CRITIQUE OF THE PERSONAL DATA PROTECTION BILL, 2018

-Venkata Sai Aditya Santosh Badana*

ABSTRACT

The expert committee chaired by Justice B.N. Srikrishna in its final report aptly titled 'A Free and Fair Digital Economy– Protecting Privacy, Empowering Indians' submitted to the Ministry of Information Technology has embarked upon a draft 'Personal Data Protection Bill, 2018', that could structure the data protection framework in India for decades to come.

The bill is a host to several structural reforms including amendments to several Legislations for the harmonious interpretation and birth of new rights, such as Data Portability, Data Protection, Impact Assessment and an omnibus enforcement. A quasi-judicial agency, the 'Data Protection Authority' is also proposed. The bill also calls for imprisonment terms in the event of violations of sensitive personal data and hefty penalties in case of non-compliance. The focal point of the bill is 'informed consent', which irrefutably forms an integral test before imposing penalties. Additionally, the Competition Commission of India has been empowered to regulate the combinations of data processing entities, which fall short of the turnover thresholds. While the practical utility of the European Union's General Data Protection Regulation (hereinafter EU GDPR) is yet to be seen, the bill is drafted in a way to ensure that it passes the espoused adequacy test of the Court of Justice of the European Union (hereinafter CJEU), and not to stifle the proliferation of digitalisation in India.

It is in this backdrop, that we intended to author this doctrinal paper which is innately structured to elucidate the nuances and the ramifications of the bill on Aadhaar Litigation and State Surveillance. An intricate emphasis has been laid down over the infirmities and shortcomings of the existing bill. Given the infancy of the bill, one can only hope that the bill remains flexible to alterations in the light of global experiences.

*Student, ICFAI Law School, Dehradun.

EXTENT OF APPLICATION OF THE DRAFT BILL

The definition of 'personal data' is extremely wide in comparison to the 2011 'sensitive personal data' of individual rules.[1] Barring a few provisions, the instant bill has application to manual storing and processing of personal data. Thus, several non-digital businesses such as small grocery stores, handling even non-sensitive personal data are likely to be burdened with huge compliances, unless the authority provides exemptions.[2] Notably, data of sensitive personal nature is treated differently, i.e., placed on a higher footing, mandating higher standard of compliance, as well as explicit consent for its processing. For the purpose of data localisation, an additional category of information is identified, i.e., 'critical personal data', however, the definition of the same did not find its place in the bill. Section 3(35) of the instant bill outlines "*sensitive personal data comprises of financials and health information, sexual orientation etc.*"

Section 3(29) of the bill attempts to define 'Personal Data' in line with European standards as, "*data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information*".

The bill was not only extended to the processing of personal data collected within the territory of India and collected by Indian citizens/companies, but is also designed to have extra territorial application. It is stretched to the processing of data-by-data fiduciaries or processors of data principals not present within the territory of India; if such processing is:

1. in connection with any activity which involves profiling of data principals within the territory of India, or
2. in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India;

The bill fails to comprehensively define what constitutes 'carrying on business in India'. To exemplify, the Australian privacy principles[3] without defining 'carrying on business'

[1] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011.

[2] Nishith Desai Associates, 'New Data Protection Law Proposed in India! Flavors of GDPR' (*Nishith Desai Associates*, 30 July 2018) <https://nishithdesai.com/information/research-and-articles/nda-hotline/nda-hotline-single-view/article/new-data-protection-law-proposed-in-india-flavors-of-gdpr.html> accessed 2 August 2018.

[3] Privacy Amendment (Enhancing Privacy Protection) Act 2012.

have interpreted to include commercial enterprise, 'systematically and regularly with a view to profit' or to embrace 'activities undertaken as a commercial enterprise in the nature of a going concern, i.e., activities engaged in for the purpose of profit on a recurring basis'.

