individuals. The exemption of the individuals from the fangs of the penal provision does suggest that the intention of the legislature behind enacting the said section was primarily to the body corporates dealing with processing of personal data. However, in the view of the author the scope and ambit of the provision is immensely limitedand the following are the pre conditions that must be satisfied in order to attract the penal provisions.

- The Data in possession must be of sensitive character
- The Computer resource processing the data must be owned and run by a body corporate.
- The body corporate must not be negligent in handling the data and there must be a lack of reasonable security standard.
- Most importantly, such negligence must have resulted in wrongful gain or wrongful loss.

Apart from the very restrictive provision that seeks to protect the breaches of informational privacy in the non-contractual relations, the Indian legislature in 2009, through an amendment introduced section 74 A of the Information Technology Actto protect the privacy under the contractual relations.

The IT (Amendment) Act, 2008 (ITAA 2008), introduced in the aftermath of the 26/11 Mumbai attacks has established a strong data protection regime in India. It addresses industry's concerns on data protection, and creates a more predictive legal environment for the growth of e-commerce that includes data protection and cyber crimes measures, among others. Sensitive personal information of consumers, held in digital environment, is required to be protected through reasonable security practices by the corporates. Additionally, ITAA 2008 made it obligatory for them to protect data under lawful contracts by providing for penalty for breach of confidentiality and privacy.

- **Information Technology (Reasonable Security Practices andProcedures and Sensitive Person Data or Information) Rules, 2011**

As implicit from the provisions of the Information Technology Act, 2000, the definition of the sensitive personal data was nowhere provided, leaving out a wide room for confusion and instances of misinterpretation. The section 43 A of the Act provides for the framing of new rules from time to time and in exercise of this power, the Ministry of Communications and Information Technology in 2011 came up with the "Information

technology (Reasonable Security Practices and Procedures and Sensitive Person Data or Information) Rules, 2011". It would be optimum for our analysis to have a glance at some of the relevant parts of the rule to have a holistic view ofthe existing data protection regime in India.

While the rules, do leave a major chunk of the definitions of the IT Act, 2000 unaltered, they do fill some of the major loopholes of the Act and thus seek to chalk out a workable piece of data protection legislation that is conducive to the protection of informational privacy of the citizens. One of the most notable additions of the Rules is the definition of theSensitive Data.

The Rule is quite widely worded and does take into its fold almost all the data that can have a direct bearing upon the right to privacy of an individual in case it gets leaked. However, the proviso to the rule does exclude the data already in public domain from the ambit of the definition of sensitive data.

The requirement to obtain the consent of the provider of the sensitive data does embody the necessity of element of consent for processing the data. Further the rule specifies that the data shall be collected only for the purpose sanctioned by the law. These rules further recognize the established principles of data protection including the right to purpose limitation, the right to fairness in processing and the principle of time limitation. In addition to these principles, the rules also require the body corporates collecting sensitive information to have a robust privacy policy and take adequate measures to afford safety to the personal sensitive data of the individuals. However, the rules provide a free pass to the government to send all the principles of data protection on a toss and allow the government and the law enforcement authorities to access the sensitive personal data of the individuals without their consent. Moreover, the adjudicating body Cyber Appellate Tribunal is appointed by the central government. With no independent adjudicating body in place and no shield against the possible intrusions into the right to privacy by the government, a robust data protection regime in India remains a distant dream.

- **Privacy in the Health Sector**

There can be no denial to the fact that the information related to the health and medical history of the citizens do form an inherent aspect of the right to privacy. It has been repeatedly heldby the Constitutional Courts in India and abroad that the disclosure ofthe medical details could lead to an unwarranted invasion into the personal domain ofthe individuals thereby causing extreme disturbances to the tranquility of the person.The Supreme Court while highlighting the importance of the information self-determination in the matters concerningthe medical history, in Mr. X v Hospital Z held that:

"Right of Privacy may, apart from contract, also arise out of a particular specific relationship which may be commercial, matrimonial, or even political. As already discussed above, Doctor-patient relationship, though basically commercial, is, professionally, a matter of confidence: and, there-fore, Doctors are morally and ethically bound to maintain confidentiality. In such a situation, public disclosure of even true private facts may amountto an invasion of the Right of Privacy which may sometimes lead to the clashof one person's "right to be let alone" with another person's right to be informed. Disclosure of even true private facts has the tenancy to disturb a person's tranquility. It may generate many complexes in him and may even lead to psychological problems. He may, thereafter, have a disturbed life all through".

