pen ACCLAIMS

Volume 6, July 2019 ISSN 2581-5504

"Aadhaar and Data Protection: Compatible or Conflicting?"

Vismay G.R.N.
The National University of Advanced Legal Studies (NUALS)

Abstract

The Aadhaar issue is a topic that has taken centre stage in public discourse over the past few months. It is a contentious area which has garnered significant public outcry among citizens, academicians, lawyers and experts. The Government however, seems adamant to get its way in this issue. The critics of Aadhaar, believe that the scheme is not in consonance with the right to privacy and that there is a large scope for misuse of personal information that is consolidated by the Aadhaar scheme in the absence of a data protection framework in place in India. The various facets of the Aadhaar scheme and the scope for misuse are issues that need to be discussed in detail and the need for a comprehensive data protection law comes to the fore in this context. Significant emphasis ought also to be given to the various provisions of law that presently exist in India with regard to data protection. The works discusses the inadequacy of existing law on data protection and why there in an increasing need, now more than ever, to have a comprehensive data protection law in the country. The need of the hour is that the government enacts a legislation that provides a regulatory framework for data protection. This ought to be done according to the well-settled, cardinal principles of data protection. The government has set up a committee under the chairmanship of former Supreme Court Judge B.N Srikrishna. to come forward with recommendations to assist the government in drafting a Data Protection Bill. The Article points out how certain recommendations of the expert committee have been ignored in order to allow the Aadhaar Scheme to circumvent the provisions of the Bill. The loopholes of the Bill have been discussed in detail and the need for the government to amend these provisions before the Bill is enacted is pointed out.

Introduction –

In recent years, there has been significant public discourse at the national level as well as on the international level, on the issue of *Aadhaar*, the privacy issues that accompany it and its constitutional validity. In this context, the need for a data protection law has been discussed widely. The word *Aadhaar* when translated to English means 'foundation' or 'base'.[1] It is essentially a 12-digit number that is assigned to the residents of India based on parameters like biometric and demographic data.[2] It aims at establishing a centralized repository of data.

The authority created to assign theses numbers is the Unique Identification Authority of India (UIDAI). The authority maintains that this scheme was rolled out in order to enable residents

[1] Vidhi Doshi," India's top court upholds world's largest biometric ID program, within limits" *The Washington Post*, September 26,2018, *available at*: https://www.washingtonpost.com/world/asia_pacific/indias-top-court-upholds-worlds-largest-biometric-id-program-within-limits/2018/09/26/fe5a95b0-c0ba-11e8-92f2-ac26fda68341_story.html?noredirect=on&utm_term=.192b4be19caa (Visited on January 29,2019).
[2] *Id.*

to enter into various transactions just by producing their *Aadhaar* numbers, without the need of producing any other further documentation. It is claimed by the Government of India that this would promote the inclusion of the marginalised sections of society and make welfare administration easier.

In a Circular[3] the UIDAI states that "the use of *Aadhaar* as identifier for delivery of services/benefits/subsidies simplifies the government delivery process, brings in good governance, transparency and efficiency, and enables beneficiaries to get their entitlements directly to them in a convenient and hassle-free manner. *Aadhaar* obviates the need for producing multiple documents to prove identity, etc."

An Act, called the Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016[4], was passed in the Lok Sabha on March 11,2016. The Act is said to aim at providing good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services to the residents of India by assigning of a unique identity to each individual.[5]

This scheme has been at the receiving end of unbending criticism from a section of society. One argument that is raised by the opposers of *Aadhaar* is that this scheme never really intended to achieve these stated goals and that the rationale behind it is actually commercial in nature. It is further contended that Aadhaar can be used by the state to carry out several activities that are violative of the right to privacy in the absence of a legal framework to regulate it.[6] Further impetus was given to these arguments when on August 23rd, 2018 the Supreme Court held in the Puttuswamy Judgement[7] that the Right to Privacy is a fundamental right under article 21 of the Constitution of India.

