RECENT JPC REPORT INTRODUCES FURTHER CHALLENGES TO DATA PRIVACY IN INDIA

INTRODUCTION

The information technology era runs on the data oil. It is not surprising to know that there are 4.88 billion users of the internet today which makes it to nearly 60 percent of the global population. Concerning India, it has 540 million active internet users so far, still, the country lacks data protection legislation. It is governed by the Information Technology Act, 2000, Telegraph Act,and the new IT Rules, 2021 for data breaches and privacy concerns.

Data privacy concerns have grown manifold with the rise in the data breaches by social media platforms like Facebook, Twitter and which nowadays has a popular food chain too, Domino's pizza, in which orders of 18 crore people's data was leaked which involved their name, address, mobile, email, etc. Sharing of data by the people on these companies is done keeping in mind, that such reputed companies are built on the edifice of trust, and they will not hamper their privacy. Hence, this wide amount of data sharing is not looked at through the lens of doubt or concerns of privacy by most individuals. In times of data breaches that have personal details, loss of intricate personal information can lead to threatening consequences, if misused.

Tracing back the history, an Expert Committee on privacy was first headed by Justice A.P. Shah who presented a report in 2012, which serves as an influential document for setting up both international & national privacy standards. The need to bring about data protection legislation was strongly felt in the year 2017, which brought forth the landmark judgment of K.S. Puttaswamy vs. Union of India which had recognized privacy as a fundamental right. Following this, the Expert Committee chaired by Justice BN Srikrishna laid down the report on Data Protectionin 2017. The Personal Data Protection legislation was drafted in the year 2018. Later the bill was sent to the Joint Parliamentary Committee (JPC), which has laid down the report before the Parliament after reviewing the 2019 legislation on 16th December 2021. The report has been laid down along with finalized Data Protection Bill, 2021 by the JPC.

Major Changes Introduced By JPC

The key provisions introduced by the JPC, are changes in its name from the Personal Data Protection Bill, 2019 to Data Protection Bill (DPB), 2021. This change was done to make the bill inclusive of all types of data as the bill recognizes both personal and non-personal data. It has

raised concerns about the financial transactions done through the SWIFT network and suggested the development of alternative systems similar to Ripple (USA) and INSTEX (EU), to be developed in India. This recommendation by the panel was done to wipe out the existing privacy concerns of the financial data of the citizens of India, which has been compromised widely. Further, an alternate payment system that will be developed in India would ensure not only privacy but also give a boost to the domestic economy as well.

The committee has requested that the government ensure that a mirror copy of sensitive and vital personal data, which may already be maintained by foreign organisations outside the nation, is brought back within a set time frame. It has also requested that the laws for data localization be fulfilled to the letter and spirit of the legislation.[i]It directed the government to establish a formal certification process for all digital and IoT (Internet of Things) devices, which would also ensure the integrity of all such devices in terms of data security. These recommendations laid down an extensive policy to develop an alternate payment system, and the inclusion of a system that supports both local businesses as well as start-ups in the future. These key provisions will be fruitful in the long run.

Is Regulation of Social-Media Required?

The Social Media Regulation is also included by the JPC committee which has provisions similar to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021").Sub-Rule 1 and 3 of Rule 9 have been stayed by the high courts of Bombay and Madras, as they take away the independence of media due to excessive control by the government.Hence.The IT Rules, 2021 regulate social media organizations that predominantly facilitate online interaction between users as "social media intermediaries." The term "intermediaries" is important because, under the IT Act, such businesses are exempt from liability under section 79 of the IT Act, 2000 for user-generated content if they meet certain legal requirements.

The JPC report attempted to replace the term "intermediaries" with "platforms," indicating that such organizations can be recognized as publishers and held accountable for the information they host. These provisions were much needed but the issue is that this bill is about data protection and not social media regulation which is presently being covered under the IT Rules, 2021. This will, in turn, bring two regulatory laws addressing the same issue differently, adding to the already existing burgeoning task of regulating social media companies.

Consent: The Cause of Concern

Consent is pivotal for privacy protection all around the world. Processing of data without express consent is an infringement of the right to privacy globally unless it is prohibited by the very law. Clause 11 of the DPB, 2021 establishes consent as the foundation of any privacy law but sub-clause 6 imposes a penalty in case the data principal withdraws consent without any legal basis. On the contrary, article 7(3) of the GDPR of the EU, vests the people with the right to withdraw consent at any time and does not impose any penalty for it.

Clause12 further dilutes the provision of consent that was envisaged in Clause 11. Section 12 includes grounds where consent may not be required such as for providing any service or benefit [under Clause 12(a)(1)] or for issuance of any license or certificate[under Clause 12(a)(2)] or where the processing of data is necessary under the order of the tribunal [under Clause 12(c)]. These provisions continue to give the state the right to process personal data without consent which is a serious concern.

