VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

SNEAK PEAK OF THE PERSONAL DATA PROTECTION BILL, 2019

- B Aparna Sundar[1]

Ever since Aadhar was made compulsory by the Government, a spate of debate arose and finally the Puttuswamy judgment made Right to Privacy as a Fundamental Right. Following the Srikrishna committee Report, The Personal Data Protection Bill, 2019 was tabled before the Lok Sabha. What does this novel Bill entail? How does this Bill protect the interests of people? How does it govern private and state enterprises? What are the rights people enjoy under this Act and what are the duties data holders ought to follow? All the above questions are answered in the research paper below. This paper highlights the relevant provisions, the blatant lacuna in some and also the implications of the provisions affecting the common man. The functioning of the Data Protection Authority and the powers vested in them is also discussed.

I. Introduction - Data Trends

Digital India is the talk of the day! Laptops, netbooks, palmtops, mobile phones, and smartphones have made it easier to transmit data. But at what cost? At the cost of violation of our fundamental right of privacy. The need of the hour is not a total ban on all social networking sites and devices but a compliance mechanism to ensure that we are not constitutionally violated of our fundamental right.

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 {hereinafter referred to as the SPDI Rules} are framed under the Information Technology Act, 2000 consisting of merely 8 provisions that

[1] Advocate, Madras High Court

deals with sensitive personal data, disclosure, reasonable security practices and procedures. Though this existed as a piece of legislature to protect data, it never really did effectively serve the purpose for the same.

The most recent Bill tabled before the Lok Sabha in December 2019, provides some solace to apprehensive netizens.

There being an increasing flow of information dissemination through the virtual media, the current social configuration demands protection of data from being misused and abused by third parties or even Governments. This paper is a study about the most recent Personal Data Protection Bill, 2019 passed on the basis of the recommendations of Srikrishna Committee Report and the Draft Data Protection Bill, 2018 also submitted by the said committee.

Ours being a largely globalized social setup with the scheme of digital India gaining utmost importance there is enormous transfer of details like name, age, personal information, likes, preferences, political lineage, bank account details, credit & debit card passwords, etc. are in public foray by websites that uses the information. There are several automated questions that the user is made to accept which by default gives permission to the websites to make use of this data for any purposes that the user is unaware of.

II. Existing Legal Scenario of Data Protection In India

The SPDI Rules, 2011 provided under Section 43A of the InformationTechnology Act holds a body corporate accountable and responsible for any misfeasance caused by their action or inaction in the implementation and maintenance of appropriate security measures and protocolsin processingsensitive personal or private data and information. The SPDI Rules provide a definition clause for sensitive personal data[2] and warrant the implementation of a framework for addressing any issue relating to such data.[3]Consequently, the Rules also provide for the enterprise collecting the information to follow a protocol for certain other requirements like consent,[4] legal purpose,[5]limitation of purpose,[6] subsequent decline of consent[7], etc., have been imposed on the entity collecting such information.

[2]Rule 3, SPDI Rules.
[3]Rule 4, SPDI Rules
[4]Rule 5(1), SPDI Rules

The most talked-about precedent on Privacy, the *Justice K.S. Puttaswamy Vs. Union Of India*[8] has brought the Right to Privacy under the ambit of Fundamental Rights. The current scenario after the Cambridge Analytica imbroglio, Google & Facebook fiascos and the dire threats of Chinese apps there has come a need to bridge the gap between privacy and electronic data, i.e., protection of data and information privacy against every entity seeking for such information, sharing such information, using such information and as a matter of fact, protection against the Government itself.

Consequent to the Supreme Court judgment, the Union Ministry of Electronics & Information Technology (MEITY) constituted an Expert Committee to research and cull out the firing data protection abuses and suggest a framework to solve them. The appointed Committee was spearheaded by the retired Supreme Court Judge BN Srikrishna and consisted of 10 members which submitted a report on Data Protection issues along with a model law, Personal Data Protection Bill on 27th July 2018. The recent Bill, 2019 is indeed a new eye-opener for Indian jurisprudence.