Several provisions of the Aadhaar Act were subsequently challenged in the Supreme Court, citing that they violate the individual's right to privacy. The Supreme Court in the Aadhaar Judgement[8] read down several provisions of the Aadhaar Act, in order to bring it in tune with the Right to Privacy. Section 57 of the Act which empowered the State or any corporate or person to use the 12-digit Aadhaar number to establish the identity of a person has been read down by the Court. The Bench stated in the Judgement that "that portion of Section 57 of the

[3] Notification for use of Aadhar under section 7 of Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act,2016. No 23011/Gen/2104/Legal-UIDAI issued on 15th September, available at https://uidai.gov.in/images/circular_section_7_of_aadhaar_act_15092016.pdf last seen 17/01/2019 (Visited on January 29,2019).

[4] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits And Services) Act, 2016 (Act 18 of 2016) *available at: https://uidai.gov.in/images/the_aadhaar_act_2016.pdf* (Visited on February 14,2019).

[5] *Id.*

[6] Rahul Bhatia," Critics of Aadhaar Say They Are Under Surveillance, Allege Government Harassment" *The Wire*, February 14, 2018, *available at*: https://thewire.in/economy/critics-aadhaar-say-surveillance-allege-government-harassment (Visited on January 29,2019).

[7] See https://www.sci.gov.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf (Visited on February 14,2019).

[8] See https://www.supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf (Visited on February 14,2019).

Volume 6, July 2019 ISSN 2581-5504

Aadhaar Act which enables body corporate and individual to seek authentication is held to be unconstitutional."[9]

Section 33 of the Act which defines the procedure for sharing demographic information and photographs was also read down with the court holding that "An Individual, whose information is sought to be released, shall be afforded an opportunity of hearing."[10]

The court also struck down Section 33(2) which permits disclosure of information, including identity and authentication of information, made in the interest of national security in pursuance of a direction of an officer not below the rank of joint secretary specially authorized by an order of the central government.[11]

In spite of these measures taken by the Indian Judiciary to protect the Right to Privacy there still exists several issues that can only be addressed by a comprehensive data protection framework. This framework needs to be brought in, in order to prevent data from falling into unscrupulous hands. This data needs to be protected against privacy breaches and from falling into the hands of those who use this personal data for carrying out activities other than the activities consented for. The fact is that where personal data is not properly contained and there is freedom to harness the data, the repercussions are likely to be astronomically toxic and deleterious.[12]

Data protection has taken the limelight due to the advances in digital technology which has facilitated the creation of databases. Data protection law is especially significant in modern times. Processing of personal data has always been an integral part of human activity. It has long been integral to the functioning of various government agencies especially since the emergence of 'welfare states.[13] The delivery of various government subsidies and services also employ intensified processing of personal data. This has commonly been justified by claiming that these services flow only to those who are in need or are legally entitled to them.[14] In recent years, fiscal imperatives have also justified the need for agencies to obtain increasing specific knowledge on their clients and customers. Personal data has been termed the 'new age oil 'due to the unprecedented economic significance it has in the modern 'information society'[15].

Digital databases allow for the reduction of storage costs. This expanded ability to store data has been complimented by an increased capacity to access and use it. In India, the government is attempting to convert/store a lot of personal data in the digitised form. This has

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *See generally* Taylor L. The ethics of big data as a public good: which public? Whose good? *Philosophical transactions Series A, Mathematical, physical, and engineering sciences.* 2016; 374(2083).
[13] *Infra* note 20, at pg. 4.
[14] James Rule, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* 43,45,48,49 (Elsevier,1980).
[15] World Economic Forum (WEF), *Personal data: The Emergence of a New Asset Class* (WEF, January 2011), *available at* : http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (Visited on January 25, 2019).

made data easier to preserve, access and share. This data includes biometric information, bank records, financial statements, income tax returns, phone numbers, subsidy schemes, public distribution systems and even information on enrolment to competitive examinations. The same technology that has expanded the role and usefulness of databases permits quick and easy reproduction of the data. 'Robots' and other computer technology can be used to download data from databases without any human intervention.[16]

It is in this context that the need for a data protection law in India becomes apparent. Since Data protection laws seek to regulate directly the exploitation of personal data, such law has the potential to interfere (positively or negatively) with many of the processes mentioned.[17]

The primary focus of data protection is to protect fundamental rights and freedoms, particularly the right to privacy, which incidentally, was recognised as a Fundamental Right by the Supreme Court of India in the Puttuswamy Judgement[18]. To make this right consequential, it is the duty of the state to put in place a framework for data protection that not only protects the individual from the dangers of informational piracy originating from state and non-state actors but also a framework that serves the common good.[19]

The Privacy Issues of Aadhaar and The Existing Mechanism to Regulate it

The Aadhaar scheme could prove to be a privacy hazard from a number of angles. When information of individuals is kept in a centralised database, the chances of it being misused increases. When one single Identification number in used to connect numerous data storehouses of individuals, the vulnerability of the information being misused increases.

