AN ANALYSIS ON DATA PROTECTION IN INDIA

Sruti Devan. K, LLM, Presidency School of Law, Bangalore

ABSTRACT

The development and advancements in science and technology had compelled the legislature of the countries all over the world to bring new laws into existence. Data Protection laws is one among such laws, which emerged very recently to combat the cyber attacks against a person's right to privacy. Right to privacy includes right to protect his/her data too. Now a days, data privacy and its protection is a concern of every individual due to the misuse of technological developments. Data Protection is a mechanism which talks about how to protect a person's data from unauthorized access and malicious insiders. Indian constitution being a constitution which gives priority to rights than duties had already emphasized the importance of right to data privacy and its protection impliedly through Art. 21,19. Even though the Indian Penal Code, Information Technology Act and Right to Information Act talks about it, still India doesn't possess a separate legislation for the data privacy and its protection. The purpose of this research paper is to study the existing legal status of Data Protection laws in India and also to check the current status of the proposed Personal Data Protection Bill and the challenges faced by the bill in our society etc. For this purpose I had used many statutes including Indian Constitution , Indian Penal Code , IT Act , RTI Act as primary sources of data and read many articles and books etc as my secondary sources of data.

Keywords: Data Privacy, Data Protection, Indian Constitution, Information Technology, Indian Penal Code, Personal Data Protection Bill, Sreekrishna Committee, Data Security Council of India.

INTRODUCTION:

The concept of Data Protection is not a new concept for Indians. It is a part of our Upanishads which talks about meditation, which need to be done in a silent environment away from public interference and the concept of curtains defined in the classic literature works like Ramayana are the best example for that. In this 21st century, when the whole world is undergoing through a "Digital Revolution", Government of India also envisaged the idea of digital world through its "Digital India" initiative very recently. But the question is, whether a country like India which doesn't possess a specific statute for Data Protection will be able to succeed in this initiative? Here comes the importance of Data Protection. Every country which has a vision of complete digitalization and digital economy must have a strict, transparent and accountable data protection laws as its own. Through this research paper, I had tried to conduct an elaborated study on the concept of data protection, its importance in India, various statutes talking about it, its effect on society and also the Indian proposed bill on Personal Data Protection.

Research Objectives:

- To do a detailed study on the concept of Data Protection and its relation with Data Privacy in India.
- To locate the current position of Data Protection under various statutes of India including Indian Constitution.
- To know about the evolution, features and concerns of Personal Data Protection Bill and Srikrishna Committee recommendations.

Research Methodology:

The methodology I used for this research paper is purely doctrinal in nature. I used Indian Constitution, Indian Penal Code and Information Technology Act as my primary sources and some renowned articles, books and some websites related to Data Privacy and Data Protection as my secondary source of data.

Research Questions:

1. Whether any Indian statutes talks about Data Protection? If yes, up to what extend?

2. What are the reasons for the delay in passing of the Personal Data Protection Bill and what are the related concerns?
3. What will be the effects of Data Protection on Society?

CONCEPT OF DATA PROTECTION

'Data Protection' talks about a set of privacy laws, policies and procedures that intend to minimize interference into one's privacy caused by the compilation, storage and distribution of personal data. Here the word Personal data means any information or data which speak about a person and he/she can be recognized from that information or data. Normally such data or information will be collected by the Government itself or by any private corporate body or by agency. In other words, data protection is a mechanism talking about the protection of data from any unauthorized access. The methods and extent of data protection varies from a person to business and business to government accordingly.

NEED OF DATA PROTECTION IN INDIA

1. In this data economic world, the corporate bodies and big companies started to consider Data as an asset and also finds value in its storage, collection and distribution. In order to fulfill this vision, they started to protect their Big data.
2. Right to Privacy which (includes personal data)being a fundamental right in India, the government of India has an obligation to formulate and implement a legislation for Personal data protection.
3. In order to combat the rising cyber attacks like identity theft, data stealing and all, we need a specific legislation with strict sanctions and a redressive mechanism.

DATA PROTECTION IS A RIGHT?

Data protection is a right because this it is interrelated to Right to Privacy (which includes privacy of data) a fundamental right in India. And no data privacy is possible without data protection. So data protection is also a right.

