OBLIGATIONS OF DATA FIDUCIARY AND PROTECTION OF DATA: AN ANALYSIS

Mayuri Taware, LLM, B.B.A. LLB, DCL, DFS, Assistant Professor at KLE Law College Kalamboli, Navi Mumbai

ABSTRACT:

The number of ways we use information has increased so dramatically in the twenty-first century that it is now widely referred to as the "information age." The reality of today's digital environment, practically is that almost every single activity that a person engages in involves some type of data transaction. The Apex Court of India in Puttaswamy judgment has stated the importance of data by giving examples of Uber, Alibaba, Facebook, Alibnb just by making use of data and not owning vehicles, no inventory, creation of content or real estate respectively are one of the huge companies in today's world. Data is becoming an increasingly important and pervasive part of our lives. Data counts as the pulse of the modern global economy. It will be no exaggeration to say and in fact has been mentioned by many that data is now not only considered as 'new oil' but as a 'new currency' in itself. At present we have Information Technology Act 2000 which governs data protection regulations in India. It stated that unauthorized access to data is a crime, and that anyone who causes a wrongful harm must pay restitution and face prosecution. India has been one of the largest data generators. With the implementation of government projects such as unique biometric identification, e-governance systems, and the Aadhaar Act, among others, the collection, processing, and sharing of personal data of individuals has become a critical issue in India in recent years. In recent years, India has experienced a rash of cyber security incidents, major data breaches. While the transition to a digital economy is still underway, personal data processing has become commonplace in both the public and private sectors.

This paper intends to analyze the viability, outcome, set of operations, functions performed and see whether there is any requirement of establishments and adoption of any kind of new structural changes by one of the important constituents of data protection, Data Controllers / Fiduciaries.

Keywords: Data, fiduciaries, informational privacy, protection.

INTRODUCTION

With the growing evolution and increasing reliance on technology, and movement and collection of information for nearly every activity it is indeed necessary to understand the importance of data is today's world. As a result of pandemic, technology has been a silver lining since the digital usage increased unanimously. Specifically with the advent of an internet era, the information and data so processed or collected becomes of much more relevance as it contains personal details of the individuals including what are the things that are purchased by them, the mode of payment of such purchases, the sites being visited by them, the places to which they travel and many more specific personal details relating to birth place, origin, healthcare, location etc. getting transferred and being collected by other entities.

Data is the new oil, with the ability to unleash the true economy's power. It has become a critical component of business model and has in fact generated and given growth opportunity to new market. India generates mammoths amount of data and is one of the largest data generators in the world.. In today's world, information technology is at the pinnacle of everyone's everyday life. The world is gradually becoming more and more connected through sharing data with the advent of artificial intelligence (AI) and block-chain. Therefore it calls for data to move freely across borders to continue the growth of the global economy and foster innovation. India is considered as a hub of data market by multinational companies. Data analytics studies humungous amounts of data to unearth hidden patterns, correlations and provides new insights. This helps in enabling the businesses to remain competitive by reaching out to smarter decisions and functioning more efficiently, making higher profits and much more content and happy customers. Every day, every person generates significant volumes of sensitive personal data while exploring the World Wide Web, whether knowingly or unknowingly. The protection of people's personal information has never been more under jeopardy. By combining datasets from various sources and domains, as well as applying data analytics and artificial intelligence technologies, new insights can be generated that can be used to create new and innovative products, services and act as a tool for surveillance. Data is on the verge to replace humanism. Data is on the verge to replace humanism. With the rise of data centers and other linked industries that have the potential to offer considerable job opportunities, data localization can provide a big boost to the digital economy in the home market. Data can help India achieve its goal of becoming an 'Aatma Nirbhar Bharat' by

enabling technology-driven innovation in almost every sector of the economy and across all levels of government.

