THE PERSONAL DATA PROTECTION BILL, 2018 in reference to JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA[1]

---THE AADHAR JUDGEMENT

ABSTRACT

"Defence mechanisms protect us. Fortresses isolate us, and far too often it begins with the former and end up constructing the latter."- **Craig D. Lounsbrough**[2]

Every Individual has a unique identity as well as a self-esteemed protection towards his/ her own selves, their known selves and their belongings. In this article the authors have discussed the importance of Protection of Individual Data which has been facing integral infringement with the advent of technology. Furthermore, the authors have put forth the government initiative and the optimism of the Judiciary in implementation of the Aadhar judgement by way of the famous case law driving towards the same and in order to ensure the privacy protection of the citizens with the introduction of various legislations and the adoption of various provisions from the global data protection regulations so enforced in the European nations.

Lastly, the authors have tried to critically analysed the similarities and advantages of both the Aadhar Act, 2016 and the Data Protection Bill, 2018 and has sought the difference between the domestic legislative representation of the introduced Bill called the Data Protection Bill, 2018 and opinionated differences in the same when compared to the Global Data Protection Regulations, 2016.

1. INTRODUCTION

1.1 Overview

India is a vast country with a population of over 1.2 billion people residing at every corner of the land. The evolution of Human being has been a continuous theory and the protection of these creatures by one another has time and again proved itself, nurturing the fate of the living beings. However, the question that arises is how we separate the identities of these people from each other. In ancient times, people used the system of Kinship in order to differentiate people of their Kin. Those who belonged to identical Kin were considered related and so they upheld once identity. Later came, the era of Castes, where people were divided into different classes and castes which helped the other people of the similar groups to identify their co- heads. However, all of these practices were unhealthy to the society in various ways such as the caste system divided men into superior and inferior category, whereas the Kinship divided

[1] Aishwariya Chaturvedi and Khajit Thukral [The Data Protection Bill, 2018 in reference to Justice K.S. Puttaswamy & Anr. v. Union of India- The Aadhar Judgement] [Amity Law School, Noida]

[2] https://www.goodreads.com/author/quotes/4172966.Craig_D_Lounsbrough (last accessed on August 4, 2019)

them into small Individual units. Secondly, these systems preached the group identity of a men and not an individual identity, as obviously, the name of the class could not be carved on each human.

The modern Indian History and the end of the British era, established a unique process of identifying every Individual based on their Birth mark Identity, the Country they belonged and various other sub categories which proved to be more fruitful for both the administration as well as the Individuals. One such initiative is the Aadhar Initiative introduced by the Unique Identification Authority of India. The Authority believed that every individual is a unique being in itself and thus shall be identified by his/ her unique persona; hence, the Aadhar India initiative was flagged by the government with a vision to empower the residents of India with a unique identification and to provide such digital platform that would help them authenticate themselves anytime and anywhere.

Further, Right to Privacy, morally, is the utmost basic right of the every living organism. Whether it be human beings or animals, interruption and interference into an individual's personal chorus of life is deeply criticized. The Indian Legislation lacks to provide protection to such Individual's data privacy policy, however, till date it has been interpreted that Article 21 of the Constitution of India, which deals with Right to Life and Personal Liberty, also includes the Right to protect of Individual Privacy, but the same has always been deferred upon. Though measures have been taken to amend the existing legislations to protect the integrity of an Individual in case of any harm to the person, no such provisions have been made to protect the Private property rights of an Individual, especially when it comes to an Individual's personal information or personal data being infringed by the social media havocs. In a recent measure, The Parliament of India has introduced a measure that shall protect the privacy right of Individual's especially with regard to social media haphazard of Data Misuse of each Individual and whether such provisions have just been copied from the International Protection Regimes and Legislations or whether such has been interpreted and implemented into the Bill inter alia the Indian Citizens.

2. THE REFERENCE

2.1 The Aadhar Bill, 2016 now called the Aadhar Act had undergone trek of circumstances and challenges in its flagship since the year it was introduced. By the Unique Identification Authority of India[3] (hereinafter mentioned as UIDAI). In the journey of a decade the legislature introduced two separate bills, a detailed analysis of the was done by the Standing Committee, multiple challenges were filed in the Supreme Court and fierce debates took place in the Parliament before the Aadhar Bill could get its assent from the President, to flourish itself as a lawfully embedded legislation.

The process below is a detailed time- line of the birth to the maturity period of the Aadhar scheme (2006-2016):

[3] The Unique Identification Authority of India is a statutory authority established under the provisions of Aadhaar act 2016 by the Govt. of India under the Ministry of Electronics & Information Technology https://uidai.gov.in/about-uidai.html (last accessed on August 4, 2019)

- **3rd March, 2006**

The Ministry of Communication Information and Technology along with the Department of Information and Technology combined gave an administrative approval for the implementation of a scheme to issue a Unique Identification for the Below Poverty Line People and their families.

- **4th December, 2006**

The Constitution of an Empowered Group of Ministers[4] (EGom) combined two schemes under the heads- The National Population Register under the Citizenship Act and Unique Identification Scheme.

- **Year 2007**

The first ever meeting of the Empowered Group of Ministers took place wherein the need for creating an identity relating to the residents database was felt and this led to the creation of the Aadhar scheme.

- **Year 2009**

The Unique Identification Authority of India (UIDAI) was established under the foresight of the Planning Commission for issuing Unique Identification Numbers[5] (UIN) to the residents of India proposed by the Central Government of India.

It was also decided that the UIDAI was going to be executive in nature and hence, Mr. Nandan M. Nilekani was appointed was appointed as the first chairman of the Authority.