STATUTES RELATING TO DATA PROTECTION

1. **Indian Constitution:** The development of the Constitutional right to privacy started in 1950s in the milieu of police supervision of the accused and domiciliary visits to a

person's home at midnight. In the case of ***M.P Sharma v. Satish Chandra***[1], Supreme Court held that, even though search and seizure is a part of the responsibilities of a police officer, conduction of it at midnight is a violation of Article 19(1) (f) of the Constitution. The Court added that a mere search by a police officer did not affect any right to property, and the seizure related to it is just temporary in nature. So it will act as a reasonable restriction on the right to privacy. Later in ***Kharak Singh v. Union of India***[2] cse, the court held that right o liberty comes under art.21. In ***R Rajagopal v. State of Tamilnadu***, the petitioner was an editor, printer and publisher of a Tamil weekly magazine published in Tamil Nadu who wanted an order limiting the ***State of Tamilnadu***[3] from snooping with the authorized publication of the autobiography of Auto Shankar, a prisoner awaiting the death penalty. Later in another case[4], Justice. Jeevan Reddy, explicitly mentioned that that, the right to privacy is implicit in art.21, and 19 of the Indian Constitution.

2. **Indian Penal Code, 1860:** The Indian Penal Code has come into existence during the British rule in India. The first draft was formulated in 1860s under the leadership of Lord Macaulay. Indian Penal code doesn't satisfy the whole need of Data Protection in India. Our Indian Criminal law does not exclusively deal with breaches of data privacy. Under the Indian Penal Code, legal responsibility for such breaches must be dependent upon the related crimes. For example, Section 403 of the India Penal Code talks about penalty for dishonest misappropriation or conversion of "movable property"[5] for one's own use. When it falls under the liability of other, then the question arises on the opposite that whose right are to be protected. The Section 405 and Section 409 talks about the punishment for misappropriation of some other person's property under the concept of breach of trust. Section 378 talks about theft but there is no specific section talking about the theft of data or information. In this matter, there are two ways to addresses the legal right which one may can endure. In reality, the crime is done against the state only, thus the right of the state to maintain law and order it's a severe concern. The connection of the word 'data protection' with 'Indian Penal Code' on addressing

[1] AIR 1954 SCR 1077
[2].AIR 1963 SC 1295.
[3] (1994) 6 SCC 632.
[4] (1994) 6 SCC 632
[5] 'Movable p1roperty' has been defined as property which is not attached to anything and is not a land.

the right is appropriate. In this texture the state can also come under the purview to protect the data of an individual.

3. **Information Technology Act (Amendment) 2008:** Indian Parliament had made many efforts to bring the concept of data privacy under IT Act, 2000. This Act has been amended many times to meet the new challenges posed by the development of cyber world. Among them, the latest is 2008 Amendment Act. According to the Data Protection & Information Technology (Amendment) Act 2008, the words 'data protection' and the 'Information Technology" has its own connotation with each other. The objectives of the Act precisely talks about the protection of the cyber related rights. This Act includes provisions to prevent the illegal use of computers, computer systems and data stored within. There are a number of other provisions related to 'data protection'. The newly inserted section 43A and Section 72A of the Act also talks about the protection of data. The main drawback of this legislation is that the present provisions talking about the data security and confidentiality are insufficient to cover the newly emerged cyber crimes.

4. **Right to Information Act, 2005:** In India, the practical establishment of right to information of citizens to secure information comes under the control of public authorities to promote transparency and accountability. Section 2(j) of the RTI Act talks about the definition of 'right to information[6]'. Here an issue arises that, the 'data' which was kept with the public authority are safe or not especially the digital data under clause (iv) of Section 2(j) is properly maintained or not. Therefore the data protection under this Act is a concern and being taken care as a matter of an individual's right. In ***Bannett Coleman v. Union of India***[7] the court held that 'it is unarguable that by freedom of press means the right of all people to speak, publish and express their views, ideas etc' and 'freedom of speech and expression includes the right of all citizens to read and be informed'. In ***Indian Express Newspaper (Bombay) v. Union of India***, the Court mentioned that, "the basic idea behind the concept of freedom of speech and

[6] "Right to Information" means 'the right to information accessible under this Act which is held by or under the control of any public authority and includes the right to: (i) Inspection of work, Documents, Records; (ii) Taking notes, Extracts or Certified copies of documents or records; (iii) Taking certified samples of material; (iv) Obtaining information in the form of Diskettes, Floppies, Tapes, Video cassettes or in any other electronic mode or through printouts where such information is stored in a computer or in any other device'.

[7] AIR 1973 SC 60

expression is that, all members should be able to form their beliefs and express them freely to others. In addition, the principle implicated here is the people's right to know". Later in ***PUCL v. Union of India*** added that, the right to information was further be superior to the status of a human right, essential for building governance transparent and accountable. The Supreme Court has also mentioned that the right to information is inbuilt in Article 19 of the constitution; therefore we can say that the existing linkage between these two concepts is right based.