The bill therefore integrates the principles of nationality and territoriality with the rationale to extend the Data Protection Authority's jurisdiction not only to personal data of persons present in India; but also to personal data processed in India by foreign entities and personal data processed by Indian companies. The bill is an earnest attempt to maintain proportion between seeking to bring under its purview the applicability of the bill to the personal data of foreign residents,[4] and at the same time has made certain notable exceptions to prevent stifling of data processing activities in India.

For instance, the definition of 'personal data' is not limited to Indian residents and citizens as section 2 of the instant bill employs a method of having territorial nexus with India for establishing jurisdiction. Under section 2, if any person or entity within India processes the data, then the provisions of the bill will apply. This step endorses the ideology that India is seeking to provide an equivalent level of data protection to the data of foreigners, hence increasing the chances of gaining 'data adequacy' status from the European Union.[5]

Nonetheless, the expert committee took cognizance of the requests of the domestic data processing stakeholders under section 104 of the instant bill, which grants the Central Government the power to exempt the processing of personal data of data principals located outside India by Indian data fiduciaries, if pursuant to a contract executed with a person outside the territory of India.[6]

NOTICE

Under the bill, the data fiduciary is required to provide a data principal with a nebulously written adequate notice, prior to the collection of personal data as enumerated below,

1. Comprehensively and elaborately detailed information in multiple languages, must be provided in relation to the personal data being collected, in the event of

[4] Ministry of Electronics and Information Technology, *White Paper on Data Protection Framework for India* (2018).

[5] 'Office Memorandum No 3(6)/2017-CLES' (*Ministry of Electronics & Information Technology*, 31 July 2017) <http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf> accessed 5 November 2018.

[6] Associates (n 2).

collection of personal data, or as soon as reasonably practicable if the personal data is not directly collected from the data principal (hereinafter Notice). However, the instant bill has failed to outline such multilingual notices, which were deemed necessary.

2. Progressively, in-line with the Data Protection Act of the United Kingdom, the notice should be clear, concise and easily discernible.

Irrespective of the above, from a ground level implementation standpoint, it has to be noted that practical issues that are likely to arise, are as follows:

1. Information about enterprises, individuals with whom such personal data is intended to be shared is liable to be enlisted in the notice itself. However, what is not clear is whether the names of the particular entities are to be disclosed, or the nature and category of entities. The final draft should address these lacunae, because it is not possible to anticipate the sharing of data with by the data fiduciary
2. The collection source of personal data is also liable to be disclosed. It has to be noted that gauging the source in a decentralized data-clusters sharing architecture may get very unascertainable, more so, because multiple group companies or related entities maybe involved.
3. This enormity of data notices may become a source of 'data fatigue' to data principals, ultimately frustrating the objective.

Additionally, the proposed Data Protection Authority has been delegated with the power to earmark the list of specifics to be disclosed in notices. One can only hope that the Authority does not make the notice very cumbersome by an unreasonably prolix list.

According to the Council of European Law and European Data Protection Directive Laws Well, controllers of processing operations are obliged to inform the data subject in advance, about their intended processing.[7] This obligation does not depend on a request from the data subject, but must be complied with proactively by the controller, regardless of whether the data subject shows interest in the information or not.

The information must include the purpose of processing, as well as the identity and contact details of the controller.[8] The Data Protection Directive requires further information to be given where this 'is necessary, having regard to the specific

[7] Convention 108, art 8(a); Data Protection Directive 1995, arts 10, 11.