- **3rd December, 2010**

The UPA government introduced the National Identification Authority of India Bill, 2010 in the Rajya Sabha.

- **10th December, 2010**

The Lok Sabha referred the NIAI Bill, 2010[6] to the Standing Committee and ordered a detailed research scrutiny and a research analysis of the same.

- **December, 2011**

The Standing Committee on the Bill presented its report and rejected the fill in its first instance. The Committee further recommended the inclusion of well- defined privacy legislation and a data protection law in order to pursue the Identification scheme and also warned about the existence of certain private agencies that are being contracted for the collection of Individuals sensitive personal information.

[4] https://cabsec.gov.in/archive.php?page=28
[5] https://docs.oracle.com/cd/E12454_01/sim/pdf/141/html/user_guide/chapter5.htm
[6] https://www.prsindia.org/billtrack/the-national-identification-authority-of-india-bill-2010-1196

- **Year 2012**

A Petition against the Government was filed before the Supreme Court of India by Justice K.S. Puttaswamy (former Judge of the Karnataka High Court) wherein he contested that the Aadhar scheme does not have any legal or statutory basis and that it would lead to the infringement of the Fundamental rights of the Individuals under Article 14 and 21 of the Constitution of India.

- **Year 2014**

An order was passed in the case of '***UIDAI v. Central Bureau of Investigation***[7]**'** the petition which was later clubbed with the petition of Justice Puttaswamy's petition, by the Supreme Court asking all the agencies to revoke the order that they had or might have had passed entailing that no benefits could be availed by those who did not have an Aadhar. The order also forbid the UIDAI from sharing any information so presented to them by way of Aadhar of any Individual's database without the consent of the respective Data Subject.

- **Year 2015 (August)**

A three judge bench of the Supreme Court passed an order putting complete restriction on the rule of making Aadhar mandatory for availing benefits in the scheme of LPG and PDS and held that no rightful benefit shall be declined to any citizen claiming the reason of lack of Aadhar. The Court also threw light on the question of Right to Privacy to be included as a Fundamental Right under the Constitution.

- **Year 2015 (October)**

A five judge Bench of the Supreme Court was constituted which was seeked or giving clearance in the august order. The bench exemplified by stating that Aadhar shall not be compulsory for availing any of the benefits so vested upon the citizens especially in the schemes such as LPG, PDS, MNREGA, PM's Jan Dhan Yojana etc. The bench further asked the CJI to constitute a special bench for hearing the final arguments on the matter.

- **Year 2016**

- 3rd March: The Aadhar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Bill, 2016 [8]was introduced in the Lok Sabka as a Money Bill.
- 11th March: The Bill was given consent by the Lok Sabha with no amendments and was forwarded to the Rajya Sabha, for consideration.
- 16th March: Rajya Sabha requisite the Bill back to the Lok Sabha making amendments and recommendations. The Lok Sabha did not consider the Recommendations and passed the Bill back to the Rajya Sabha in its original form.

[7] https://uidai.gov.in/images/news/Supreme_Courts_Order_in_WP_247_277_304_of_201716062017.pdf (last accessed on August 4, 2019)
[8] https://www.prsindia.org/billtrack/the-aadhaar-targeted-delivery-of-financial-and-other-subsidies-benefits-and-services-bill-2016-4202 (last accessed on August 6, 2019)

- 25th March: President gave his assent to the Bill.
- 26th March: The Aadhar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Bill, 2016[9] was notified into the Official Gazette of India.
- The Bill was again challenged several times and the hence the case of '**Justice Puttaswamy and Anr**[10].' Stood pending in the Supreme Court.
  - Year 2018

The five Judge Bench of the Supreme Court pronounced the much awaited Aadhar judgement creating a link between the protection of Private Data and the usage of Aadhar for Security purposes.

3. THE JUDGEMENT

A 4:1 majority judgement was passed by the Five Judge Bench of the Supreme Court comprising of the Learned Chief Justice of India Dipak Mishra, A.K. Sikri, J., A.M. Khanwilkar, J., D.Y. Chandrachud, J. and Ashok K. Bhushan, J. upholding the Constitutional validity of the Aadhar Act, 2016, wherein, they barred certain provisions of the Aadhar Act related to the disclosure of Information of the Data Subject without his/ her consent, the cognizance to be taken for certain offences and the use of Aadhar databases of Individuals by the Private Entities.

3.1 PART- I

(JUDGEMENT OF CJI DIPAK MISHRA, A.K. SIKRI, J. AND A.M. KHANWALIKAR, J.)[11]

1. Any disclosure of information is prohibited under Section 33(1) of the Act[12] including identity information of an Individual or authentication records, provided in cases when the same is by an order of a competent court. It was held that this provision shall be read down with the clarification that an individual, whose information is sought to be disclosed, shall be given an opportunity of hearing. During the course of such hearing the individual has the option of objecting to the disclosure of information provided they are on approved and accepted grounds in law, including Article 20(3)[13] of the Constitution which has the Inclusion of Privacy as a right.
2. It was further held that Section 33(2)[14] of the Act in the present form shall be struck down with the future established liberty to enact a suitable provision, Although, for the disclosure of information in the interest of national security under section 33 (2) of the Act shall not be compromised with; however, for the purpose to be executed, an officer (higher than the rank of a Joint Secretary) shall be given such a power.