ANALYSIS

ROLE OF DATA FIDUCIARIES

A Data Fiduciary according to Digital Data Protection Bill, 2022 is an entity, service provider that is accountable for complying with the data protection law. They are the key decision-makers. They have final say and control over the reason for data collection, as well as the means and methods of data processing. Personal data refers to data relating to individuals which defines the characteristic, trait, attributes like age, gender, education, qualification etc. Here individuals are termed as data principal. The relationship between data principal and fiduciary is built on fundamental expectation of trust. Regardless of any contractual relationship, an individual expects her personal data to be used fairly, in a way that serves her interests, and in a way that is reasonably predictable. A fiduciary relationship is defined by this they play a key role in ensuring the fair collection of data, processing the data and storage of data. Data principals expect varying levels of trust and loyalty in the digital economy, depending on the nature of data shared, the purpose of such sharing, and the entities with which data is shared.

Data fiduciaries exist in various sectors including but not limited to financial insurance, defense, health, communication, information technology etc. For example; Banks, RBI, SEBI, National Payments Corporation of India, Income Tax Department, enforcement directorate, law firms, social media players, supermarkets, pharmaceutical companies, corporate, RTO offices, data collecting bodies for purpose of surveys are fiduciaries in various sectors. Data fiduciaries are further classified as significant data fiduciaries. Significant data fiduciaries are the one which processes sensitive personal information depending on the factors such as volume, sensitivity, turnover, risk of harm, use of new technologies, any other factor causing harm from such processing.

WHAT DATA FIDUCIARIES DO?

Data Fiduciaries executes one of the most important function that is processing of personal data. Processing of personal data as defined under the Data Protection law “gathering,

recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure through transmission, distribution, or otherwise making available, restriction, erasure, or destruction are examples of operations carried out on personal data.*"*[1]. The term processing has a very wide ambit and covers almost everything that can be done with the data. It also encompasses activities and techniques like data mining, geotagging, sharing, geocoding, extracting, clustering, transferring, data matching, data warehousing. Almost everything an organisation can do with data in its lifecycle, including the initial acquisition and eventual destruction of the data, as well as storage in between or any use of the data, is considered processing. Processing should be done in a fair, legitimate, relevant, adequate, accurate, complete, updated, transparent manner.

THE EFFECT OF DATA FIDUCIARIES FUNCTIONING ON DATA PROTECTION

Data fiduciaries ensures protection of the digital privacy of individuals by granting individual autonomy to determine what extent of information is been processed, to choose when, how, and how much personal information about themselves is shared with or transmitted to others, and the right to object to online profiling, marketing and targeted advertising since data protection is the biggest concern nowadays. One of the vulnerable section of the society are children's. Children make up a significant portion of internet users, and their personal and sensitive information is frequently collected through their use. They are distinct from adults in the legal system because of their vulnerability and perceived lack of understanding of the consequences of their actions. Before processing any type of data, a data fiduciary (similar to a data controller) verifies the age of the child and obtains the consent of the child's parent or guardian. Data fiduciaries are prohibited from profiling, tracking, or behaviorally monitoring children, or targeting advertising directed at them, as well as any other processing of personal data that could result in significant harm to the child.

Large scale data harvesting scandals, data loots which grabbed the attention towards data protection are Pegasus Spyware in which the alleged targets in India were, opposition leaders, political strategists and ministers, tacticians , minority leaders, supreme court judges, religious leaders, journalists, activists, administrators such as Election Commissioners, and heads of the Central Bureau of Investigation in India, according to the

[1] Sec 3(36),Digital Data Protection Bill, 2022.

Pegasus Project investigations (CBI).[2] After phone analysis of the above mentioned targeted group it revealed that their phones were targeted by the Spyware. Through Pegasus by transmitting data covertly from their hard drive, a user can obtain covert information about someone's else device. Their motive was to gain access to the information stored on targeted audience. Pegasus spyware was used as a harsh weapon to infringe right to informational privacy of the targeted audience which may have incidentally resulted in breach of national security and private security.

Data breach in debits and credit sectors of banking sector - Various banks including but not limited to banks in India has evidenced data breach in banking instruments such as debit and credit cards. In this majority of debit and credit cards were compromised due to infusion of malware in the payment service system providing point of sale and ATM services. It led to fraudulent use of card in another countries when actually the card possessors were located somewhere else. It casts equal responsibility on all the parties involved in this there should be thorough checks before on boarding any third party providing outsource services to an entity.