[8] Convention 108, art 8(a); Data Protection Directive 1995, arts 10(a), 10(b).

circumstances in which the data are collected, to guarantee fair processing in respect of the data subject'. Articles 10 and 11 of the directive outline, among other things, the categories of data processed and the recipients of such data, as well as the existence of the right of access to and the right to rectify the data. Where data is collected from the data subjects, the information should clarify whether replies to the questions are obligatory or voluntary, as well as the possible consequences of a failure to reply.[9]

CONSENT

The Expert Committee's White Paper has devoted a substantial time to deliberate upon discussing consent and plugging the gaps of Sensitive Personal Data or Information (hereinafter SPDI) Rules, 2011.[10] Some of the salient features edified under the draft bill are specified hereunder:

1. For collection, storing, processing of 'personal data', the consent has to be clear, specific, free, informed, and is capable of withdrawing. Each of these terms are defined under section 12 of the instant bill.
2. For collection, storing, processing of 'sensitive personal data', explicit consent is required for which the terms 'clear, specific, free and informed' need to achieve a higher threshold.

In the observations that lead up to his conclusions, Justice Chandrachud has also noted that data protection regulation is a complex issue, which needs to address how this data is being used must be protected. Fourth, data protection regulation should ensure that data is not collected in a manner that is discriminatory towards anyone.

Any viable alternative to the Consent Model must address the issues outlined above. It must ensure that data controllers, who have access to personal information of data subjects, remain accountable for the harm they cause, regardless of whether they have obtained consent from the data subject. The model must also ensure that, since privacy is a personal boundary, each individual should have the autonomy many aims.[11] The first of these aims is the individual's right to be left alone. Second and more importantly, the regulation needs to ensure that the individual's identity is protected. Third, the individual's autonomy in making decisions about the use of data about them, and their right to know to determine his own boundaries when it comes to privacy and in doing

[9] Data Protection Directive 1995, art 10(c).

[10] Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011.

[11] *KS Puttaswamy v Union of India* (2017) 10 SCC 1.

so, have the ability to circumscribe the uses to which data controllers can put his data[12]. The Codes of Practices to be issued by the Data Protection Authority are likely to provide further guidance to achieve valid consent/explicit consent.[13]

UIDAI LITIGATION

The report edifies that the State processes incredible amounts of personal data in its official capacity as a data fiduciary. Hence, the Government-affiliated agencies, instrumentalities are also subject to the proposed law. Under sections 13 and 14, general permission has been granted for the functions of the state under the bill for the processing of personal data.

Additionally, section 13 of bill permits the processing of personal data by the State for it to exercise its functions for the issuance of any certification, license or permit and providing benefits to the data principal by the State. Section 19 is of significance because it also provides for a general permission for the State to process sensitive personal data for the exercise of any:

1. function of Parliament or any State Legislature and
2. functions of the State for the provision of any service or benefit to the Data Principal as authorized by law.

The implication of these provisions is that prior consent of the data principal is not deemed required for the collection of personal data or sensitive personal data to achieve the State's functions. The provisions blatantly allow the functioning of the Aadhaar Act[14] and UIDAI.

However, these provisions only appear to exempt the applicability of the bill only for consent in collection of the data is concerned (i.e., they grant a lawful ground for processing) and not from the other provisions. For instance, for the purpose of section 96, they inherently do not award immunity to the UIDAI from the obligations to process data fairly under the bill, nor do they exempt the employees of the UIDAI from the penal provisions.

---

[12] Rahul Matthan, 'Beyond Consent: A New Paradigm for Data Protection' (*Takshashila Institution*, 20 July 2017) <http://takshashila.org.in/takshashila-policy-research/discussion-document-beyond-consent-new-paradigm-data- protection/> accessed 5 November 2018.

[13] European Data Protection Supervisor, 'Opinion 7/2015: Meeting the challenges of big data' (*EDPS*, 2015) <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 5 November 2018.

[14] Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act 2016.