Certain aspects of data portability should be also clearly laid out in the final version of the Data Protection Bill, such as intellectual property ownership of the data transferred and whether data generated includes derivative data which could be a dilemma for the online businesses sharing analytical data. Additionally, rather than diluting clause 12 and inserting the constraints of proportionality and legitimate state, the objective of non-consensual processing of personal data is being sought. This in turn backfires the privacy test laid down by Supreme Court in Puttaswamy's judgment. This principle of necessity will be evaluated as per the convenience of government as it has established itself contrary to the maxim *Nemo judex in causa sua.*

Overarching State Powers

The bone of contention that subsisted in the form of clause 35 of the Personal Data Protection Bill, 2019 (which allowed sweeping powers to the central government and exempted certain agencies under the bill) has been retained by the committee in the new DPB, 2021 also. The JPCgave the rationale that this clause was for "certain legitimate purposes" and also said there was precedent in the form of the reasonable restrictions as enshrined under article 19 to curtail the liberty of individuals in the national interest and that the same was under the landmark Putttaswamy Judgement as well.[ii]

The central government had been given wide powers with regards to the appointment of the Data Protection Authority (DPA), in the Personal Data Protection Bill, 2019. Further changes made by

the JPC also add to the powers of the executive as it employs the Attorney General, an independent expert, a director of an IIT, and a director of an IIM to appoint the DPA. The problem subsists as their appointment is also done by the will of the executive. Although it has the brightest minds of the country, the independent functioning of these authorities is still in question as it is difficult for them they will defy the authority appointing them.

In the employer-employee relationship, the employer stands in an advantageous position in comparison to its employees. The activity of gig workers is closely monitored by their employers allowing them to further extract a large amount of the data of their online activity and subjects them to be at the mercy of their employers. For example, Zomato has terms in their partner delivery contracts in which they have the right to access, analyze, process, and store the data of their employees. However, the committee has laid down that unnecessary processing of non-consensual data of the employees by the employers should not be done, which is indeed a welcoming step. However, Social Security Code, 2020, recognizes Gig workers as employees but the code has overlapping definitions which add to the complexity of its implementation. For example, it ignores domestic work, which is performed by a large percentage of women who are engaged through platforms like Urban Company. As a result, both the legislation will fail to provide the rights to women Gig workers.

Is The Data of The Children Safe?

A much-needed laudable step added by the committee is with regards to the data processed by the online platforms which now includes that children can also revalidate their consent when they become majors. But the JPC has done away with the guardian data fiduciary provision, citing it is not required. This will ensure restriction in tracking the data of children which would be a remarkable step. Data fiduciary can discover they are dealing with a child by involving a system verifying the age which in turn requires everyone to confirm that they are an adult and further defeats the purpose.

Furthermore, it has also suggested the removal of a key principle that is "in the best interest of the child" which has its roots in Article 3 (1) of the International Conventions on Child Rights of which India is a signatory as well. The committee explained its decision stating it was done to avoid any reconsideration that may be sought under the garb of the best interest of the child by the platforms. Every data controller's action must be guided by the best interests of the child, and there must be a level of protection beyond which no user, particularly a child user, falls.[iii] The data protection commission of Ireland has laid stress on the principle of the best interest of the child

to regulate their data, through a public consultation report which is in line with the GDPR. These suggestions need reconsideration as the best interest of the child is the very basic legal principle that JPC seeks to remove.

Do We Have TheRight To Be Forgotten In India?

Right to be forgotten includes delinking of the personal data or relevant information related to the data principal accessible through search, websites, social media platforms or any public platform to be removed. In short, it allows individuals to delete their personal data from the internet. In the DPB, 2021, it has been included under clause 18; however, it is yet to receive the force of law. It is well known that the adaptation of this right in India has been inspired by the General Data Protection Regulation of the EU. The recent case of Jorawar Singh Mundy vs. Union of India has also given a nod, from the end of the judiciary that the right to be forgotten is under the ambit of the right to privacy which is a fundamental right.

The misuse of this provision haunts as the question that next comes up is who gets to decide what can be removed and what information is in the public interest? For India, the right to be forgotten in Clause 18 is limited by the data fiduciary's obligation to respond to these rights. It may even decline a request for such removal whereas in the EU, in a recent case, it was held that it is upto the platforms to decide. Court of Justice of the European Union-backed Google and held that a search engine's "right to be forgotten" did not require it to remove search results from all of its domains. This provision in India can be misused by censoring relevant information in the public domain.

Conclusion

Overall, the committee has provided a twenty-four-month period for the implementation of the draft. It has been silent on the issues of data collected before the bill came into force, how that data processing will be affected by its enactment and what measures should be taken to bring such processing following the provisions of the bill. While the JPC Report and the 2021 Bill make advances and address several challenges that people face in today's digital world, they have also been criticized. Privacy and data protection take precedence in the digital age, and they must be afforded the same level of security. But there are a few loopholes in the bill, as discussed earlier which if go neglected will defeat the purpose that was intended to serve by this framework. However, when fully implemented, it will bring India's data protection rules in conformity with

those of other countries. As a result, major companies would also begin to prepare for adherence to the data privacy laws of India.

---

[i]Committee of Experts under Justice B.N Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians.," 2018, 21.

[ii]Committee of Experts under Justice B.N Srikrishna, "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians.," 2018, 133.

[iii]Rep. *Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing*. Dublin, Ireland: Data Protection Commission, Ireland, 2021,14.