III. Overview Of The Bill

This piece of new legislation is one of a kind consists of 98 Sections divided into 14 Chapters and a Schedule. The apparent repercussion that this Act brings upon the citizens, other than the inherent satisfaction of privacy protection, is the compliances, requirements, pre-requisites to be fulfilled by data collectors hereinafter. Whether or not the protocols to effect the provisions are apt or protractive in nature needs to be analysed at this point.

It is very pertinent to note that currently, 80% of the most used internet sites by Indians are partially or completely owned by foreign companies particularly belong to the United States of America.[9]In such circumstances, on the occurrence of gross data violation and severe

[5]Rule 5(2), SPDI Rules
[6]Rules 5(4) and (5), SPDI Rules
[7]Rule 5(7), SPDI Rules

[8] (2017) 10 SCC 1, Order passed in WP 494 of 2012 on 24th August 2017 by 9 judge bench overruling *Kharak Singh vs. State of UP* 1963 AIR 1295 and *M.P Sharma v Union of India 1954 AIR 300*, which had earlier decided that a right to privacy is not a fundamental right under Part III of the Indian Constitution

[9]Alexa, Top Sites in India *available at*https://www.alexa.com/topsites/countries/IN (Visited on February 25, 2024)

susceptibility to privacy violation, enforcement bodies would be forced to ask information from US enterprises. It has been recorded that the United Kingdomhad acquired for data belonging to customers for around 54,000 user accounts owned by American technology companies in the year 2014.[10]In recent times, the Indian Government has called for records from Google. Out of 4,000(approximately) user data disclosure requests by Indian governmental agencies, only 54% of data was produced and a humongous 46% of data was refused to be produced.[11]

The Bill is not aimed to the effect that if local processing takes place, the perfect dream of a non-violation-protection-of-data would be achieved as even when the data is locally & physically processed in India, the question of conflict of law shall arise which may lead to endless litigation with respect to jurisdiction, applicability of law, seat of arbitration, enforcement of award, etc.Hence, a direction to hold, and safeguard the electronic data in the domestic nation could in the longer run assist in state protection and law enforcement. This is possible when a protocol can be brought about to save atleast a copy of the information submitted within local boundaries.

IV. Broad Features Of The Bill

The basic concept in the definition clause:

- Data '**Controller**' has been replaced by Data '**fiduciary**'[12]
- Data '**Subject**' has been replaced by Data '**principal**'[13] – Netizens, the person(s) who provides the data for processing.
- **Significant data**[14]fiduciaries are the ones who process huge volumes of data reiterated based on the quantity, content and sensitivity of personal data, risk & harm undertaken by the fiduciary

[10]Andrew Keane Woods, Against Data Exceptionalism, 68 *Stanford Law Review*743 (2016)
[11]Google Transparency Report, India *available at*<https://transparencyreport.google.com/userdata/overview?user_requests_report_period=series:requests,accounts;authority:IN&lu=legal_process_breakdow n&legal_process_breakdown= >(Visited on February21, 2024)
[12]Section 3(13)
[13]Section 3 (14)
[14]Section 26

The Bill incorporates Data Processing Obligations provided under Chapter II, incorporating many guidelines suggested by the Justice A.P. Shah Committee in his report submitted before MEITY in 2012. The elements absorbed from the AP Shah Committee Report in the Bill are limitation clauses on collection and purpose, notice pre-requisites, storage issues and the principle of accountable responsibility.

Sensitive Personal Data, children's data and other specificterms have been provided under Chapter IV. In the case of children, Section 16 states that the consent of the parents or guardians and the verifiability of the age of the children have been provided, despite the fact that there are exception created for theconsent of parents when it involves the counselling of a child and the protection of child rights, which however could have been further elucidated by the drafters of the Bill with details considering the hike in online counselling these days.

V. Scope of Consent

The collection of data and processing for the purposes of Aadhaar[15] falls under the ambit of Section 19(2)(a) (Chapter V) which includes the processing of data required for the function of the State or in compliance of law or order of a Court . The scope of "consent" which is a looming factor not in favour of the Aadhaar oriented processing of personal data, has not been detailed, directed or even observed in the Bill.