[9] supra
[10] https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf (last accessed on August 9, 2019)
[11] https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf (last accessed on August 12, 2019)
[12] https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf (last accessed on August 12, 2019)
[13] https://indiankanoon.org/doc/366712/ (last accessed on August 15, 2019)
[14] https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf(last accessed on August 16, 2019)

3. To avoid any kind of misuse of the Database, a Judicial Officer shall be appointed. The Court further referred that such provisions of application of judicial mind for arriving at any conclusion that such disclosure is in the interest of national security, shall be prevalent in few jurisdictions.
4. Section 7[15] shall include such 'Benefits' and 'services' which are resonant to some kind of government subsidy such as the welfare schemes of the Government targeted at a certain or particular class of deprived people, hence benefit that help the needy to survive in a basic lifestyle shall be only covered under 'benefits' etc. The expenditure for the same shall be drawn from the Consolidated Fund of India.
5. In Section 2(d) of the Act, which was pertained to authentication records, it was held that such records did not include **'metadata'** as per the Regulation 26(c) of the Aadhaar (Authentication) Regulations, 2016[16]. And hence was struck down in the judgement. However, Liberty was given to the Legislation to reframe the regulation, provided they keep detailed parameters of the recommendations of the Court.
6. It was further recommended keeping in view the Individual liberty of protection of person data that Section 47[17] of the Act which provide for taking cognizance of an offence in case of a complaint made by any statutory Authority, any officer or person authorised to do shall be amended and a provision to include the filing of such a complaint by any such individual/victim as well any other person interested whose right is being violated.
7. As far as Section 57 in its present form was concerned, it was held that it is susceptible to misuse in one or more of the following cases:

   (a) The provisions of this Section are used in order to establish the identity of an individual 'for any purpose' provided, that such a purpose is backed by any law in force. Further, if any such "law" is made afterwards, then it shall be subject to judicial scrutiny.

   (b) The purpose so defined shall not be limited to any particular law but shall be done pursuant to 'any contract to this effect' provided that such contract is not forbidden under the any law for the time being in force. It was held that this shall not be permissible as a contractual provision is not backed by a law and, therefore, the first requirement of proportionality test was not met.

   (c) The provisions of the section authorised not just the State, but also 'any private corporate body or any person' to avail authentication services on the basis of signed agreement between the parties such as the individual and any such body corporate or person. Hence, it was held that even if the legislature did not intend in the manner of the present interpretation, the aftermath of the same would enable commercial exploitation of individual's biometric and geographic information by the private or corporate entities. Thus, that part of the provision which enabled

[15] https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf(last accessed on August 17, 2019)

[16] https://uidai.gov.in/about-uidai/legal-framework/regulations/2046-aadhaar-authentication-regulations,-2016-no-3-of-2016-page-41-67.html (last accessed on August 19, 2019)

[17] https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf (last accessed on August 20, 2019)

the body corporate and individuals to seek any such authentication on the basis of a contract was interpreted to impinge upon the right to privacy of such data subjects and thus the following part of the Section was declared unconstitutional.

8. Another important issue that was answered was the mandatory linking of the Aadhar of an Individual to his/ her bank account in order to continue to avail the services of the Bank. It was held that the Court has put on the test of Proportionality in order to check whether a certain provision of the Act would lead to any infringement of the right of Privacy of any Individual. It was observed In the above mentioned aspect and was held in violation of the right to privacy of a person which extends to banking details which would further amounts to depriving a person of his property. And hence it was held that the linking of Aadhar with the bank account did not satisfy the test of proportionality.
9. Retention of data beyond the period of six months is impermissible. Therefore, Regulation 27 of Aadhaar (Authentication) Regulations, 2016[18] provided that any data fiduciary could archive the data of an Individual or a body corporate for a period extending to five years. It was held that the retention of Individual's data for such a long period of time would lead to a sense of insecurity to the personal information of the Individual and hence, the provision was struck down.
10. The Court further discussed on whether While examining the validity of a particular law that allegedly infringes right to privacy – it should apply the doctrine of 'strict scrutiny' or the doctrine of 'just, fair and reasonableness'. To solve the dilemma the court relied upon the view in case of the privacy judgment and hence, the Court preferred to adopt the doctrine of 'just, fair and reasonableness'. It was further sub- judicated that the **Doctrine of 'just, fair and reasonableness'**[19] was in consonance with the judicial approach adopted by this Court while construing the definition of 'reasonable restrictions', which state that the State has the power to impose restrictions in the matters of public interest, as per Article 19 of the Constitution.
11. There needs to be a balancing of two facets of dignity of the same individual whereas, on the one hand, right of personal dignity and autonomy are a part of the right to privacy, another part of dignity of the same individual is to lead a dignified life as well (which is again a facet of Article 21 of the Constitution[20]). Therefore, when the State comes out with welfare schemes and strives to provide a dignified life to the people in harmony and with human dignity then in this process most of the aspects of the autonomy is sacrificed, and hence, the balancing of the two becomes an important task which can only be achieved by the interference of the Courts. For,

[18] https://uidai.gov.in/about-uidai/legal-framework/regulations/2046-aadhaar-authentication-regulations,-2016-no-3-of-2016-page-41-67.html (last accessed on August 22, 2019)
[19] http://www.legalservicesindia.com/article/1519/Principles-of-Natural-Justice-In-Indian-Constitution.html (last accessed on August 24, 2019)
[20] https://www.lawctopus.com/academike/article-21-of-the-constitution-of-india-right-to-life-and-personal-liberty/ (last accessed on August 24, 2019)

there cannot be undue intrusion into the autonomy on the pretext of conferment of economic benefits.