Along with it data breaches in health care sectors, during the outbreak of Covid-19, telecom , sports, infrastructure, retail, IT-BPO and manufacturing sectors, freight and logistics enterprises, automobile sectors, electoral process , stock market, stolen customer credentials, financial damages, phishing, unemployment frauds during pandemic, identity thefts. According to the reports India stands in third position in global data breaches.

Panama papers are the documents containing personal financial data of individuals possessing wealth and which have been kept private by them. In Panama papers scam the aforesaid information was leaked and published. It grabbed rising attention in India because of intrusions of famous personalities who were the targeted audience in the Panama paper scam. The Panama paper once again enlightens us about the vital role they play in data protection and the results of breach of data protected. It also makes us aware that the systems in placed should be updates proper internal check should be there and be audited frequently. Proper checks and controls, internal policies are to be prepared and complied for data sharing, data collection and data disbursal.

[2] Namrata Biji Ahuja " *Pegasus: Investigations worldwide hold a crucial lesson for India*" The Week Magazine, 2022 available at https://www.theweek.in/theweek/current/2022/02/19/pegasus-investigations-worldwide-hold-a-crucial-lesson-for-india.html Last visited on April 11, 2023; 2:06 PM

Terrorist groups have used the internet to propagate their ideas, recruit terrorists, and plan operations. They conduct events and discussion forums, upload inflammatory videos, and use social media platforms and even action video games to interact with potential recruits. Some terrorist organizations even have their own official terrorist usernames. Internal security, as well as social and civic discord, are all threatened. As well as outspread of hate content via websites and social networking sites operates as a vehicle for the spread of discontent and disorder. Thus, data fiduciaries take into account such risk assessments and analyse, conduct security safeguards.

Breach of unpublished price sensitive information- In a recent ongoing case SEBI the regulator has expelled NSE former chairperson Chitra Ramkrishna for disbursing restricted data to someone and seeking guidance for execution in her work and discharging of her role in the organization. It shows serious concern about the time of span it was going on. People at eminent positions need to be inducted, vigilant on continuous basis to be in touch with the changing roles and responsibilities cast on them.

Data breaches in digital era and applications like Adobe, Canva, ebay, Equifax, Dubsmash, Heartland Payment Systems, LinkedIn, Marriott International, My FitnessPal, Myspace, NetEase, Sina Weibo, Yahoo, Zynga, Animal Jam signifies a dire need of the hour to have a stringent regulations on data fiduciaries for safeguarding data.

OBLIGATIONS OF DATA FIDUCIARY BEFORE COLLECTION OF DATA

Any person who processes personal data must do so for a legitimate, explicit, and lawful reason. As a basic manner of establishing the lawfulness of processing, ‘consent’ is used. The data fiduciary is usually the one who collects personal data and decides how it will be used. The data fiduciary determines the means and purpose of processing. However, the Data Fiduciary may hire another company to process data on its behalf. The basic requirement is that personal data be processed in a fair and reasonable manner to protect the data principal's privacy. This clearly indicates that the goal is to preserve an individual's privacy, and that there is an obligation to ensure that this goal is met in a fair and reasonable manner. By arming her with relevant information and putting the ultimate decision of whether or not her personal information will be used in her hands, Notice purports to respect the data principals basic autonomy. Before collecting personal data, every data fiduciary must provide notice to the data principal. The information should be provided to the data principal; the requirement behind

processing such data, the modes of collecting data, the name and personal details of data fiduciary as well as the data protection officer, the origin from which data is to be collected, information about any cross-border personal data transfers that the data fiduciary intends to make, retention period, the entities or third parties with whom the data is been shared, if personal data is to be processed on the basis of consent, the data principal's right to withdraw his consent, as well as the procedure for doing so, the legal basis for such processing, as well as the ramifications of failing to provide such personal data, the period for which the personal data will be kept, or, if no such period is known, the criteria for determining such a period; and any other information that the regulations may require, notifications regarding data breaches, grievance redressal procedure, right to file complaint. This components of notice should be stringently followed. The transparency and accountability measures are a directive that every data fiduciary must take the essential steps to make specific information available to data principals, the data authority, and the general public and be held accountable for any processing of data as specified.