In status quo, information about a person's life is stored in a number of unconnected data storehouses. This information might range from information on air travel, eating preferences, entertainment preferences, etc. The only person that is capable of connecting all these unconnected data storehouses and create a full picture of one's life is the person themselves because it is only the person who has access to all these unconnected data storehouses.

When Aadhar is used to connect all these data bases by means of a single Identification number, one can access all these different data storehouses and obtain a complete picture of the person's life. This could lead profiling of the individual to ascertain the preferences, prepossessions and the propensities of the individuals.

Data protection laws, essentially being regulatory in nature, address the way in which data is gathered, registered, stored, exploited, and disseminated. These laws relate to and permit the identification of individual physical/natural persons. It aims to safeguard certain interests and

[16] Mark J. Davison, *The Legal Protection of Databases* 2-3 (Cambridge University Press, New York, 2003).
[17] *Infra* note 20, at pg. 5
[18] *Supra* note 7
[19] A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians: *Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, available at:*
http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (Visited on February 14,2019).

Volume 6, July 2019 ISSN 2581-5504

rights of individuals in their role as data subjects.[20] Apart from privacy, these interests are generally expressed in terms of integrity or autonomy.[21] The primary aim of these laws is to control the behaviour of those who undertake the process of processing and those who work for them. They provide a deterrent to data leakages by stipulating certain sanctions and penalties[22]. It essentially imposes a security burden on the government who is the controller of the information[23].

Existing Laws in India that protect personal data

At present there in no data protection legislation in India.[24] Data Protection in India is presently given scanty and deficient coverage by a number of laws in India. These laws deal with issues that range from intellectual property, crimes, and contractual relations. However, there is growing awareness among the people whose information is collected that there ought to be a more comprehensive, all-inclusive and specific legislation that deals with data protection in India. Despite the pressure that is being exerted from internal forces, the government has deferred the passing of a comprehensive legislation. With the absence of specific legislation, the only protection that can be offered to data collected by Aadhar are by means of the existing provisions of various laws.

The primary statute that deals with this point in question is the IT Act, 2000. Section 42 of the Act only offers cursory protection against breaches in data protection. Section 43(b) is limited to the unauthorised downloading, copying or extraction of data from a computer system, essentially unauthorised access and theft of data from computer systems. Section 43(b) is limited in scope, and fails to meet the breadth and depth of protection that EU Directive mandates. The law creates personal liability for illegal or unauthorised acts, while making little effort to ensure that entities handling data, are made responsible for its safe distribution or processing.[25] Due to the inadequacy of the existing laws to provide thorough data protection, a new, specific legislation must be brought into force.

The present cycle of data protection law seems to have originated in the year 2003 in California. It was in this year that California introduced the world's first data breach

[20] A data subject is any person whose personal data is being collected, held or processed. For the purpose of this article, data subjects are the residents of India who have been allocated Aadhaar numbers.
[21] Lee A. Bygrave, *Data Privacy Law* 1 (Oxford University Press, Oxford, 2014).
[22] *Infra* note 26, at pg. 61.
[23] *Id.*
[24] Although the Personal Data Protection Bill was introduced in Parliament in 2006, it was never passed. The Information Technology Act, 2000 contains certain provisions for the protection of data but it is not comprehensive. In 2004, an Act to amend the IT Act, 2000, was close to enactment. However, this failed to happen due to the change of India's Central Government. Andy McCue, Offshore Data Protection Law Flounders, SILICON.COM, available at https://www.silicon.com/research/specialreports/offshoring/0,3800003026,39130054,00.htm
[25] Vinita Bali, *Data Piracy: Can India Provide Adequate Protection for Electronically Transferred Data?* 167 (N Sudarshan ed., 2005).