A detailed list of exemptions hs been provided under Chapter VIII that specifies the security needs of the state and for prevention, detection and investigation of crimes. Other exemptions are involving legal proceedings, research, and journalism& reporting. Other grounds of processing under Chapter III include that for compliance with a law or judicial order and processing necessary for an exigency like medical emergency, safety, etc.

Processing of personal data employed in agencies for recruitment, appointment, termination, attendance, or 'any activity' in relation to the assessment of employee performance has also been allowed under the Bill.[16] The important point that has to be stressed here is the depth of the processing of personal data permissible keeping in check issues relating to surveillance of workplace and even sexual harassment. Another clause provided is for the processing of data

[15]The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[16] Section 13, Bill

under the head of 'reasonable purposes' provided in Section 14. This provision is not manifestly apparent and in all probability, the Data Protection Authority of India (DPA), would come out with pertinent Notification and Rules regarding the same. This provides for myriad interactions like prevention of unlawful acts, recovery of debts, processing of data in the public domain and even whistleblowing.

Boilerplate clauses

Sufficient evidence leads to the truth that the interrelationship between notice and consent does not exist in the current scenario. Consent forms are largely extensive, standard form contracts with the only option of signing on the dotted line. Boilerplate clauses rule the internet and there is no question as to the veracity of how the netizens have mostly no option but to succumb to technological giants in case of a dispute. Hence, the people who sign these consent forms or who agree to consent to the terms & conditions do not ever read them, even if they do the terms are so abstruse to be understood thereby making fair and just consent impossible.[17] The present system of consent framework is on the patent truth that: on the internet-driven economy today, consent as a pre-requite norm is not necessary.

Keeping in regard to the above truth, well-read, educated and awarenetizens continue to frequently give their consent to the collection of personal data and resort to trends that are in violation of their personal privacy. The usage of boilerplateterms are phenomenally rampant today in the online contracts, that even adjudicatory organs have acknowledged their legal veracity, despite the unequal bargaining power of parties and questions on lack of informed consent having been obtained.[18]

The complexity with regard to the above mode of consent is that the adequacy of consent as a mode of data protection to prevent violation is feeble and insufficient. Instead of completely doing away with consent, what is the need of the hours is to have a modified framework for increasing the efficiency of consent needed to be made and the Bill provides a way for the same.

[17] B. W. Schermer, "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection"16 - 2*Ethics and Information Technology* (2014).
[18]*TradeComet.com LLC* v. *Google, Inc.*, (693 F. 2010 SDNY 370, 377),*Ftej*av. *Facebook, Inc.*, (841 F.2012 SDNY 829)

Any personal data provided can be processed only upon receiving consent. And the consent to data ought to have all the requisites of legal consent.

Free[19] Informed[20] Specific[21] Clear[22] Capable of being withdrawn[23]

Processing of only necessary information for whatever purposes shall be undertaken by the data fiduciary. Legal consequences and for the effects of withdrawal on consent given of any personal data required for the performance of an agreement shall be borne by the data principal.

