RIGHT TO PRIVACY IN INDIA: DATA PROTECTION

***RAHUL SURESH[1]**

INTRODUCTION:

We live in an era where highly sensitive and personal information of an individual could be hacked through the internet in a matter of seconds. Such information holds enormous personal value to an individual and the incapability of misusing such data would be biggest relief for every person in today's world. Unfortunately, such level of data protection is still a utopia due to the absence of effective legislative measures which has been a desperate need since the last two decades. In order to keep a basic check and balance system, the government introduced the Information Technology Act, 2000 i.e. the first regulatory measure of data protection taken by the Indian government. The government has still not recognized the urgent need for change in this sector. In 2015, an immensely advertised campaign on Digital India was also put in force which was focused towards creating a larger online service and delivery platform within the country through spreading awareness in the public. But a significant step in achieving every new goal is to possess a fool proof execution of the plan, hence the decision of providing a wider platform to the digital world to enter into the lives of the people was an inadvertent decision. The prevalent condition of our data protection measures are terrifying and the level of knowledge possessed by various individuals across the world makes it quite an easy task for them to hack into the servers and leak/misuse various sensitive information. I believe it is high time for the government to find the eligible personnel to build a secure platform to protect such highly sensitive information before taking the big step of building a digital India.[2] In 2016, the government introduced Aadhar cards for every Indian citizen that worked as an identification method as well as receiving financial benefits from the government. It became a major privacy concern when the government made it mandatory to link their Aadhar card numbers to their permanent account numbers so as to create new bank accounts and filing of tax returns, to provide a helping hand to the government employees to catch tax evaders. Such compulsory linking of Aadhar cards would provide easy access for the government to gain control over various sensitive and financial information of its citizens without the knowledge of such person. The lack of rules

[1] Symbiosis Law School, HyderabadAcademic Year - 4

[2] Ajay Kaushik, Data Protection in Digital India, Business World, Available at http://www.businessworld.in/article/Data-Protection-in-Digital-India/29-02-2020-185228/

and regulations to ensure the access to such information is provided to the government only for the benefit of the people, has made it a risky move.[3]

In 2019, the Data Protection bill was introduced in the parliament. Even though it seemed like that this bill has put forward the required changes to strengthen data protection which we have been longing for all these years, but all it did was to grant the government with more power in their hands to use the information in accordance to their own requirement. The Bill clearly states that it allows the government to exempt any of its agencies from the requirement of this legislation and also empowers the government to decide how their use of such information would be reviewed. Possessing the legal ability to use such sensitive information with mere restrictions in itself is enough for them to misuse such information to the disadvantage of a person.

JUDICIAL BATTLE OF DATA PROTECTION RIGHTS:

The legislative action towards building a strong and reliable platform of data protection has been extremely disappointing and they are still backing the argument of the constitution not providing a right to privacy to the people. Without the recognition of this right, the authority of the public to question the usage of their personal information by the government would be unreal. In order to avoid an unfair accumulation of power in the hands of the government, the judiciary has played a significant role in the recognition of the right to privacy through various recent judicial pronouncements. The first case on 'Right to privacy' as a fundamental right was heard by the Supreme Court in the case of "*MP Sharma and Ors v Satish Chandra, District Magistrate, Delhi and Ors*"[4], where the Hon'ble court held against the existence of any such right as 'Right to Privacy' under the Indian Constitution and also stated that there is no reasonable explanation for it to be included as a fundamental right now. However, the judiciary was quick enough realise the importance needed to be given to this specific right in order to provide personal liberty to its people that has been guaranteed under the Indian constitution. The same had been stated by Justice Subba Rao in the case of "*Kharak Singh v State of Uttar Pradesh and Ors*"[5], where he brought out the close relation between right to

[3] Shivakumar Shankar, Indian Government's Push to Data Governance Can Be a Game-Changer For Insurance Industry, Lexis Nexis, Available at https://blogs.lexisnexis.com/insurance-insights/2018/04/indian-governments-push-to-data-governance-can-be-a-game-changer-for-insurance-industry/
[4] 1954 SCR 1077
[5] (1964) 1 SCR 334