12. The Court, while analysing the entire case facet was also of the opinion the triple test scheme laid down to adjudge the reasonableness and check the invasion to privacy of an Individual's data does not contemplate The Aadhaar scheme as it is backed by the statute, i.e. the Aadhaar Act. It was further discussed that the Act serves legitimate aim of the State towards the protection of Public interest, which has been made evident from the 'Introduction' as well as the 'Statement of Objects and Reasons' part of the Act, which reflect that the aim that the Act is being passed to ensure that social benefit schemes that are far- fetched for common people is within their reach and they could benefit from the same.
13. After analysing the Submissions of the Applicants as well as the Respondents, the Court held that it was of the Opinion, that the subject matter in the context of permissible limits for invasion of privacy such as the triple test formula which included:

(i) the existence of a legal or statutory backup;
(ii) the establishment of legitimate interest of the State, and
(iii) the test of proportionality[21]

The Aadhar Act therefore, passed all the three tests that would make it safe for enforcement and further implementation for the establishment of Individual identity and thus the Act was upheld as Constitutionally Valid.

3.2 PART-II

(JUDGEMENT- D.Y. CHANDRACHUD, JUSTICE)[22]

While giving the Judgement under the Aadhar Act, and after analysing the facts and circumstances of the Case, Justice D.Y. Chandrachud gave a dissenting judgement wherein he believed the implementation of the Aadhar Act would lead to a direct infringement of the Privacy of an Individual as there can be no test of Reasonableness as to what would constitute the usage of an Individual's data in the matters of Public Interest. In his judgement, he gave the following key points that suggested that his opinion did not construe with the judgement of the Ld. CJI:

1. He was of the opinion that adequate norms shall be laid down to define the entire procedure of the collection of an Individual's Biometric and personal data and that proper sanction shall be drafted to draw a limit of period of retention of such data based on informed consent of the Data subject. He further held that, along with specifying the time period for retention of the data, the Individuals shall be given an option to opt-out and the right to access, correct and delete data in

[21] https://barandbench.com/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches/ (last accessed on August 27, 2019)
[22] https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf (last accessed on August 30, 2019)

case the Individual is under the belief that his privacy rights are infringed by the Data Fiduciary, and hence he opined that The Aadhaar Act was bereft of the afore mentioned provisions.

2. Further, he questioned the constitutional validity of the Aadhar Act as its introduction under the Money Bill. He held that the Aadhaar Act, 2016 is unconstitutional as it fails to meet the necessary requirements to be certified as a Money Bill under Article 110(1). Of the Constitution.
3. Under the Act, the Sections 2(g), (j), (k) and (t) are over exerted, as the term "such other biological attributes" has the scope to be expanded.
4. While observing the Proviso to Section 28(5)[23] of the Aadhaar Act, which pertains to disallow an individual's access to his/ her biometric information that forms the very core of his or her unique Identification, he held that the provisions of this section are in violation of the fundamental principle, that the ownership rights of an individual's data must at all times vest with the individual.
5. Section 29(4) of the Act vests wide discretionary power over UIDAI providing that it could publish, display or post core biometric information of an individual for the purposes specified by the regulations are in violation of the Right to Privacy of that Individual and hence the nature of this section is arbitrary.
6. Further, it was held that Section 47 which adjudicated that a court can take cognizance of an offence punishable under the Act in case the complaint is made by either UIDAI or any such officer or person authorised by the Act to do so, was in violation of the citizens' right to seek remedies and thus held that Section 47 was arbitrary as it failed to provide a proper mechanism for the individuals/ victims to seek rightful remedies in case violation of their Privacy rights.

7. As per Section 23(2)(s) of the Act, a grievance redressal mechanism was formulated in case of any grievance or infringement of an Individual's right which is contradictory in nature as UIDAI in itself is the administrating body of the Aadhaar project, and that such a provisions shall lead to a compromise in the independence of the grievance redressal body.
8. The contemplating provisions of Section 23 (2) (s) leads to the absence of an independent regulatory body and a monitoring framework which could provide for a robust to safeguard the provisions of data protection and that the Aadhaar Act does not pass a muster against any challenge on the ground of reasonableness under Article 14 of the Constitution of India.
9. The extensive definitions of the expressions 'services and 'benefits' under Section- 7 of the Act enables the government to arbitrarily regulate every facet of its engagement with the citizens under the Aadhaar platform. The exclusive inclusion of the terms 'services' and 'benefits' in Section 7 is contemplation to the kind of function which is inconsistent with the right to informational self-determination. It was thus held that Section 7 exclusionary and arbitrary in nature and violates the provisions of Article 14 of the Constitution in relation to the definition of benefits for the backward classes and thus is Unconstitutional in nature and be struck down.

[23] supra

10. Further while discussing the issue of seeding the Aadhar Act to include the definition of PAN, it was held that that the Aadhaar Act in itself is unconstitutional for having been enacted as a Money Bill without holding any constitutional validity of the same and hence on the touchstone of the test of proportionality, such seeding of Aadhaar to PAN under Article 139AA[24] of the Constitution does not stand independently of the Constitution and shall not be permitted for implementation.

Hence, after analysing all the submissions of the Applicants and the Respondents, the Court had directed its judgement as per the provisions of Article 142[25] of the Constitution submitted that the existing data of the data subjects which was already collected shall not be destroyed for a period of one year and that During this period, the data shall not either be used for any purposes of any manner, whatsoever neither by the government nor by any Individual or corporate entity and that at the end of one year, if no fresh legislation is either formulated, adopted or enacted by the Union government in conformity with the principles which have been enunciated in this judgment, the data shall be destroyed.