Volume 6, July 2019 ISSN 2581-5504

notification law.[26] This year is considered to be a watershed moment in the evolution of data security across the globe.[27]

In framing and enforcing a data protection law, the government must be guided by a few cardinal principles of data protection law. These principles are not mutually exclusive and considerable overlapping exists between them. There principles are essentially abstractions, however, they do carry a normative character of their own.[28]

THE CARDINAL PRINCIPLES OF DATA PROTECTION LAWS

The Principle of Fair and Lawful Processing

The primary principle of data protection law is that personal data shall be processed fairly and lawfully.[29] This principle is considered to be primary as is embraces and generates the other principles as well. Bygrave believes that the word 'lawfully' is self-explanatory. He however believes that the word fairness can mean numerous things. He is of the opinion that the word fairness undoubtedly means that data controllers must account for the interests and reasonable expectations of data subjects. He says that the collection and further processing of personal data must be carried out in such a way that it does not interfere unreasonably with the data subjects' privacy-related interests.[30]

Another facet of this principle is that data subjects must not be unduly pressured into supplying of personal data to others. Therefore, fairness implies protection from abuse by data controllers of their monopoly position.

The notion of fairness further implies that the processing of personal data be transparent for the data subjects. This not only prevents the surreptitious processing of personal data but also acts against deception of data subjects as to the nature of, and purposes for, the processing.[31] another requirement of the link between fairness and transparency is that, as a point of departure, personal data shall be collected directly from the data subject and not from any third parties.[32] This principle is especially relevant in the Indian scenario. At present the is no safeguard against the obtaining of personal data by third parties.

The Principle of Proportionality

The proportionality principle is far from unique to data protection law. It is a principle that is firmly established as a general principle in EU law, manifesting itself in a multitude of legal instruments and judicial decisions in various contexts. This principle was enumerated in the Puttuswamy judgement as well. It essentially has a three-pronged approach in EU Law.

[26] Stewart Room, *Butterworths Data Security Law & Practice* 2 (Wadhwa, Nagpur,2010).
[27] *Id*. at 3.
[28] *Supra* note 20, at 145.
[29] *Id*. at 146.
[30] *Id.*
[31] *Supra* note 20, at 147.
[32] *Id.*

Volume 6, July 2019 ISSN 2581-5504

1) Suitability – Is the data processing measure concerned suitable or relevant in realising the goal it is aimed at meeting?
2) Necessity – is the data processing measure concerned required for realising the goal it is aimed at meeting?
3) Non – excessiveness – is the data processing measure go further that that which is necessary to realise the goal it is aimed at meeting?[33]

This principle was laid down by Kaul J., in the Puttuswamy Judgement. In the context of data processing, He held that-

1) The action must be sanctioned by law;
2) The proposed action ***must be necessary*** in a democratic society for a legitimate aim;
3) The extent of such interference must be proportionate to the need for such interference;
4) There must be procedural guarantees against abuse of such interference.

The Principle of Minimality

The principle of minimality stipulates that the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is collected and further processed. The principle goes under a variety of other terms as well, such as 'data avoidance' and 'data frugality'.[34]This principle does not shine clearly or brightly in all data privacy codes, though such a requirement can arguably be read into the more general criterion of the principle of fair and lawful processing. [35]

The Principle of Purpose Limitation

The principle of purpose limitation, stipulates, in short that personal data should be collected for specified, legitimate purposes and not used in ways that are incompatible with those purposes. It is known by several other names, namely 'finality' and 'purpose specification'.[36]

The principle aims to ensure that both the way in which personal data is processed and the results of such processing conform with the reasonable expectations of the data subjects. It is also additionally grounded in the concern for ensuring that personal data is used for purposes to which it is suited.[37]

The Principle of Data Subject Influence

One of the core principles of data protection law is that persons should be able to participate in, and have a measure of influence over, the processing of data on them by others. Data protection laws rarely contain one special rule enumerating this principle in the manner formulated above. It usually manifests itself as a category of rules.

[33] *Supra* note 20, at 148.
[34] *Supra* note 20, at 151.
[35] *Id.*
[36] *Supra* note 20, at 153.
[37] *Id.*, at 154.