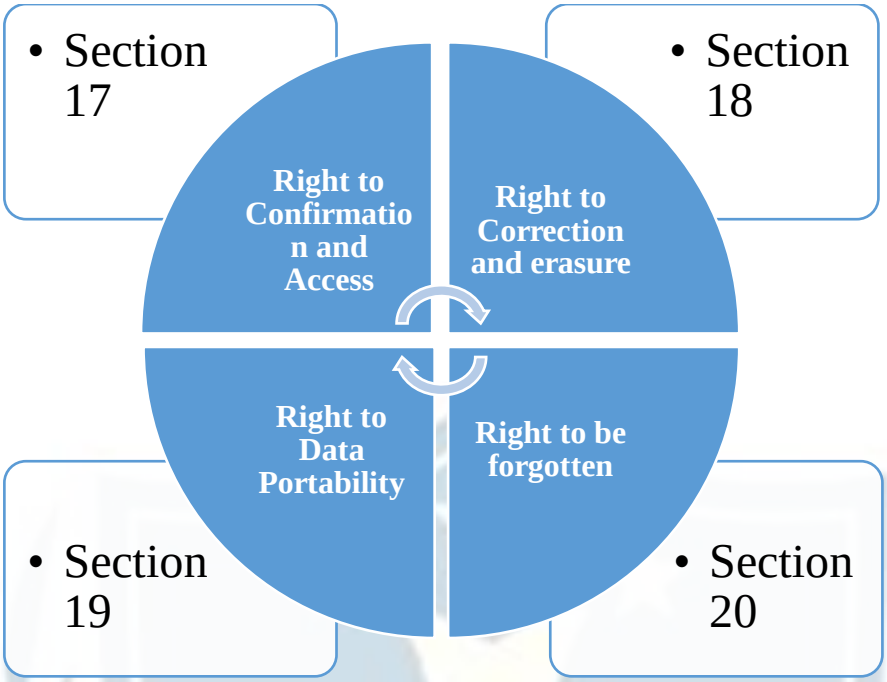
The mandate of a compulsory possession of Aadhar card for Ration shop facility, Bank Account usage, pension schemes falls under Section 12 of the Bill which states the usage of personal data for State functioning, indirectly making the Supreme Court ruling infructuous.

VI. Rights Warranted Under the New Bill

It is safe to say that the right to privacy being a fundamental right, the rights enumerated under the Bill also are fundamental rights.[24]

Chapter V of the Bill comprising of Sections 17 to 20 enumerates the rights of data principals which include –

[19]Section 11(2)(a)
[20]Section 11(2)(b)
[21]Section 11(2)(c)
[22]Section 11(2)(d)
[23]Section11(2)(e)
[24]*Justice K.S.Puttaswamy(Retd)* v. *Union Of India* (2017)10 SCC 1



These are the principal rights or entitlements that the providers of data enjoy.

The first set of rights involve the rights to access, confirmation and correction; the next set of rights bring the ambits of objections that a data principal can raise at any point and lastly, the third set of rights in its unique scope and dimension is simply the right to be forgotten.

I. Right to Access

The basis of this right is to ensure that the data principal can comprehend, process and verify the legality of personal data processing. The right to access pertains to the right of the data principal to getaccess to his personal data which is stored with the data fiduciary. This provides access for the owner of the personal data to get a set of all the personal data shared by him during the stage of consent.[25]Only at the point when the owner of the personal data knows what is the information legally or illegally has been acquired by the data fiduciary, can the data principal enforce their rights against the processing fiduciary. It is pertinent to reinforce the fact that in the lack of any right to assent, the duties set on the data fiduciary will end up as mere clichés.

II. Right to Correction

The right to correction guaranteed under the Bill is FOUR-fold

[25]Ian Long, *Data Protection: The New Rules*25 (Jordan Publishing, Bristol, 2016)

- the correction of inaccurate or misleading personal data;
- the completion of incomplete personal data;
- the updating of personal data that is out of date and
- the erasure of personal data which is no longer necessary for the purpose for which it was processed.

However, the fiduciary can deny correction on proper justification given to the principal.[26]

III. Right to Data Portability

This right is very simple as it is an enabling provision for the principal to transfer data from one fiduciary to another[27] and receive data from the fiduciary in a machine-readable format.[28]

IV. Right to be forgotten

The right to be forgotten implies the act of data principals to reduce, erase, decrease, delete, or re-enter the personal details shared by them on the internet that need not necessarily befalse, forged, anachronistic,biased, shameful, misleading and embarrassing.[29] Such revelation, need not be a repercussion of only lawful processing. Both legal and illegal processing by the data fiduciary falls under this proviso. The general principle which a data fiduciary ought to follow is lawful processing of data as well as employing just, fair and reasonable means. The definition of unfairness and degree of just means is variable and therefore if the user is of the strong belief that unfair disclosure of personal data has taken place, remedy does exisit. That is the remedy of right to be forgotten.