3.3 PART-III

(JUDGEMENT- ASHOK K. BHUSHAM, JUSTICE)[26]

Justice Ashok K. Bhushan did not give a partially concurring judgement, wherein he denied the entire conclusion made by the Ld. Chief Justice of India Dipak Mishra nor did he extensive contemplate with his judgement, unlike Justice A.K. Sikri. Justice Bhushan stated that as much as it is important to implement legislation for the purpose of establishing a unique identity to the citizens, it shall not be forgotten that with the advent of technology, it is of vital importance to first safeguard the privacy of the Individuals. He also contemplated that nothing shall stand above the provisions of the Constitution and his disagreement with the enactment of the Aadhar with the help of the following points:

1. As long as the provisions of Sec 7 of Aadhaar Act, 2016, are concerned, he was of the opinion that making Aadhaar number necessary for receipt of government provided subsidies, benefits and services is not in violation of the constitutional provisions and he further observed that some cases of authentication failure shall not be made the ground to nullify the entire provision.
2. Further, it was held that Parental consent for providing any sort of biometric information of an Individual or a body corporate shall be made mandatory under Regulation 3 and any information related to demographic statistics under Regulation 4 of Aadhaar (Enrolment and Update)

[24] https://indiankanoon.org/doc/556297/ (last accessed on September 7, 2019)
[25] https://indiankanoon.org/doc/500307/(last accessed on September 9, 2019)
[26] https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf (last accessed on September 11, 2019)

Regulations, 2016 shall also be made mandatory and strict sanctions shall be made in case of non- compliance of the same.

3. After the analysis it was held that certain provisions of the Act such as Section 29 which deals with restriction on sharing information by the government agencies and Section 33 which provides for the use of Aadhaar data-base for Police Investigation and Interrogation purposes were upheld and declared found not in violation of Article 20(3) of the Constitution of India.
4. He further held that in the question of privacy infringement of an individual for linkage of the Aadhar with bank accounts as per Rule 9 as amended by PMLA (Second Amendment) Rules, 2017 shall be made mandatory and was thus upheld and was found not to violate the provisions of Articles 14, Article 19(1)(g), Article 21 & Article 300A of the Constitution.
5. The provisions contained in Section 47 of the Act which did not allow an individual to file a complaint for infringement or any offence under the Act was upheld, however, the last part of Sec 57 which was related to the grant of permission for usage of Aadhaar by the State or any such body or body corporate or person, in pursuant to any contract was held unconstitutional.

4. THE DATA PROTECTION LEGISLATION

Shortly after the enactment of the Aadhar Act, 2016 and the judgement of the Court in the case of **K.S. Puttaswamy & Anr. V. Union of India**[27] year 2018, the GoI felt the requirement for the formation of a proper legislation in order to safeguard the personal data of an Individual as well as the companies and the body corporate within the territory of India, the GoI presented the Data Protection Bill, 2018 in the Parliament in order to consulate a sanction for infringement of provisions of the Aadhar Act, 2016 and hence the timeline below justifies the adoption of Data Protection Regulation from the European Union and the difference between the same.

When the Information Technology Act, 2000 (hereinafter referred to as the "IT Act") first came into force on October 17, 2000 it had provisions related to all the cyber-crimes, however, it lacked provisions for protection of personal data and the procedure to be followed to ensure the safety and security of sensitive personal information of an individual. This led to several other amendments and bills being passed and finally The Information Technology (Amendment) Act, 2008 inserted Section 43A in the Act which notified the Information Technology (The Reasonable security practices, procedures and sensitive personal data or information) Rules, 2011[28] (hereinafter referred to as the "2011 Rules"). The 2011 Rules came out to be of absolute importance especially with regards to the ambit of the definition of Personal Data of an Individual. There were certain key features which made the bill to become an epitome of Individual Security.

[27] supra
[28] supra

4.1 The key features of the 2011 Rules:

- These 2011 Rules applies to body corporates and persons located in India. The provisions of **Section 43A** of the Companies Act provides that *'Every time a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining a reasonable security in order to protect such data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the affected person(s)*[29]
- A list of items has been provided which shall be treated as '*sensitive personal data*' such as passwords, biometric information, sexual orientation, medical records and history, credit/ debit card information, etc. However, certain exceptions were provided in case of any information which is freely available or accessible in the public domain is not considered to be sensitive personal data.
- In case a corporate body seek any such sensitive personal data it must draft a privacy policy which shall published on the website of the body corporate, containing all the details of information being collected and the purpose of usage.
- Reasonable security practices must be established by such body corporate seeking data for ensuring the maintenance of confidentiality of such data.
- The body corporate shall obtain consent from concerned Individuals for collecting such sensitive personal data in case of it usage for lawful or other necessary purpose.
- The purpose so mentioned must be clear and understandable to common people and the information shall be used only for such purposes the consent for which has been given and such data shall be retained only till the time, as required.
- Apart from keeping a check on the protection of personal data, the 2011 Rules also provide for solutions in case of dispute such as:

    1. Establishment of Grievance Office which shall be responsible to address grievances of information providers within one month from the date of such application for resolution of such Grievances.
    2. Body corporates must have an audit of the reasonable security practices and procedures implemented by it by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant up gradation of its process and computer resources.

- In case of Infringement of the Rules or any other rules so provided in any law enforced for the purpose of Protection of Data the such punishment as provided for disclosure of information in case of breach of lawful contract and Imprisonment which may be for a term not exceeding three years, or with a fine which may be Indian Rupees 5 million or with both.