While the report solicits certain alterations to the Aadhaar Act tailored to suit the bill, interestingly, the bill is silent on the particular provisions that are to be supplanted, while the same bill specifically suggests amendments to the Right to Information Act, 2005 and Information and Technology Act, 2000.[15]

DATA PROTECTION AUTHORITY

The instant bill also gives rise to the advent of an omnibus Data Protection Authority, much similar to European Union Data Protection Supervisor, however it's not evident and functions under the aegis of the Central Government as evident by the section 98 of proposed bill. The Authority's ambit has been widened under section 60, which includes, inter alia, enforcing the provisions of the instant bill, specifying residual categories of sensitive personal data, specifying circumstances when a Data Protection Impact Assessment needs to be undertaken, registering and notifying significant data fiduciaries and data auditors, etc. These functions are quasi-judicial and multi-faceted and rule-making.[16]

One progressive provision under bill, which garnered a lot of global attention, is the advent of 'Data Protection Awareness Fund', which will be maintained from the fines imposed by the Data Protection Authority with a motive to increase awareness on data security practices.

PENALTIES AND OFFENCES

The draft bill merely adopts the path of EU GDPR[17] in terms of financial penalties by not only proposing the imposition of fixed financial penalties (ranging from rupees five crore to fifteen crore), but also penalty based upon a certain percentage (ranging from 2-4%) of its 'total worldwide turnover' in the preceding financial year and in some specific cases pertaining to failure in implementing security safeguards, processing of children's personal data, data transfers, not taking prompt breach notification action in case of a data security breach, Data Protection Impact Assessment etc. It has to be noted that, the term 'total worldwide turnover' is not only limited to data fiduciaries but also to its group of entities.

[15] Associates (n 2).

[16] 'The OECD Privacy Framework' (*OECD*, 2013) <http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 5 November 2017.

Additionally, the bill provides for criminal penalties (ranging from 3-5 years of imprisonment) for intentional and reckless damage caused with knowledge, for certain offences, such as:

1. Obtaining, disclosing, transferring or selling (or offer to sell) of SPD, causing harm to the data principal;
2. Obtaining, disclosing, transferring or selling (or offer to sell) of PD, causing significant harm to a data principal;
3. Re-identification and processing of previously de-identified PD, without the consent of the data fiduciary or data processor.

DATA PORTABILITY

With a motive to grant data principals more control over their data, the bill embarks upon a provision titled 'Data Portability', whereby data principals may unilaterally seek their personal data in a 'structured, commonly used and machine-readable format' from the data fiduciary. The instant bill, nevertheless, is silent on technical specifications of such a format, or what would be the threshold to constitute 'common use' of the format.[18]

The personal data that is liable to be submitted to data principal must be primarily comprised of the following:

1. Data already provided by the data principal to the data fiduciary;
2. Data which has been generated by the data fiduciary;
3. Data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained.

However, the data portability provision of the bill leaves a lot to be desired, for example, it fails to mention whether the data sharing would be treated as mere transfer, or complete ownership is to be transferred. Moreover, derivative data of the 'Collected Personal Data' is not included.

[17] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data; General Data Protection Directive' COM (2012) 10 final.

[18] European Data Protection Supervisor Opinion 7/2015 of 9 November 2015 Meeting the challenges of big data [2015] <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 5 November 2018.

It has to borne in mind that Indian-based start-ups and data fiduciary entities will have to endure a higher standard of compliance, which may increase the operation costs. Further, it has been deliberated by the Commission that data portability requirements under Article 20 of the General Data Protection Regulations impose a disproportionate cost on small and medium enterprises, as they may lack the resources to understand and implement the law and systems for enabling the portability of the data. On the contrary, by imposing such a high compliance burden uniformly and without regard to market position, a uniform data portability requirement may hinder competition in the market.[19]

INFIRMITIES OF PERSONAL DATA PROTECTION BILL, 2018.

FAILURE TO REALIGN STATE SURVEILLANCE

As opposed to postulating surveillance framework separately, it was consolidated in the bill by the virtue of section 42 of the instant bill on the 'security of the State' enumerates that processing of personal data 'in the interests of the security of the State' shall be immune from the obligations of the Act, barring section 4 and section 31, if it is:

1. Authorized pursuant to a law made by Parliament;
2. In accordance of the procedure established by law;
3. Necessary for, and proportionate to, such interests being achieved.