There are rules that ensure that the data subject is aware of the data-processing activities generally. Secondly, and arguably of greater influence, are rules aimed at making persons aware of the basic details of the processing of the data on them. This category of rules can be further sub-divided into three –

1) Rules requiring data controllers to collect data directly from the data subjects in certain circumstances;
2) Rules requiring data controllers to orient data subjects directly about certain information on their data processing operations; and
3) Rules prohibiting the processing of personal data without the consent of the data subject. [38]

Thirdly, there are rules that grant data subjects access to data that is kept on them by other entities. Most, if not all data protection laws provide for this right.[39]

The Principle of Data Quality

The principle of data quality stipulates that personal data should be valid with respect to what it intends to showcase, and relevant and complete with respect to the purposes for which it is intended to proceed. All data privacy laws contain rules directly embodying the principle, but they vary in their wording, scope and stringency. [40]

The Principle of Data Security

The principle of data security holds that personal data should be protected against unauthorised attempts to disclose, delete, change, or exploit it. A representative provision to this effect is article 7 of Convention 108.[41]

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against un authorised access, alteration and dissemination.[42]

The Principle of Sensitivity

The principle holds that the processing of certain types of data that are regarded as especially sensitive for data subjects should be subject to more stringent controls than other personal data. This principle is found primarily manifested in statutory rules that place special limits on processing of predefined categories of data.

Certain jurisdictions however lay down certain situations wherein sensitive personal data can be processed. This can be done when-

[38] *Supra* note 20, at 158.
[39] *Id.*, at 161.
[40] *Supra* note 20, at 163.
[41] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, Strasbourg, *available at*: https://rm.coe.int/1680078b37 (Visited on January 26, 2019).
[42] *Id.*

1) The data subject explicitly consents to the processing;
2) The processing is necessary for the data controller to meet legal obligations and is authorised by national law;
3) The processing is necessary for protecting the 'vital interests' of that data subject;
4) The processing is undertaken by a non-profit organisation and the data is not disclosed to third parties without the consent of the data subjects;
5) And when the data in question is manifestly made public by the data subject, or the processing is necessary for pursuit of legal claims.[43]

It is important that in a democratic legal system, the instrumentalities of the state, especially the government carries and deserves the public trust[44]. If the government does not take concrete steps to self-regulate, the chances of the crescendo of public mistrust abating are slim.

It can be said that the data subjects

are owed a duty of confidence by the Government of India. a duty of confidence can arise either in contract or in equity. A duty of confidence in equity will arise if there is actual or anticipated misuse of the information by the government by disclosing details of the data subjects to a third party without the consent of the data subject or by the actual misuse of the information by the government itself.[45] A duty of confidence can also arise where information with the necessary quality of confidence is obtained or received by a public authority acting pursuant to a statutory duty or power.[46] Private information may be considered to have the necessary quality of confidence.[47] The Aadhaar scheme essentially brings the numerous silos of personal data of an individual under the roof of a single unique identification number. It is a logically corollary that if all the private information is concentrated in a single platform, the standard of duty of confidence owed is considerably larger.

The Data Protection Bill and its Inadequacies

The Government seems to have realised the need for a comprehensive data protection legislation and accordingly drafted up the Data Protection Bill, 2018.[48] The government of India by means of an order[49] dated 31st July, 2017 constituted a committee of experts chaired by Justice B N Srikrishna, Former Judge, Supreme Court of India, to deliberate on a data protection framework in India. The committee subsequently submitted its report[50] on data

[43] *Supra* note 20, pg. 165-66.
[44] *Infra* note 26, at 273.
[45] *Supra* note 26, at 39.
[46] IRC v National federation of self- employed and Small Businesses Ltd [1981] 2 All ER 93.
[47] *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (QB).
[48] *Infra* note 51.
[49] Available at http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf (Visited on January 28,2019).
[50] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Report: *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics & Information Technology, 2018).,

protection on July 27,2018. Upon consultation of this report, the Government came out with a draft Bill[51].

This Bill has several positive features in it. The Bill has essentially been modelled on the General Data Protection Regulation (GDPR)[52], which is a document that provides for the legal framework of data protection in the EU. The draft Bill has incorporated into it several well recognised privacy principles on how notice should be sent to individuals before data is collected. The Bill prescribes explicit consent for sensitive personal data.[53] It has also been incorporated with some of the critical rights of individuals which includes the right to conformation and access, right to correction and right to data portability which go a long way in providing individuals control over their data. However, the Bill also has a number of drawbacks.