Thus, it can be inferred that Section 43A[30] of the Act provides for a complete package of rights, remedies and procedure for both the Individuals as well as the body corporate to ensure that the Sensitive personal

[29] supra

[30] http://www.mondaq.com/india/x/626190/data+protection/Information+Technology+Reasonable+Security+Practices+And+Procedures+And+Sensitive+Personal+Data+Or+Information+Rules+2011 (accessed on September 23, 2019)

Information of an Individual remain protected and secure, though it was later inferred that the 2011 Rules had certain drawbacks which led to further amendments in the legislature made for Protection of Personal Data, as discussed further.

4.2 DATA PROTECTION BILL, 2018 (Introduction)

With the advent in time and technology, there felt a need to establish a proper legislation in order to provide appropriate remedy towards the threat of increasing Internet access into personal lives of Individuals and the synchrony with cyber-crimes. Hence, a Bill was introduced in Parliament in the year 2018 that proposed to bring privacy under the ambit of legislative structure. Although, this is not the first Bill on privacy introduced in Parliament, the bill is different from the previous Bills in the sense that it seeks to take consent of an individual in case of collection and further processing of his/ her personal data, mandatory. In the context of sensitive and personal information, the person must provide his or her express and affirmative consent for the collection, use, storage of any such data.

This Bill unlike the Rules of 2011, applies not only to private corporations or body corporate, but is equally applicable to state entities, government agencies or any other persons acting on their behalf. The scope of the definition of "third party" under the Bill now also includes the public authorities. This is a symbol of a significant change in law dating back from the existing regime under the IT Act 2000 and 2011 Rules in India.

4.3 Objectives of the Bill

The **Preamble** of the Data Protection Bill, 2018 reads as follows:

WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy; WHEREAS the growth of the digital economy has been meant the use of data as a critical means of communication between persons; WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy and to respect the informational privacy of individuals, and ensuring empowerment, progress and innovation; AND WHEREAS it is expedient to make provision: to protect the autonomy of individuals in relation with their personal data and to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to explicitly specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for the transfer of personal data cross-border, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish the Authority(Data Protection) for overseeing processing activities[31]*;*

[31] https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

However, Section 20(2)[32] of the Bill with respect to Sensitive Personal Data, provides that no sensitive data shall be processed for any other purpose apart from its intended use **provided** that such data may be used for welfare schemes and social protection laws. Hence, this implies that the Aadhaar scheme would also have access to a person's personal, sensitive information. This Section is analogous and contradictory into its own provisions and with the present dispute on-going at the Supreme Court and will continue to be subject of debate due the existing privacy concerns.

Although this Bill is still pending in the legislature, it can be said that it is much more in line with the stricter Global Data Protection Regulations (hereinafter to be referred as 'GDPR') norms it is unlikely to come into force until the pending litigation regarding the Aadhaar scheme[33] comes to a conclusion regarding the use of the Government of the personal sensitive data of the Residents of India.

4.4 General Interpretation

The term Data protection hereby refers to procedures, policies and provisions that are seeking to minimize intrusion or infringement into the privacy of an individual's life caused by the non- consensual collection and usage of their personal data. Different terms have been defined in this Bill such as Personal Data, Data Processing, Data Principal, Data Fiduciary, and Data Processor.

- ***Personal data***[34] *is defined as any information which renders an individual identifiable.* ***Data processing***[35] *is defined as any operation, including collection, manipulation, sharing or storage of data.* ***Data principal***[36] *is defined as the individual whose personal data is being processed.*
- ***Data Fiduciary***[37] *is defined as the entity or individual who decides the means and purposes of processing data.*
- ***Data Processor***[38] *is defined as the entity or individual who processes data on behalf of the fiduciary.*

The data fiduciary shall provide the data principal with the following information such as:

i. The purposes for which the personal data is to be processed and the categories of personal data being collected;
ii. The right of the data principal to withdraw the consent and also the procedure to withdraw for such withdrawal.
iii. The source of collection of such data if the personal data is not collected from the data principal.

[32] https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018 (accessed on September 24, 2019)
[33] https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-scheme-does-not-violate-right-to-privacy-says-sc/articleshow/65969846.cms?from=mdr (accessed on September 26, 2019)
[34] https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last accessed on September 27, 2019)
[35] supra
[36] supra
[37] supra
[38] supra

iv. The period for which the personal data will be retained (The data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed.)

4.5 Grounds for processing of personal data

The Bill of 2018 allows data processing by fiduciaries based on the consent provided by the Data Principal. In order for the consent of the data principal to be valid it has to be free and shall not be caused by anything forbidden by the law such as Coercion, Undue influence, Fraud, Mistake etc. (Section 14 to 18 of the Indian Contract Act, 1872)[39] and the data principal shall also be provided with all the required information as required in the Act for such consent. However, there are certain circumstances in which the consent of the data principal is not required, these are:

i. Any statutory function of the Parliament or the State legislature in case such information is required by the State for providing benefits to the individual;
ii. If such information is required under any law or in case of compliance with the judgement of any Court.
iii. If such information is necessary to respond to any case of medical emergency or an outbreak or breakdown of public order.
iv. If such information is mandatory for background check for the any purpose related to employment such as I case of Recruitment.
v. For any other reasonable purposes whether or not specified by the Data Protection Authority with regard to illegal or unlawful activities such as fraud detection, credit scoring, debt recovery, and whistle blowing.

4.6 Grounds for processing Sensitive Personal Data

Sensitive personal data[40] under the Bill means '*personal data revealing passwords, financial data, biometric and genetic data, caste, religious or political beliefs*'. The Data Protection Bill specifies strict and stringent grounds for processing of any sensitive personal information and also provides that such an act would require seeking explicit consent of an individual prior to processing.