Section 43 of the instant bill provides for very similar disclosure and 'informed consent' exemptions, if the processing of personal data is in 'the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law' and is, (a) authorized by a law made by Parliament and State legislature, and (b) is necessary for, and proportionate to, such interests being achieved.

It is pertinent here to note that, these aforementioned requisites in the section are in concomitant with the Supreme Court's outline in *Puttaswamy v Union of India (UOI)*.[20] To that effect, the bill makes the Network Traffic Analysis System (hereinafter NETRA)[21] and Central Monitoring System (herteinafter CMS) programs inefficacious, which are

[19] Fred H Cate, Peter Cullen and Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century* (Microsoft Corporation 2013).

[20] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

[21] Udhbav Tiwari, 'The Design & Technology behind India's Surveillance Programmes' (*The Centre for Internet and Society*, 20 January 2017) <https://cis-india.org/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes> accessed 10 November 2018.

deprived of legislative backing for any mass surveillance program. Nonetheless, the bill is a lost opportunity to crystalize the surveillance regulatory sphere in India.

ABSENCE OF JUDICIAL SANCTIONS

The requisites enshrined under section 42 and section 43 of the bill reinstate the surveillance framework that pre-dates the independence of India, under the Indian Telegraph Act, 1885 and the Information Technology Act.

Categorically speaking, the intent of both the aforementioned provisions is to catch all regulatory having wide amplitude, these provisions empower the enforcement agencies to intercept messages and communication on the grounds of sovereignty and integrity of India, security of the State, and public order. Section 69 of the Information and Technology Act permits the interception, decryption, and monitoring of information for the 'defence of India', without any pre-requisite of demonstrating 'public emergency' or 'public safety'.[22]

It is pertinent to note that the bill is in consonance with *PUCL v Union of India* (1997)[23], which made the position abundantly clear that these laws 'do not require any prior judicial authorization' or necessitates judicial approval to conduct surveillance, and instead place reliance on the sanctions of competent authority. In 2013, few interesting RTI replications outlined that the Union Government alone issues around 7500-9000[24] telephonic monitoring and interception orders each month, (The number of orders would have substantially increased by 2018). This clearly points out the fact that targeted surveillance can be resorted by enforcement authorities without proving an iota of substance to the competent authority.

Taking into account the unwarranted and abusive surveillance programs, in various jurisdictions such as Canada[25], United States of America (sanctioned by the FISA Court[26] under the aegis of Department of Justice), and the Commonwealth of Australia[27], judicial

[22] Raman Jit Singh Chima, 'Srikrishna On Data Protection: Need to Examine Both Bill & Report' (*The Quint*, 30 July 2017) <https://thequint.com/voices/opinion/personal-data-protection-bill-2018-Instant-srikrishna-committee-loopholes-surveillance> accessed 3 November 2017.

[23] *People's Union Of Civil Liberties v Union Of India* AIR 1997 SC 568.

[24] 'India's Surveillance State: Communications Surveillance in India' (*SFLC.In* 2014) <https://sflc.in/sites/default/files/wp-content/uploads/2014/09/SFLC-FINAL-SURVEILLANCE-REPORT.pdf> accessed 4 November 2018.

[25] Canadian Security Intelligence Service Act 1984, RSC 1985, c 23.

[26] The Foreign Intelligence Surveillance Act 1978 (USA).

[27] Surveillance Devices Act 2004 (Australia).

control is built into the domestic/foreign surveillance framework, through the process of overseeing and approving warrants and surveillance requests. However, the instant bill entirely sidesteps this issue.

UNACCOUNTABILITY OF INTELLIGENCE AGENCIES

The most prominent intelligence and enforcement agencies of India (Intelligence Bureau, Research & Analysis Wing) having been constituted by executive notification and stripped of statutory or legislative recognition, this instant bill missed the opportunity to draw the circumscribed limits of reasonable targeted sensitive data collection and creating accountability standards.