PERSONAL DATA PROTECTION BILL OF INDIA (PDB BILL)

Evolution of PDB Bill:

In India, the right to privacy in was declared a fundamental right by our Supreme Court of India on August 24, 2017, in its landmark judgment in the case of ***Justice K.S. Puttaswamy and Anr. v. Union of India And Ors.***[8] ("**Right to Privacy Case**"). After this Judgment, the requirement of legislation to protect the personal data and privacy of individuals was raised. As a result, in August 2017, the Central Government of India appointed a data protection committee under the chairmanship of retired Supreme Court judge, Justice Srikrishna and on July 27, 2018, the committee headed by him released an extensive white paper showing the importance and need of data protection law in the country. Consequently in July 2018, the committee released the final draft of Personal Data Protection Bill, 2018. Later the Personal Data Protection Bill, 2019 ("**PDP Bill**") was introduced in the loksabha with few modifications. Then on December 12, 2019, PDP Bill had been referred to a Joint Parliamentary Committee ("**JPC**") for further debate and examination. And after around 2 years, the committee submitted its report with various recommendations and changes.

Key recommendations of JPC Committee:

A short summary of the key recommendations of the Report is given below:

1. **Change of name & scope of "Data Protection Bill"**: According to the recommendations of the Report, the JPC has suggested to change the name of the bill to "Data Protection Bill", by this means, it will cover the non-personal data too. But regarding this matter, there exist a concern concerns from the stakeholders that

[8] (2017) 10 SCC 1.

inclusion of both personal and non-personal data in the same legislation will dilute the objectives and purpose of the PDP Bill, which was brought out with an aim to provide protection of personal data only.

2. **Selection of Data Protection Authority (DPA)**: Under the PDP Bill, the role of stakeholders in the selection of a DPA was limited. But this Report recommends that the selection committee of the DPA must have more representation from technical, legal, and academic experts, in addition to the bureaucrat officers included in the selection committee. This will bring the members of the DPA under the control of the Central Government indirectly because all members in the selection committee are appointed on command of the Central Government.

3. **Exemptions to government**: The PDP Bill exempted the Government under the draft legislation, for protecting the national interest. But this Report added conditions to this exemption, and recommended that the Government may exempt itself from the provisions of the legislation only after a *fair, just, reasonable and proportionate procedure.*

4. **Data breaches**: According to the PDP Bill, the companies were asked to report personal data breaches, when such breaches cause harm to the data subject. But here under the recommendations made by the committee, the Report not only mandates preservation of record of all kinds of data breaches, despite of whether the breach is related to personal or non-personal data, but also mentioned a time period of 72 hours for reporting such breach.

5. **Social Media regulation**: The old bill pointed out that the social media intermediaries must be subject to higher assessment. But here under this report, to curb the threat of fake news and fake accounts, the Report suggested the verification of all user accounts on social media intermediaries. The Report also mentioned that the intermediary framework which comes under the Information Technology Act, 2000, has failed to achieve its objectives. The report recommended to treat the social media intermediaries as '*publishers*' in certain specific contexts, particularly in relation to content of unverified accounts.

6. **Children's data**: The PDP Bill had explicit provisions for the protection of data relating to children and also had defined the concept of guardian data fiduciary as a data

fiduciary that operates commercial websites or online services aimed at children, or processes large amount of personal data relating to children. But this Report had suggested for the deletion of the concept of guardian as a different class of data fiduciary because it may dilute the objective of safeguarding children.

7. **Data Localization**: Under the PDP Bill, data localization provisions were already existed, later the JPC strongly advised for the storage of all data in India itself for national and security reasons. This Report suggested the government to bring copies of all sensitive and personal data and information that is stored in abroad and thus the data of all entities operating India should be localized in India itself.

1. FEATURES OF THE PERSONAL DATA PROTECTION BILL, 2019:

This Personal Data Protection Bill, 2019 **("PDPB")** was introduced on December 11, 2019. The purpose of this Bill is to provide protection to the privacy of personal data of individuals and to establish a Data Protection Authority of India for to deal with such related matters. The Bill will supersede Sec. 43A of Information Technology Act, 2000 which talks about the compensation payable by corporate bodies for failure to protect Personal Data. This bill talks about the manner in which personal data is to be collected, processed, used, disclosed, stored and transferred.