However, sensitive personal data may be processed if such processing is strictly necessary for the following:

- Any statutory function of the Parliament or the State legislature in case such information is required by the State for providing benefits to the individual;
- If such information is required under any law or in case of compliance with the judgement of any Court.
- If such information is necessary to respond to any case of medical emergency or an outbreak or breakdown of public order.

[39] https://indiacode.nic.in/handle/123456789/2187?view_type=browse&sam_handle=123456789/1362 (accessed on September 27, 2019)
[40] https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last accessed on September 27, 2019)

- If such information is mandatory for background check for the any purpose related to employment such as I case of Recruitment.
- For any other reasonable purposes whether or not specified by the Data Protection Authority with regard to illegal or unlawful activities such as fraud detection, credit scoring, debt recovery, and whistle blowing.

4.7 Exemptions

The Bill although has strict compliance towards the protection of Individual data, however, it does provides exemptions to certain activities involving the data processing. It states that processing the personal data of an individual shall not amount to the specified obligations and the data principal shall not enjoy the rights defined in the Bill, if their personal data is processed for any of the following purposes:

i. In the interest of the Security of the state and public justice.
ii. In case of Prevention, investigation, detection, and prosecution arising out of contraventions of law.
iii. In case of legal proceedings in the interest of justice.
iv. For any of the research or archiving or any other statistical purposes.
v. Any other personal or domestic purposes for the matter of legal proceedings.
vi. Any form of Journalistic purposes.
vii. Manual processing of data by the small entities.

5 GENERAL DATA PROTECTION REGULATIONS- the blueprint of DPB, 2018

The GDPR in its very sense means to provide a new set of rules to the citizens of the European Union more control over their personal Data. It aims to simplify the regulatory environment for business so that so that the European Union can fully benefit from the developing economy. The Data protection norms started evolving in the European Union from the late twentieth century. It was in the year 1995 that the first directive for individual's data protection directive was adopted which was knows as the European Union Protection Directive (Directive 95/46/EC)[41] following which in the year 2012 The European Commission proposed a reform in the Rules of 1995 in order to strengthen the data protection norms and boost the digital economy in Europe. On 12th March, 2014 the European Parliament received a strong support in relation of implementing the Global Data Protection regulation and on 24th April, 2016 the Regulation was agreed upon by the Parliament and the Council and 24th May, 2016 after 20 days from the publication in the Official Gazette the GDPR came into force.

[41] https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en (accessed on September 27, 2019)

In the entire draft of the Global Data Protection Regulations[42], there are about in total 99 Articles that set out the rights for the individuals and certain obligations for the organisations that are covered by the regulation. The entire text consists of eight rights for individuals in total. The regulation also includes a new provision for fine regime and a responsibility endowed upon the organisations to obtain the consent of data subjects from whom they collect personal information.

5.1 Penal Provisions[43]

The GDPR has been for a substantial amount of its divisions has been one of the most debated elements during its passage of enactment. The GDPR has the ability to fine businesses of the regulators that don't comply with it. For eg: If in case any organisation does not process an individual's data without consent and in a wrongful manner, it shall be fined. Further, if it is so required to be appointed and does not have a data protection officer, it shall be fined. In case of a security breach, it shall be fined. However, these penalties usually depend upon the intensity and gravity of the breach of such obligations; nonetheless, the penalties so imposed are thereby expected to have a strict and prompt compliance. In the United Kingdom, these penalties are decided by the Denham's office in altercation with the Regulations wherein the GDPR provisions provide that smaller offences shall result in fines up to €10 million and/or two per cent of a firm's global turnover (whichever is higher)[44]. Those with a higher/serious degree of offences shall have fines up to €20 million or four per cent of a firm's global turnover (whichever is higher)[45]. Thus, it can be stated that these penalties are higher in monetary than the £500,000 penalty the ICO previously issue.

6. KEY DIFFERENCES BETWEEN THE Data Protection Bill, 2018 & THE GDPR, 2016

The Data Protection Regulation in India, although is being regarded as the replica of the GDPR norms in terms of various aspects such as the Definition clause, the requirement of consent for processing of personal data, the limitations of such personal data usage and the strict compliance of the regulatory provisions of the legislations. There are certain areas where the Data Protection Bill has adopted a different approach from the GDPR in various aspects, most important of which is the provisions for criminal penalties for harms arising out of such infringements and the treatment of relationship between the Data processor and its consumer. Few other differences have been listed below:

[42] European Parliament, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Pub. L. No. Official Journal L 281, 0031, 1995 https://gdpr-info.eu/ (accessed on September 28, 2019)
[43] https://gdpr-info.eu/ (last accessed on September 28, 2019)
[44] https://gdpr-info.eu/ (last accessed on September 28, 2019)
[45] https://gdpr-info.eu/ (last accessed on September 28, 2019)