It provides for a Data Protection Authority (DPA). The Authority has been given considerable power to steer the data processing activities in both the public and the private sectors. Provision 22 of the Bill is relevant in this regard. Under this provision, the Authority has the power to specify categories under which personal data may be considered to be sensitive personal data. They include situations when –

1) The risk of significant harm that may be caused to the data principle by the processing of such category of personal data;
2) The expectation of confidentiality attached to such category of personal data;
3) Whether a significant discernible class of data principles may suffer significant harm from the processing of such category of personal data; and
4) The adequacy of protection afforded by ordinary provisions applicable to personal data.

It is curious to note that this provision, not only empowers the Authority to identify categories, but also to decide on what sort of protection measures ought to be brought in to protect this data.

It is desirable that this Authority is impartial and independent, however, section 98 of the Bill provides for the power of the Government to issue directions to the Authority that it thinks necessary for the protection of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order, and in such times as it deems necessary. The most disturbing fact is that according to provision 98(4), the decision of the Central Government on whether a question is one of policy or not, shall be final. This tilts the balance of control over data protection in the country in favour of the State. This is undesirable as the

available at: http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf (Visited on January 7,2019).

[51] The Personal Data Protection Bill,2018, *available at*: http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (Visited on January 7,2019).

[52] The General Data Protection Regulation 2016, *available at*: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN (Visited on January 7, 2019).

[53] Manaal Bhomal," Loopholes in The New Data Protection Bill 2018." *Wtdnews,* September 29,2018, *available at*: http://wtdnews.com/loopholes-in-the-new-data-protection-bill/ (Visited on January 28,2019).

Government is not restrained from implementing schemes like the *Aadhaar* scheme as the DPA effectively does not have the power to regulate policy measures and schemes put forth by the Government.

Special emphasis ought also to be given to section 13 of the Bill. This section gives a blank check to the state to process personal data without obtaining consent. Under Section 13, personal data of individuals can be processed "for the exercise of any function of the State."[54] Further Section 19 of the Bill allows for the data to be processed if the processing is necessary by the State for any function of the Parliament or any State legislature and the exercise of any function of the State authorised by law.[55] This is a rather worrying model to consider especially if the expansion of Aadhaar into so many facets (welfare programmes , IT returns, healthcare subsidies, sim cards, etc.) of our lives is considered. Under this data can be used arbitrarily by the government without the consent to the individual. We find that this is not in conformance to the diction of the Judgement delivered in The Puttuswamy case wherein the court held that there must be an informed consent which had to come from the individual.

The Bill identifies a child as a person who is yet to attain the age of 18 years[56] and provides for the collection of data with parental consent. It aims at casting an obligation on those that collect data to desist from profiling, tracking, targeting advertising at children, etc[57]. In spite of prescribing these higher order responsibilities, the Bill misses out on a foundational obligation – to ensure that the child is informed in a 'simple and explanatory manner the need for care in handling data concerning itself'.[58]

Children below the age of 18 years are frequent users of the internet.[59] They exchange a lot of data online without the knowledge of their parents. Substitution of the child's consent with that of the parents will not ensure adequate protection of children.[60]

The situation in Europe is starkly different. The General Data Protection Regulation in the EU provides that consent of children above 16 years of age is required to process their data.[61] Further the Bill does not provide for an opt out mechanism for the children whose data has

[54] Amber Sinha, "Draft Privacy bill and its loopholes" *Livemint,* July 28, 2018, *available at: https://www.livemint.com/Opinion/zY8NPWoWWZw8AfI5JQhjmL/Draft-privacy-bill-and-its-loopholes.html* (Visited on January 19,2019).

[55] Praavita, "Can the Aadhaar Act and a Data Protection Act Coexist?" *The Wire,* July 30, 2018, *available at: https://thewire.in/law/can-the-aadhaar-act-and-a-data-protection-act-coexist* (Visited on January 19,2019).

[56] *Supra* note 51, sec 3(9).

[57] *Id.,* sec 23(5).

[58] Maansi Verma, "Personal Data Protection Bill: Loopholes Pertaining to Empowerment of Children, consent and Surveillance State" *Firstpost,* Sep. 21, 2018. *Available at* : https://www.firstpost.com/tech/news-analysis/personal-data-protection-bill-loopholes-pertaining-to-empowerment-of-children-consent-and-surveillance-state-5233111.html (Visited on January 19,2019).