This binding precedent of the Hon'ble Supreme Court, in the clearest of terms lays down the rule that even the true information about the medical history of a patient can't be disclosed without their consent. Even the SPDI Rules, 2011 categorize the health-related information as sensitive data and hence prescribe that these data can't be disclosed to a third party without their consent. However, to the contrary, the Clinical Establishment Rules, 2012 mandate the hospitals to maintain an electronic record of the medical history of the patients. However, due to the non-application of the rules on the public bodies, the Hospitals run by the governments are exempt from any of these rules and thus provide name-sake of protection from the unwarranted intrusions in the right to privacy of the citizens.

- **Existing Surveillance Regime in India**

The most crucial aspect of the upcoming data protection law in India is the limits that it seeksto impose upon the scope and width of the right to privacy. The law being at a very nascent stage in the field, it is imperative that it shall take a few years for the courts to come up with a settled approach in order to gauge the extent to which the right to privacy can be exercised. The judgment in Puttaswamy, for sure is going to set in motion a regime that will secure data privacy of billions of Indians to a great extent. It would be wrong to presume that Puttaswamy is the end of the endeavour of securing data privacy of the citizens, instead it's the beginning. At This juncture we are concerned with the what the Court held in Puttaswamy and how did it justify it and how shall the upcoming data protection regime in India be influenced by it.

It may be noted that the prime cause of contention between the petitioners and the respondents in Puttaswamy was related to the nature of right to privacy. Whether theright to privacy is an absolute one or does it come with inherent limitations? And if itisn't absolute, what are the imitations and how does the court justify them? The law on the subject is at quite a nascent stage but the Puttaswamy does provide a template to determine the situations in which the breach of privacy by the state can be justified. Through the course of our discussion in the following sections we shall seek to explore the nuances of the limitations placed by the SC on the right to privacy. This is the most important part of the issue at hand as the government is likely to accept that citizens have the fundamental right to privacy yet it shall certainly look for alternatives to justify its interference in the private domain of the individuals. The Data Protection Bill, 2019 has been sent to the select committee which is highly unlikely to alter the "exemptions" clause in the proposed bill.

CONCLUSION

The preamble of any legislation is one of the most vital factors influencing its interpretation by the judiciary. Thus, it becomes optimal to have a preamble that is precise and assertive about its object. The Data Protection Bill's prime objective should

be guaranteeing the right to data privacy of the citizens of India and fosteringa data protection regime that is sensitive to the remotest of the breaches to the right to privacy. The preamble must also incorporate within its fold an unequivocal commitment from the government against illegal intrusion in the private realm of theindividuals with a detailed roadmap of surveillance reform. The preamble should also take into the account the pressing need for creating awareness within the countryabout the contours of right to privacy and thus felicitate a privacy conscious society.It is proposed that the preamble of the Data Protection Bill, 2019 be amended as:

The preamble that in pith and substance incorporates these objectives will provide agreater width to the rights recognized in the legislation. It is submitted that the aspects like fostering a digital economy and undue emphasis on the economic aspectsof data shall do no service to the right to privacy. While, these objectives may be ancillary to a robust data protection regime, the rights to privacy must not be pushedto the backseat on the premise of fostering digital economy. The preamble must "*calla spade a spade*" and recognize the pressing need for the surveillance reform in the country and lay down a vision for a regime that is truly protective of the right to privacy in the long run. The preamble must in unequivocal terms endorse the constitutional necessity of protecting and preserving the fundamental right to privacyand thus a need for setting up a truly independent body to enforce it.

REFERENCE

- Adriana-Maria Sandru; Daniel-Mihail Sandru, *Humanitarian Law and Personal Data Protection,* 2018 PANDECTELE ROMANE 58, 61 (2018).
- Addison Litton, *The State of Surveillance in India: The Central Monitoring System's Chilling Effect on Self-Expression,* 14 WASH. U. GLOBAL STUD. L.REV. 799, 720 (2015).
- Aimee Boram Yang, *China in Global Trade: Proposed Data Protection Law and Encryption Standard Dispute,* 4 ISJLP 897, 901 (2018)

- Alan F. Westin, Privacy and Freedom 33 (1967); Andrew J. McClurg, *Kiss and Tell:Protecting Intimate Relationship Privacy through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 901 (2006).
- Alex B. Makulilo, *The Quest for Information Privacy in Africa*, 8 JOURNAL OF INFORMATION POLICY 317, 337 (2018).
- Alina Savoiu & Catalin Capatina Basarabescu, *The Right to Privacy*, ANNALS CONSTANTIN BRANCUSI U. TARGU JIU JURIDICAL SCI. SERIES 89, 101 (2013).
- Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 999-1002 (1995).
- ANNE S. Y CHEUNG, ROLF H WEBER, PRIVACY AND LEGAL ISSUESIN CLOUD COMPUTING 248 (2015).