Data Principal's → **Data Fiduciary's**

Assessment of unfairness → **Assessment of unfairness**

VII. Sensitive Personal Data[30]

Many of the enactments of personal data protection point out the obligations to be observed while processing such data on the side of the data fiduciaries. Unfortunately, it is a frequently

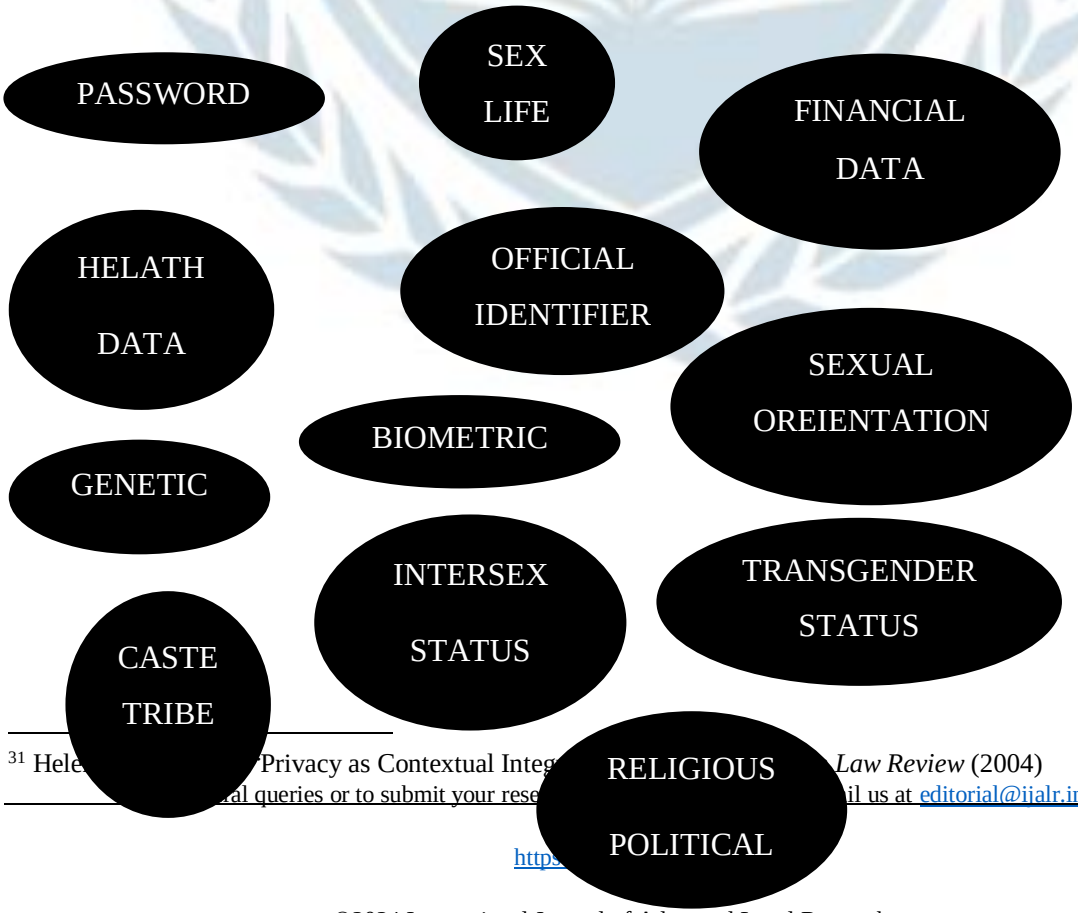
[26] Section 18(2)
[27] Section 19(1)(b)
[28] Section 19(1)(a)
[29] Michael J. Kelly and David Satola, "The Right to be Forgotten" 1 University of Illinois Law Review (2017)
[30] Section 3(35)

noted fact that in spite of lettering out such obligations, sections, provisions, etc., the processing of data pertaining to the identity of a person or the political citizenship of an individual could result in greater harm to the individual. Therefore, certain information in the nature of affecting the identity of a person the law has to be more fierce and aggressive to address such breaches in order to protect the right of the individual.