OBLIGATIONS OF DATA FIDUCIARIES AFTER COLLECTION OF DATA

Processing of personal data includes all activities involving personal data, from the planning of processing to the erasure of personal data. The collection, storage, use, transfer, and disclosure of personal data are all examples of personal data processing. Data auditing is the process of evaluating data for accuracy and efficacy during the course of its lifecycle in order to guarantee that it is fit for a certain purpose. The performance of the data is evaluated, and problems are discovered and addressed. Data auditing improves data quality, allowing for improved analytics and operational improvement.

Every data fiduciary is entitled to create a privacy by design policy that includes certain mandatory provisions and submit it for certification to the Data Protection Authority. After being convinced that it meets all of the requirements, the DPA will certify it, and it will then be published on the data fiduciary's and the DPA's websites. The managerial, organizational, business practices, and technical systems designed to predict, determine, and bypass harm to the data principal should be included in the privacy by design policy, which will necessitate a risk assessment audit and the development of a risk mitigation information security policy.

Data retention means storage of data for a set period of time. The data fiduciary must not keep personal data longer than is necessary to fulfill the purpose for which it is processed,

and must delete personal data when the processing is completed. Personal data may be kept for a longer period if the data principal has given his or her explicit consent or if it is required to comply with any current legal obligation. In the light of the obligations mentioned above implementing data protection principles compliant activities or ensuring the data subject's rights, protecting personal data, and conducting audits, documentation of obsolete privacy policies, retaining data, maintaining security safeguards, risks assessments, as well as alternative compliances like anonymisation of data would reach the objective of big data analytics and a boost to free and fair digital economy.

CONCLUSION

India is on the verge of adopting a data protection law that might alter the basic structure of the internet. This area of law is maturing in India, and it will hopefully be handled in the near future with appropriate solutions and strategies. Given the importance of data privacy as a fundamental right of citizens and the economic consequences of data breaches, the government should reconsider the above-mentioned challenges. A strong personal data protection law is urgently needed. Public awareness, greater implementation and regulation, and quick grievance redressal must all be prioritized. Individuals' rights to privacy and data protection are clearly jeopardized by the proposed laws, especially in the lack of any legislation to that effect. As a result, a comprehensive law protecting rights in this area and identifying their limitations is urgently needed. It is a long-awaited and desperately needed piece of legislation that will replace India's current obsolete, legacy, and ineffective data protection regime. It will help protect individual privacy rights and promote fair and transparent data use for innovation and growth, unlocking the digital economy, as compared to current standards. It has the potential to generate jobs, raise user awareness of their privacy, and hold data fiduciaries and processors accountable.

Because India is such a diverse country, operationalizing effective consent would require more than just legal and regulatory controls. In today's world, citizens have access to a wide range of government and private-sector services. These transactions entail the transmission of massive amounts of data, which is frequently sensitive or personal data. This information is frequently required for the provision of the service sought, although it is possible that such data is collected for non-essential purposes. A major worry is the protection of data obtained for lawful purposes from intrusive attacks by criminal actors. The legal basis for online

interception and surveillance must be consistent with our constitutional ideals. The government should be able to utilize its powers in a reasonable manner. In other words, procedural protections should ensure that the constitution and the law are strictly followed. It is necessary to improve notice design or to examine whether the usage of notices is the best solution to prevent malicious activities.

Further the regulatory sandbox has the possibility to be exploitative because it allows data fiduciaries to use personal information without providing adequate notice, causing them to be misinformed before giving their consent. I believe that you don't bolt on privacy; you think about it in the development process of products, you must incorporate it into your design.

Finally, in my opinion, India requires a dedicated law, similar to the EU Digital Markets Act, to provide clarity on economic governance. GDPR or India's DPA is a positive step toward their respective countries' security. It is critical to safeguard an individual's data. These days, anyone can steal or misuse a person's personal data, a company's valuable data, or government data that is critical to national security and can be extremely dangerous if it falls into the hands of an enemy country. The EU's enforcement of non-compliance is likewise impenetrable, ensuring that no hacker or intruder can steal or tamper with the data. The GDPR is heavily influenced by the DPA. Government agencies are not immune from the GDPR, which includes mandatory obligations to notify data principals in the event of a data breach.