Whilst section 30 of the bill mandates data fiduciaries and significant data fiduciaries to take 'reasonable steps' to maintain transparency and section 35 recognizes data audits, there is 'no direct requirement for law enforcement agencies to submit a report to Parliament' about the nature and scale of their surveillance and interception activities.[28]

Interestingly, Justice Sri Krishna Committee's Report takes cognizance of the lack of any inter-branch oversight of law enforcement agencies, through a statute, is "*deleterious in practice… and potentially unconstitutional" and that the union Government should "carefully scrutinize the question of oversight of intelligence gathering and expeditiously bring in a law to this effect.*"[29] Nevertheless, for the reasons best known to the Committee, the recommendations enshrined in White Paper are not endorsed in the proposed instant Bill.

FAILURE TO REFORM ADMISSIBILITY OF ILLEGALLY OBTAINED ELECTRONIC EVIDENCE

Supreme Court's landmark decisions in *Navjot Sandhu*[30] and *R M Malkani*[31] outline the legal position of evidence acquired through illegal means adducible and admissible and the judicial sanction to admit tape-recorded conversations and illegally obtained evidence forecloses any reform on the law on unwarranted data collection. This position inevitably removes the incentive of enforcement agencies as well, to comply with the safeguards.

---

[28] Associates (n 2).

[29] Ministry of Electronics and Information Technology, *White Paper on Data Protection framework for India* (2018).

[30] *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.

[31] *RM Malkani v State Of Maharashtra* 1973 SCR (2) 417.

The bill lost an opportunity to supersede and turn the tables on admissibility by outlining that data collected, stored, transferred and processed through unlawful means cannot be adduced before a court of law.

UNFETTERED DISCRETIONARY POWER OF CENTRAL GOVERNMENT ON AADHAR AND SECURITY

Chapter XV of the bill enumerates miscellaneous provisions. One principal criticism is that the proposed Data Protection Authority functions under the Central Government and is not autonomous in nature. Section 98(1) allows the Central Government to issue 'such directions' to the Data Protection Authority (hereinafter DPA), "*as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order*". These 'directions' issued by the government have a binding effect on the Data Protection Authority. Residuary clauses of the instant bill outline phraseology of 'interest of national security and public order which in broader sense awards unfettered discretion to the government to issue directions aside from the safeguards mentioned in the bill.

In fact, it is also worth noting the wording of section 19(2), that permits the processing of sensitive personal data such as passwords, financial/biometric/genetic data without consent, if it is 'strictly necessary' for the exercise of any function of the State, authorized by law for the provision of 'any service or benefit to the data principal from the State'.[32] The terminology 'service' or 'benefit' have not been defined in the bill, and this provision seems to endorse the Aadhaar Scheme. In fact, data portability rights do not apply when processing is necessary for the functioning of the State.

CONCLUSION

This draft bill underlines the need of comprehensive data protection framework and susceptibility of Indian citizenry in the light of big data and predictive algorithms. While counties like the United States are grappling for having a federal statute, India has progressively set a bar. As radically progressive as this draft bill seem to be, it has to be noted that 80 Countries have already enacted a robust privacy law as of today and if this bill is not finalized for parliamentary enactment by the forthcoming general elections, the personal data of Indians may be heavily exploited, cases in point being the Brexit Referendum and 2016 US Presidency Elections. Micro-targeting of advertisements based on sensitive personal data and shadow profiling tactics were

[32] Associates (n 2).

not enshrined and more importantly this draft bill would have been a vessel to ameliorate the Computer Emergency Response Team, functionary under the IT Act to anticipate data breaches and aiding data recovery, which leaves the bill handicapped to an extent.

To conclude, while we believe that the draft bill does leave too many ambiguities to be addressed by the Central Government, including excessive obligations on data fiduciaries and disproportionate punishments, but it certainly has a share of positives. As we continue to read, debate and delve deeper into the wording of law, our views on several of these issues may evolve.