privacy and personal liberty guaranteed to us under Article 21. Following this, there have been various similar judgments passed by the Hon'ble courts in order to protect the privacy of the people according to the procedure established by law. In the case of "*KS Puttaswamy v Union of India*"[6] also known as the 'privacy judgment' granted the right to privacy a status similar to a fundamental right instead of a mere statutory right. Due to its long history of judicial precedents, the matter was put before a nine judge bench in the Supreme Court. The Petitioners for the case argued in favour of right to privacy holding the same value as any other fundamental right under the Indian Constitution and this right could be seen under Article 14,19,20,21&25 of the Indian Constitution r/w various international covenants. Whereas, the Union of India argued against the fundamental status of any such right due to the lack of any specific mention of right to privacy within the constitution, its vagueness and the lack of need for the recognition of a new fundamental right to privacy with the prevalence of sufficient laws to protect the privacy of individuals. The Hon'ble Court rendered a judgment in favour of the Petitioners and held that "Right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the constitution". The Court made a few more observations within the judgment which included: (a) the right to privacy is a necessary right for every individual to live his/her life with dignity (b) Privacy has a positive as well as a negative consent i.e. the positive consent being the duty of the State to protect the privacy of an individual by taking the required measures and the negative consent being a barrier restraining the State from taking any such action which would infringe the personal liberty of an individual. Justice DY Chandrachud made a few additional observations in the judgment where he felt the obligation to establish a well-structured mechanism to ensure the protection of informational privacy of the people since we live in an age of information and it holds more value to the people than ever. The threat of misusing the private information is not only posed by state actors but also by the non-state actors. The intent behind requesting the government to form a data protection authority is to lay down a procedure in order to receive access to the private information of people only with their explicit consent and control over the use of any such information by the state or non-state actors.[7]

[6] (2015) 8 SCC 735
[7] Data Protection and Privacy Issues in India, Economic Laws Practice 2017, Available at http://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf

SUPERVISION OF DATA PROTECTION IN BUSINESS:

Currently, there are various regulatory bodies for data protection in different lines of work including telecommunication, medical, banking and insurance sectors.

- **Telecom Sector:**

Being a business sector which functions primarily using the personal data of its customers. The increased usage of e-services and being able to gain access to an individual's e-wallets and social media accounts with the use of their SIM cards has become an easy mode of transaction but with an increased risk of misusing personal information. People could suffer serious personal data breach by just losing their mobile phone or when a third party gains momentary access to the SIM card. TRAI provides its customers an option of blocking their SIM cards in case of such events but it might get too late by the time the SIM is blocked. In order to prevent such misuse, TRAI should come up with better security measures. One such preventive measure is to setup a SIM PIN which would not allow the user to gain access to it without entering a PIN that comes with the packaging of the SIM card.

- **Medical Sector:**

The Healthcare organisations collect a huge amount of sensitive private information of a patient ranging on a wider scale than any industry. It records information relating to the patient's financial details, sexual orientation, medical history, biometric details and many more highly sensitive private information. Healthcare organisations in India are not known to be well equipped with a strong online security system in order to protect these sensitive information from cyber-attacks. The approval of the PDP, 2019 Bill would help them to build a much better online security system as the bill imposes enormous fines on the healthcare practitioners who fail to maintain the required security measures. Such required security standards would also support the healthcare organisations to gain a competitive advantage in the healthcare business and provide better data security to its customers.

- **Banking Sector:**

The banking sector has adapted mainly into an online service platform which collects certain personal information from its customers including credit history, bank account details, personal details, etc. These details are collected in order to provide better services to its customers, with no predetermined period till when these organisations could hold this

sensitive information unless expressly agreed while giving the details to the organisation. This unwarranted access of personal data has been curbed under the PDP, 2019 Bill and it has introduced a much more transparent form of functioning where the actual owner of the personal information i.e. the customer is given back the control over such information.

- **Insurance Sector:**

Like all the other business sectors, insurance sector is also in immense need for a better data protection measure for holding the trust of its valuable customers. The insurance companies collect the personal data from people in order to determine the approximate life span or the behavioural pattern of an individual which helps them make a profit-risk analysis. The IRDAI has its own set of legal provisions which helps in bringing down the risk of breach of data privacy within the insurance sector such as; the insurers have a system well equipped with security features in which the personal data is recorded, personal information of the insured should not be released unless legally required and in case the information is transferred to a third party then the insurer must make sure that they possess the required security measures to maintain confidentiality.

Government Regulatory Bodies:

- **Information Technology Act, 2000:**

The *Information Technology Act, 2000* was amended in the year 2008 after the Mumbai terrorist attack, which provided the government with the authority of surveillance, decrypting computer system and various other communication devices which help the government to receive an immediate result regarding any online suspicious activity within the country u/s 69 of the IT Act. The Act provides for the basic safety requirements to be followed by every corporate body which collect any sensitive personal information and also punishes the offender with a monetary compensation not exceeding a pre-determined amount. A private individual also comes under the purview of this Act and will be prosecuted by the court of law for the breach of data privacy either with an appropriate imprisonment sentence or monetary compensation or both, whichever the court deems fit.

The Act has been criticised for not protecting the data privacy of the people in an unimpaired manner due to lack of provisions concerning certain potential methods of data privacy breach. The need for obtaining consent before processing an individual's, an employee's or a minor's

personal information by the authority already in consensual possession of it, these are some of those significant areas where the IT Act should have looked into. With the passing of every year we are becoming more technologically advanced and becoming highly dependent on computer networks to process and store our personal data. Such progressive times desperately call for a strong legal supervisory authority to uphold data protection across the country and IT Act being in sole possession of such power with a nation-wide reach, it has to be amended with the detection of new loopholes of privacy breach.