[59] Editorial,"83.5 per cent kids from 6-18 years active on social media" *The New Indian Express,* May 10, 2017, *available at*: http://www.newindianexpress.com/cities/hyderabad/2017/may/10/835-per-cent-kids-from-6-18-years-active-on-social-media-1603038.html (Visited on February 14,2019).

[60] *Id.*

[61] Art 8, General Data Protection Regulation (GDPR) *available at*: https://gdpr-info.eu/art-8-gdpr/ (Visited on January 27,2019).

been collected once they turn into adults. This is considered to be essential for effective data protection of an individual.[62]

Further, the Bill states that data can be processed if such processing is necessary for the exercise of any function of the State authorised by law.[63] The report by the expert committee however states that any such function of the State must necessarily be a public function.[64] This has a negative ramification. The Aadhaar Act for instance provides that The State or a body corporate or any person can use Aadhaar number for establishing the identity for any purpose. This is what has made the Aadhaar programme so problematic. If there is a denial on the part of the data subject to share their personal data, the data fiduciary denies the service that the data is sought for. This *quid pro quo* arrangement undermines the data subjects' freedom and autonomy. A framework to contemplate this has not incorporated into the Bill. [65]

It is also argued that the Bill has reinforced the concept of a surveillance state. It is argued that if the recommendations of the Committee were incorporated into the Bill, any surveillance programme that is sought to be carried out would be stopped in its tracks.[66] Instead what the Bill does is that it exempts collection and processing of data for the purpose of 'security of the State' from any rights, obligations and transparency requirement, except for "fair and reasonable processing"[67].

It has been also argued that these exceptions have been specifically designed to protect Aadhaar.[68] For instance, Section 13(2)(a)[69] removes the necessity for consent for "any service or benefit" to the data subject. This is essentially how the Aadhaar scheme operates. It makes it compulsory to have an Aadhaar number for accessing services and benefits, including subsidiaries.

Apart from these shortfalls, the Bill will also hurt businesses in India. The Bill states that every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data.[70] This may become a huge hurdle for businesses that are already operating in India. This will also have a significantly adverse impact on foreign firms in India that already have millions of users in India but store the data in their home country.[71] This may become especially undesirable for smaller businesses as they might not

[62] *Supra* note 61.
[63] *Supra* note 51, sec 13(2).
[64] *Supra* note 50.
[65] *Supra* note 61.
[66] Vrinda Bhandari ,"Data Protection Bill: Missed Opportunity for Surveillance reform" *The Quint*, July 28, 2018, *available at*: https://www.thequint.com/voices/opinion/personal-data-protection-bill-2018-draft-srikrishna-committee-loopholes-surveillance (Visited last on 27 January, 2019).
[67] *Supra* note 51, sec 4.
[68] Sruthisagar Yamunan,"Towards a surveillance state: Draft data protection law is a blow to the right to privacy" *Scroll.in,* July 27, 2018, *available at*: https://scroll.in/article/888268/towards-surveillance-state-draft-data-protection-law-is-a-blow-to-right-to-privacy (Visited last on 27 January, 2019).
[69] *Supra* note 51.
[70] *Supra* note 51, sec 40 (1).
[71] *Supra* note 53.

Volume 6, July 2019 ISSN 2581-5504

have the resources to comply with this rule.[72] This does have the short term issue of data protection in mind, however, it may prove to have adverse economic impacts in the long run.[73]

Conclusion

The Government of India holds the view that the Aadhaar scheme is essential to the streamlining of the disposal of various government services and subsidies. However, since privacy is now recognised as a fundamental right, the government is duty bound to ensure that it does not violate this right of the individuals, as well as ensure that the data of the individuals is adequately protected to prevent breaches in privacy from third parties.

It is indeed a positive sign that the Government of India has realised a need for a new data protection regime. None the less, the government needs to seriously consider the abovementioned shortfalls that exist in the Data Protection Bill if it aims at having a data protection regime that is fool proof. It should not deliberately leave a lacuna in certain questions merely for political considerations. It is important for the government to bear in mind that a data protection law in India will have far reaching consequences that extend beyond the *Aadhaar* scheme. The draft Bill ought to be modified to ensure the impartiality and the independence of The Data Protection Authority and strengthen data protection in the country. The Bill should be one which will do maximum good for the maximum number of people.

[72] *Id.*
[73] *Supra* note 53.