1. **Applicability:** The PDPB will have application to the processing of personal data collected and stored by the government, any Indian company, by any citizen of India or by any body incorporated in India and comes within the territory of India. This Act will have application on any foreign companies dealing with personal data of Indian Citizens.

2. Obligations of Data Fiduciary: The collection, processing and storage of Personal Data can be done only for a lawful purpose. When it comes to processing of data, the controller or processor who acts as the data fiduciary have the following obligations to fulfill;

1. The purpose must be clear and lawful.
2. Collection of Personal Data shall be limited to data that is required for to fulfill the purpose.
3. Prior to collection and processing, a notice should be send to data subject.

4. Prior to processing, the controller have to get the consent of the data subject.

3. **Rights to Data Subject:** This bill provides to individuals like ;right to get confirmation from the controller regarding the processing of their data, right to correct the inaccurate and incomplete data and also to update it any time, right to data portability ,right to withdraw the given consent at any stage of data processing etc.

4. **Data Protection Authority:** This bill talks about the establishment of a Data Protection Authority of India which shall protect the interests of individuals and prevent the misuse of personal data etc. Orders of this Authority can be appealed to an Appellate Tribunal and appeals against the order of aforesaid Tribunal can be filed directly to Supreme Court.

5. **Restrictions on Transfer of data outside India:** The Sensitive personal data can be transferred outside India for processing only if the data subject provides explicit consent. On the other hand, such sensitive personal data should continue to be stored in India too.

6. **Exemptions:** The central government can exclude any government agency from the application of this act in the interest of sovereignty and integrity of our country, for national security purposes and to maintain friendly relations with foreign states.

Concerns Related to Personal Data Protection Bill 2019:

- This bill is a two sided sword. On one hand, it protects the personal data of Indians by providing certain right to Data subjects, but on the other hand, it gives the central government to exclude its agencies under certain grounds.

- Under this bill, the central government can process the data of citizens including sensitive personal data at anytime without getting consent from data subjects.

EFFECT OF DATA PROTECTION LAW ON SOCIETY

We live in a world where the entire society is connected through a single imaginary thread of information by means of online platforms like Facebook, Skype, Whatsapp and Twitter. People

of our society are so dependent upon these social media platforms only to get information but also to store and share their data with people all around the world. Therefore, it s very important to protect such shared and stored data from being misused by other people or by any agency through some specific and strong legislations. In this digital era where we consider data as a part of our privacy and asset which is available everywhere, it creates an obligation on government to protect it through any means. The availability of bulk data in an open access platforms creates huge risk of offences like identity theft, misappropriation of data, other cyber-crimes, hacking, etc. Data protection includes information safeguarding too. Social media is a form of communication that done via Internet. There are many other types of social medias also like, blogs, micro-blogs, wikis and websites, widgets etc. And very recently, social networking sites like Facebook, Twitter, WhatsApp, etc have attained much popularity among people irrespective of age. The main purpose of these social media sites is to create a relationship with the world digitally. But the users knew nothing that that the data they provided and shared are not safe in the digital world and is capable of inviting troubles and cause crimes.

CONCLUSION:

When a number of organizations are using computers to keep and process information of many people, there is always a forthcoming danger that the data stored could be misrepresented or fall into the wrong hands, and can be later misused by them. After demonetization, our government has initiated several measures to increase digital payment and to go for a cashless culture. So we need an immediate attention to the matter of legal framework for privacy and protection of data of individuals and entities in India. Because, unlike UK, Australia and other European countries, India still doesn't have a strict Data Protection law. Even though Supreme Court had expanded the concept of privacy and data protection and made it as a fundamental right of every Indian citizen, the current exiting related laws are not enough to safeguard the complete enjoyment of the above mentioned fundamental right. Hence, we need a broad Data Protection Law to provide a greater clarity and safe enforceability of rights.

SUGGESTIONS:

1. A constitutional amendment can be made to include data protection right as a fundamental right and also a National Policy on Data Protection Law can be developed to ensure that the individuals have the freedom of controlling their own information collection and transmission.

2. Just like the National level Information Commission, a National level Data Privacy and Protection Commission can be established to safeguard and provide grievance redressel.

3. In this digital era, where data is considered as a valuable resource, it should be regulated properly. Therefore more legislations and regulations should be brought up for this purpose.

4. The **Personal Data Protection Bill, 2019** should be reformulated to guarantee that **it focuses on user rights and also highlight user privacy.**

5. The **governments have to take much care and consider the privacy** of the citizens when they **strengthen the right to information.**