- **Data Protection Bill, 2019:**

In 2019, the new *Data Protection Bill* was introduced before the Lok Sabha by the Minister of Electronics and Information Technology, Mr Ravi Shankar Prasad. This Bill was formed as an outcome of the KS Puttaswamy judgment passed by the Supreme Court in 2017, which directed the Union government to form a committee to build a strategic plan of action in order to provide better informational privacy to the people without infringing their right to privacy.

GLOBAL STANDING OF INDIA IN TERMS OF DATA PROTECTION:

Over the years, the world has witnessed numerous data breach which has led to the delivery of beneficial personal information of millions of people into the wrong hands. The lack of ability to prevent a data breach on such an enormous scale by well-established companies in different developed nations shows how significant it is to address the issue in hand and figure out compelling measures to safeguard these valuable information. Some of the major data breach that took place during this decade were the *Adobe data breach* in the year 2013 that resulted in the leak of credit card records of over three million of its customers and the latest one being the *Facebook data breach* in the year 2018 which resulted in a leak of personal information of nearly 50 million of its users. After being hit with the level of personal damage caused to its citizens due to data breach, several nations in Europe and the US took immediate stringent measures to avoid facing a similar situation in future. But the measures taken up by India have not been a boon as such, in fact its new measures seek to protect data by restraining the efficiency of business practices within the country and it has adopted a consent based framework which has already met failure in the 1970s.

The data protection measures adopted by India have been seen to bring a better safeguard mechanism along with a few major setbacks. The basic idea behind providing a better data protection platform within India is based upon consent based application of personal data by the data fiduciaries. But the issue lies with the method of acquiring consent by the people to process their data, as they are not fully capable of understanding the purpose behind certain requests framed by the data fiduciaries and this restrains them from providing meaningful consent. In order to become capable of regulating data fiduciaries across the country in the presumed manner, the cost of building the required equipment is definitely going to cost a fortune for every data processing business as well as the government. An estimated cost in the figures of billions needs to be met by the country to equip a similar functional security mechanism and this would significantly affect the small and medium scale enterprises due to the insufficiency of capital. India being a developing country with a majority of its business sector constituting small and medium scale enterprises has made it an even harder goal to achieve without affecting the growth of the business sector. These are the major hurdles that need to be overcome by the Indian government to make progress towards building a secure data protection platform and securing a better position globally.[8]

CONCLUSION:

India has been criticised since several decades for its lack of infrastructure to support a well-equipped data protection mechanism and it certainly has taken different initiatives to achieve that goal but the expected result in practice is yet to be seen. Firstly, I would like to lay down the drawbacks observed in the PDP Bill of 2019 which empowers the state with an excessive amount of power for regulation without clearly defining the limits of exercising such power, data fiduciaries must be held liable for their wrongful acts but not by restricting all potential acts that could lead to misuse of personal data and the attempt to implement a consent based data processing mechanism is ineffective as people are unable to provide meaningful consent.

The PDP Bill of 2019 must be reintroduced before the parliament after making a few significant changes with its prevalent provisions and such change is believed to be too crucial to bring the estimated level of data protection. The expected changes in the Bill that would truly help in fighting against the catastrophic act of data breach could be brought by

[8] Lukasz Olejnik, India's Data Protection Bill Threatens Global Cybersecurity, Wired, Available at https://www.wired.com/story/opinion-indias-data-protection-bill-threatens-global-cybersecurity/

beginning with a different approach to grant supervisory powers to the state wherein this time these powers could only be exercised within clearly defined limitations within the statute and follows a consultative process. Another significant aspect to be kept in mind is to avoid taking any such data protection measure that would lead to restrict the business within India from taking innovative steps and become more efficient. Finally, the idea of localisation of data is one of the best decisions taken by the committee that would help the DPA (Data Protection Authority) to conduct better surveillance and it has also restricted the localisation of critical personal data which is cost-effective but this level of cost-effectiveness is not reasonable for the small and medium scale enterprises. Hence, a further deduction in the cost of abiding by these rules would be well appreciated.

The government is trying to implement new provisions pertaining to data protection where people could give their consent individually for every action taken by the data fiduciaries in relation to their data and these consent based activities would be supervised by the relevant authorities established by the government i.e. the Data Protection Authority. It is expected to bring a positive change in the present state of data protection in India and it would be even better if the government realises the costs going to be incurred to build the estimated infrastructure across the country and support the smaller business with adequate financial aids which would help in speedy implementation. All the above recommendations discussed regarding the Bill would definitely help in achieving the estimated goal and as this paper has argued, the government should focus on taking feasible measures that would protect the privacy of every individual rather than forcing a discriminatory laws upon people that would eventually affect the economic as well as the overall growth of the country.