Sr. No.	Grounds	GDPR,2016	DPB,2018
1.	**Applicability**	Applies to processing activities of an est. within EU regardless of whether the processing takes place in EU or not	Applies to the processing of personal data within the territory of India and to processing of PD by the State, any Indian Co., citizen, person or body of persons incorporated under Indian law
2.	**Extra-Territorial Applicability**	Extends to processing of personal data of data subjects who are in the EU by a controller/ processor not established in the EU.	Extends to processing in connection with any business carried on in India or processing which involves profiling of data principals within the territory of India.
3.	**Consent for cross-border transfer**	The data Principals consent is needed in addition to the adequacy decision by the Central Government or the approved standard contractual clauses.	The data principal's consent is needed in addition to adequacy decision by the CG or the approved standard contractual clauses.
4.	**Breach Notification to the principal data**	The controller should communicate the personal data breach to the data subject without undue delay in cases where the breach is likely to result into risking the rights and freedoms of natural persons and shall lead the violation of their private information.	The DF- not obligated to inform the DP about a personal data breach unless and until the DPA has mandated such reporting to the data principal.
5.	**Right to be forgotten/Right**	A data subject has the right to obtain erasure of their personal data from the data controller if the grounds for such erasure under the	A data principal can only prevent continuing disclosure of the data by the DF if the grounds are

	to erasure	Regulation is fulfilled	fulfilled. No provision to erase personal data.
6.	**Ownership of data**	The ownership of Data under GDPR belongs to the data subject (Data Principal).	The PDPB does not provide for ownership of data by the Data Principal/subject.

7. CONCLUSION AND OBSERVATION

7.1 Conclusion

- THE AADHAR REGULATION

The order of the Supreme Court granted the Constitutional Validity to the Aadhar Act to the extent that it could provide a number based identity to the Individuals. However, the entire timeline of the case and the judgement that followed gave a very detailed analysis of the implementation of the Aadhar Act, 2016 and what amendments were required to effectively implement the legislation that it serves the purpose of the State as well as the Citizens.

The judgement although was a majority conclusion of the Five judge bench, only had 3 judges exclusively concurring to the enactment of the Aadhar Act, 2016. There were various opinionated discussions that led to the overall scrutiny of the verdict. However, it can be concluded that the implementation of Aadhar Act would prove to be dragging the path of security towards a positive trajectory and that this would lead to the overall development of the nation.

- THE DATA PROTECTION REGULATION

The European Union has recognized the rights of Individuals with respect to the protection of their personal data for a while now, whereas, The Indian concept of separate Data Protection legislation which still lacks the provision for Cross- sectorial law for data protection. Nevertheless, the provisions of the Data Protection Bill would increase the data protection obligations and prevent the risk of privacy infringements of Individual's data. The Bill would also provide wide range economical protection, management and collection of data of the Individual, business and the foreign corporations working within the territorial projections of India.

While the EU already had a Directive regime of 1995 for the protection of Data, the Bill of 2018 would be a novel for the Indian Legislature framework. The implementation cost for the framework would be more pricy and time consuming for the Indian Legislature as a part of enactment process. The Bill has already been in conflict with various pending legislations in various Courts in India, which would be

havoc in order to regularize the general privacy regimes. In addition, no systematic analysis of the Bill has yet been conducted to provide a proper an accurate analysis of the impact of such legislation in India.

To conclude, the adoption of specific design of institutional choices by India is likely to have a direct or indirect impact on India's economy. While the GDPR has a numeric calculated projection of the implementation of privacy regulations, parts of the Indian economy is going to face huge impact of the economy that related to it. Thus, in order to implement the foreign regulatory framework, India would need a proper statistical approach to benefit the advancing digital economy of the country with the help of these steps.

7.2 BIBLIOGRAPHY

i. https://www.goodreads.com/author/quotes/4172966.Craig_D_Lounsbrough

ii. The Unique Identification Authority of India is a statutory authority established under the provisions of Aadhaar act 2016 by the Govt. of India under the Ministry of Electronics & Information Technology https://uidai.gov.in/about-uidai.html (last accessed on August 4, 2019)

iii. https://cabsec.gov.in/archive.php?page=28

iv. https://docs.oracle.com/cd/E12454_01/sim/pdf/141/html/user_guide/chapter5.htm

v. https://www.prsindia.org/billtrack/the-national-identification-authority-of-india-bill-2010-1196

vi. https://uidai.gov.in/images/news/Supreme_Courts_Order_in_WP_247_277_304_of_20171606201 7.pdf

vii. https://www.prsindia.org/billtrack/the-aadhaar-targeted-delivery-of-financial-and-other-subsidies-benefits-and-services-bill-2016-4202

https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

viii. https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

ix. [1]https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf https://indiankanoon.org/doc/366712/

x. https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

xi. https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

xii. https://uidai.gov.in/about-uidai/legal-framework/regulations/2046-aadhaar-authentication-regulations,-2016-no-3-of-2016-page-41-67.html

xiii. https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf

xiv. https://uidai.gov.in/about-uidai/legal-framework/regulations/2046-aadhaar-authentication-regulations,-2016-no-3-of-2016-page-41-67.html

xv. http://www.legalservicesindia.com/article/1519/Principles-of-Natural-Justice-In-Indian-Constitution.html

xvi. https://www.lawctopus.com/academike/article-21-of-the-constitution-of-india-right-to-life-and-personal-liberty/

xvii. https://barandbench.com/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches/

xviii. https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

xix. https://indiankanoon.org/doc/556297/

xx. https://indiankanoon.org/doc/500307/

xxi. https://sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf

xxii. http://www.mondaq.com/india/x/626190/data+protection/Information+Technology+Reasonable+Security+Practices+And+Procedures+And+Sensitive+Personal+Data+Or+Information+Rules+2011

xxiii. https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

xxiv. https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018 https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-scheme-does-not-violate-right-to-privacy-says-sc/articleshow/65969846.cms?from=mdr

xxv. https://indiacode.nic.in/handle/123456789/2187?view_type=browse&sam_handle=123456789/1362 https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en

xxvi. European Parliament, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Pub. L. No. Official Journal L 281, 0031, 1995 https://gdpr-info.eu/