It has been observed that there is no threshold for defining of delimiting data as 'personal data' and 'sensitive personal data'. Literature does exist to show that a circumstantial approach can be adoptedwherein any data is sensitive personal data depending on the context and situation and the mode of obtaining and processing such data.[31]

The consequence of such an observance is the undeniable fact that it may increase stress on the data fiduciaries and regulatory resources as at each point of time, a rating has to be undertakento determine whether a particulardata is simply personal or is also sensitive or not, and whether or not the processing of the same would be detrimental to the individual.

The following are considered sensitive personal data and the protection of this information in regard to cross-border transfer, functions of the state, explicit consent, etc. are given a higher, stringent and strict degree of protection compared to ordinary personal data.



[31] Hele Privacy as Contextual Integ *Law Review* (2004)

SECTION 22

Thence, the primary activity of identification of kinds of sensitive data by law and clearly expressing the special duties that the data fiduciary ought to undertake phenomenally shall reduce harms caused by any data breach.As a matter of fact, depending on the cultural, social and technological dimensions of a country or a form of Government, data sensitivity varies in myriad possibilities. Despite protocols, certain critical personal data is bound to result in privacy harms despite the circumstance and need-based mode of identifying such types of data becomes obligatory.

Throughout the Bill, in most provisions regarding the protection of data a significant difference in the intensity of the protection of personal data and sensitive personal data is blatantly visible.

VIII. SPD – Children[32]

Children and Women always have held a special place for protection against men and when it comes to online-virtual protection children need to be differentiated from adults deserving a greater degree of protection.[33]The reasons for different provisions in the treatment of children under a separate head is because in general children are not capable to completely understand and comprehend the ramifications of using the internet. In the online world, the collection of data is so uncontrollable that a separate sieve for children is a necessity. Article 3 of the CRC of which India is a signatory party involves the protection and safeguarding of a child's interest and therefore mandating a separate provision.

Evidence reported reveals that children constitute 33% of internet users which calls for an alarming regulatory framework to impose stringent duties on the processing of personal data

[32]Section 16

[33]Eg.Children's Online Privacy Protection Act, 1998, USA Article 8, EU General Data Protection Regulation, 2016/679, EU Sections 34 and 35 of the Protection of Personal Information Act, 2013, South Africa

of children, most beneficial to them.[34]Only relying on parental consent, leads to the loophole of children lying about their age.The effort of the Bill in this regard has to be recognised as it provides a larger net than mere parental consent.

The provision of guardian data fiduciaries is introduced in Section 16(4). These guardian data fiduciaries are banned from processing personal data that can cause significant harm to the child[35] and the same is flexible to a certain extent when it pertains to counselling or child protective services.[36] The highlight of this provision is that when services are related to counselling or child protection, consent of parents is not required under Section 16(7).

IX. Personal Data Necessary For Purposes Related To Employment[37]

The requirement for collecting personal information pertaining to employees and job applicants by the employer is myriad. For example, employment agencies, corporations require information from individuals for the purpose of employing them. The possible information required at that time is the name, whereabouts, educational qualifications, previous experience, prior employment references that a candidate under consideration for employment might include in the prospective employee's application form. Employing agencies after recruitment would need details of their bank account, Permanent Account Number, Income Tax, Service Tax details, etc. to deposit their salaries after deduction in their respective accounts. Additional private information that may be sought by an employer may include the medical history of the employees, data relating to previous employments, previous salary and disciplinary action, if any taken in the previous employment and attendance records.In most circumstances, data collected pertaining to the above-mentioned details are done only on the active consent of the employee or prospective employee or for the requirement of legal surveillance where the law states that the organisations have to collect certain personal data under labour legal norms and modalities.[38]

[34]DordeKrivokapic and Jelena Adamovic, "Impact of General Data Protection Regulation on Children's Rights in Digital Environment",3LXIV-3 Belgrade Law Review (2016)
[35]Section 16(5)
[36]Section 16(6)
[37]Section 16
[38]Section 45(2)(c), of ESI Act, 1948 states that the employing entity will be obliged to provide for books, accounts and other documents relating to the employment, the employees and the disbursal of salaries, wages, provident fund, medical insurance Social Security Officer. Similarly, Section 13(2) (a), Employees Provident

The use of personal data for employment related issues is quite reasonable as the only information of the data principal that is processes are

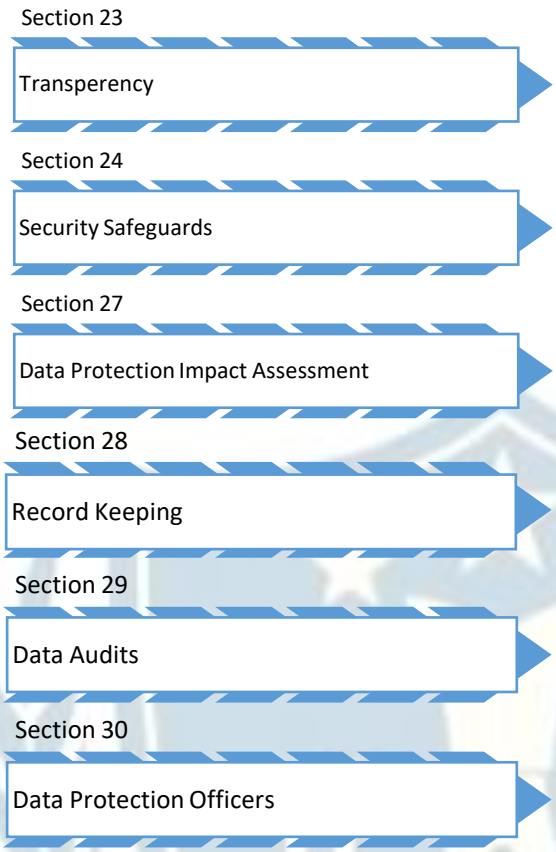
- Recruitment & Termination of employment
- Benefit sought
- Attendance
- Assessment of performance

X. Protective Measures Provided In The Bill

Mandated directions are obligated on the Data fiduciary to implement measures that **anticipate,** identify and avoid harm to the data user.[39] In order to protect the information furnished there ought to be certain policies that are to be undertaken by the fiduciary and the stringency of such measures[40] is more for the significant data fiduciaries in addition to the existing compliances for data fiduciaries[41].

The provision of significant data fiduciaries are indicated to highlight the use of special care given to data which is voluminous[42]& sensitive[43] in nature, when the turnover[44] and risk[45] involved is enormous. Another set of rules which apply to significant data fiduciaries are Sections 33, 34, 35 and 36

Funds and Miscellaneous Provisions Act, 1952 states that an Inspector has the authority to ask the employing agency to provide the required details of the employment as may be necessary.
[39]Section 22
[40]Sections 27 to 30
[41]Chapter VI – Transparency and Accountability measures
[42]Section 26 (1)(a)
[43]Section 26(1)(b)
[44]Section 26(1)(c)
[45]Section 26(a)(d)



The following information is to be made easily available & accessible under the Bill - Data collected, manner of collection, the purpose for processing, exceptional situation & significant harm, right to file complaints, rating (data trust score), info regarding cross-border transfers.[46] The risk involved with data processing and the likelihood and severity of the harm that could occur shall be avoided by

- De-identification & Encryption
- Protection of Integrity
- Prevention of misuse and unauthorised access[47]

Though the provision on transparency & security safeguards is exhaustive in nature and DPA must focus on the implementation of these sections.

[46]Section 23 - Transparency
[47]Section 24 – Security Safeguards

In the case of Cross-Border transfer of private information[48], the Privacy Bill provides that the mandates that the transfer must be effected only after satisfaction of internal approvals or procedures that shall be provided by the policies as given by the Authority and most importantly the data principal ought to

- Consent for such transfer for **personal data**
- Explicit consent for transfer of **sensitive personal data**

XI. Data Breach

The probability of breach of personal data is very high and it is bound to have grave consequences for individuals. Hence, it is a necessity to intimate data principals on such situations so that reasonable measures can be adopted to protect themselves from the harmful consequences of a data breach. However, due to problems of goodwill being affected and negative publicity, data fiduciaries may cringe from even admitting to data breaches of their customers or individuals. Therefore, a proper mandate of compliance with the Data Protection Authority when a breach has occurred has to be compulsorily provided to bring about a stringent compliance mechanism

What is personal data breach?

The three key principles of information security[49]are -

- confidentiality,
- integrity and
- availability

Not all security breaches are considered as personal data breach. The occurrences of negative repercussion on confidentiality, integrity and processing of private information that compromises the entity's capability to follow rules of the Bill will amount to breach in personal data requiring the submission of a report regarding the occurrence to the Data Protection Authority. The key ingredients in a personal data breach are**'disclosure', 'access',**

[48]Section 23(1)(g) – Cross-Border Transfer of Personal Data
[49] White Paper on Data Protection In India, http://meity.gov.in/writereaddata/files/.pdfat(Visited February 20th, 2024)

'alteration' and '**destruction of personal data'**that could be **'accidental' or 'unauthorised'**.

Notification to DPA

The sensitivity, intensity and severity of data breach vary from situation to situation. Illustration: - Unauthorised hacking of sensitive private informationkept by a Banking Company and the deletion of data of members of a club, though a breach, the former is more grave and serious than the latter. In the first situation, the seriousness of the situation warrants the issuance of notification to the DPA unlike the latter. The abuse of the process of notification ought to be avoided by overlooking harmless breaches.

The data of the compliance reporting to the DPA must most certainly include 4 things which are –

a) **nature of personal information**
b) **number of people whose data has been breached**
c) **expected repercussion of the said breach and**
d) **the precautionary actions taken by the data fiduciary to solve the breach**

On receipt of notice of such breach by the DPA, the data fiduciary shall be made to oblige to the protocols required to be followed to secure the interest of the data principal and to salvage the damage caused. The Data Protection Authority shall then be vested with the authority to record the extent of the breach and the**modality to be adopted to report the said to the data principals involved.** The violation ought to be reported to the individuals in scenarios where the rights of the principals' are violated and when some corrective action has to be taken by the individuals to mitigate the harm caused by the breach.

The authority vested with the DPA is sufficient enough to discern the circumstances on how the breach has to be handled by giving out necessary guidelines to the particular data fiduciary. It is also upon the DPA to ensure that more than enterprise-centric decisions on handling a data breach a more people-centric approach has to be undertaken by the fiduciaries. After the handling of such a breach, future corrective actions has to be mandated by the DPA to monitor and ensure that more breaches do not occur in the future besides the applicable adjudicative penal action undertaken.

XII. CONCLUSION

Recent Development inthe Global Context -

Most recently, the German Federal Constitutional Court in its order on May 19, 2020 relating to the collection of personal information and private data of the internet population living outside the German border. The Federal Court held that the Federal Intelligence Service, (alias the Bundesnachrichtendienst), is bound by the German Constitution when scrutinising telecommunications of foreign nationals and that present legal process for collecting and processing such information is violating the German Constitution. Therefore it can be understood that globally states are becoming more concerned about privacy norms.

The Road Ahead for India -

Considering the fact that this Bill is a very novel legislation in a country like India, it is to be understood that the legislation is still in its infancy and requires to be taken at the outset with all fallacies that need to be corrected in the following years to come.Also in light of the recent ban on Chinese apps by our country, it can be said that Governments are getting serious on privacy as a right. The true spirit of this legislation can be fructified in a wholesome fashion only when the Bill proceeds to become an Act and thereafter based on its implementation and effective compliance. The appointment of the Authority, the constitution of Adjudicating Officers must be without any bias. There must be a mechanism that oversees the functioning of data fiduciary as well as Government officials.