Himachal Pradesh National Law University, Shimla (India)

A UGC CARE Listed Journal

Journal Articles | *ISSN:2582-1903* | *Shimla Law Review*

Volume: V (2022)

DISSENT IN THE AADHAAR JUDGEMENT: Exploring Dimensions of the future of Privacy Jurisprudence in India

Varin Sharma

Contents

Volume V	*ISSN: 2582-1903*	April 2022 - March 2023

Notes and Comments

DISSENT IN THE AADHAAR JUDGEMENT: Exploring Dimensions of the future of Privacy Jurisprudence in India

Varin Sharma[*]

[Abstract: *The case comment focuses on the judgement of the Supreme Court of India in Justice K.S. Puttaswamy v. Union of India,1 popularly known as the Aadhaar Judgement, where the Apex Court had to decide upon the constitutionality of the Aadhaar Act.2 In its judgement, the Court struck down several sections of the Act while upholding the constitutional validity. The sections, which were declared unconstitutional along with the remarks made under the dissenting opinion of Justice D.Y. Chandrachud, form the basis of analysis of this case comment as they discuss important aspects concerning the current status as well as the future of privacy laws in India. The interpretation of the judgement along the lines of constitutional provisions for privacy laws in India and rights derived therefrom holds immense potential for the future of the citizens' privacy in a manner that strengthens their liberty and also reduces violation of basic human rights.*]

I

Background of Aadhaar Act, 2016

A project titled, 'Unique Identification for BPL Families', was given approval by the Department of Information Technology, Ministry of Communications and Information Technology, Government of India in 2006.[3] A Processes Committee was set up to create a database for the Unique Identification of families living below poverty line (BPL). Several meetings of the agencies and ministries of central

[*] Mr. Varin Sharma, 3rd Year student, B.B.A. LL.B. (Hons.), Himachal Pradesh National Law University, Shimla. *Email:* varinbba2002@hpnlu.ac.in | varinsharma@gmail.com

[1] AIR (2019) 1 SCC 1.

[2] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 Act No. 18 of 2016, (hereinafter 'Aadhar' or 'the Act').

[3] Ministry of Electronics and Technology, Government of India, UID, *available at:* https://www.meity.gov.in/content/uid#:~:text=Mission%20Mode%20Projects-,UID,of%20Communications%20and%20Information%20Technology. (last visited Apr. 10, 2023). *See* http://www.censusindia.gov.in/.

government related to the Unique Identification (UID) programme favoured the need for the creation of an identity-related resident database.[4] Subsequently, the Government of India, on the recommendation of the Cabinet Secretary constituted the Unique Identification Authority of India (UIDAI), in 2009, as an attached office under the aegis of the Planning Commission. Thus, September 2010 marked the beginning of the nationwide enrolment process of Aadhaar. On the recommendation of the then UIDAI chairperson, a Bill was introduced in the Rajya Sabha in December 2010 known as National Identification Authority of India Bill, 2010.

The purpose of creating this Authority was, primarily, to establish guidelines for the implementation of the unique identification system, which was to issue an identification number to the residents of India. The goal was that the unique identification system would serve as proof of identity which is inherently unique, as each individual will have only one identity with no possibility of duplication. Another purpose was that this number could be used to identify beneficiaries for the transfer of benefits, grants, services, amongst other purposes.

The Aadhaar (Targeted Delivery of Financial and other Subsidies, advantages and administrations) Act, 2016 was introduced as a money bill in the Parliament on 29 February 2016. The Lok Sabha passed the same on 11 March 2016. Its purpose was to set up a legal framework for the Aadhaar unique identification number project to serve as a proof of identity for the citizens of India and secure access to certain services/benefits which can be made available through the same. The services/benefits focused on food and nutrition, employment schemes, social security programmes, public distribution systems, etc.[5]

Key Features of the Act

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Bill, 2016[6], was introduced by Finance Minister Arun Jaitley in the Lok Sabha on March 3, 2016. The primary objective of this legislation was to facilitate the

---

[4] *See In Re: Rani Mistri*, 2016 SCC Cal 8283 and Unique Identification Authority of India, Press Release dated 18 February 2020 – '*Aadhar is not a Citizenship Document*', Available at: https://uidai.gov.in//images/Aadhaar_Press_Release_18Feb_2020.pdf (last visited Nov. 12, 2022). *Adhaar is considered a proof of residence and not citizenship. The labelling of Aadhar as a unique identity for Indians through various government campaigns often leads to the false notion of Aadhar being a proof of citizenship has misled a significant portion of the population and the clarification on the same is, hence, a much needed requirement*.

[5] Surbhi Gloria Singh, *What is Aadhaar? Know all about Aadhaar Bill 2016 in 11 slides*, FINANCIAL EXPRESS (Mar. 11, 2016) *available at*: https://www.financialexpress.com/photos/budget-gallery/223860/what-is-aadhaar-bill-all-you-want-to-know-in-5-points/ (last visited Jan. 13, 2023).

[6] *Supra* at 2.

targeted distribution of subsidies and services to individuals residing in India through the allocation of unique identity numbers known as Aadhaar numbers.

Eligibility:[7] Every resident of India is entitled to obtain an Aadhaar number. A resident, as defined by the Act, is an individual who has lived in India for at least 182 days in the year immediately preceding the date of application for Aadhaar enrolment.

Information Required:[8] To obtain an Aadhaar number, individuals must submit their biometric information (including a photograph, fingerprints, and an iris scan) and demographic details (such as name, date of birth, and address). The Unique Identification Authority of India (UIDAI) may, through regulations, specify additional biometric and demographic information to be collected.

Enrolment Process:[9] During enrolment, individuals are informed about how their information will be used, the entities with whom the information may be shared, and their right to access their data. After verifying the provided information, an Aadhaar number is issued to the individual.

Use of Aadhaar Number: The Aadhaar number is used to verify the identity of individuals receiving subsidies or services. If a person does not have an Aadhaar number, they will be required to apply for one, with an alternative means of identification provided in the interim. Both public and private entities may accept the Aadhaar number as proof of identity; however, the Aadhaar number does not serve as proof of citizenship or domicile.

Authentication:[10] The UIDAI will authenticate an individual's Aadhaar number upon request by an entity, provided that the individual has given consent for their information to be collected. The information disclosed can only be used for the purposes for which the individual has consented.

The UIDAI will respond to authentication queries with a positive, negative, or other appropriate response, but it is prohibited from sharing an individual's biometric data, including fingerprints and iris scans[11]. The UIDAI is required to keep records of the entities requesting verification, the time of the request, and the response provided.[12] However, the purpose for which an individual's identity is verified is not recorded.

---

7 *Id.*, S. 3 read with 2(v).

8 *Id.*, S. 3.

9 *Id.*, S. 3(2).

10 *Id.*, Chapter III, S. 7 – 8.

11 *Id.*, S. 8(4).

12 *Id.*, S. 23(2).

Protection of Information:[13] Biometric data, such as fingerprints and iris scans, may only be used for Aadhaar enrolment and authentication and cannot be shared with anyone or publicly displayed, except as permitted by regulations.

Disclosure of Information: There are specific circumstances[14] under which information may be disclosed. In cases of national security, a Joint Secretary of the central government may authorize the disclosure of Aadhaar numbers, biometric data, demographic information, and photographs. Such a decision is subject to review by an Oversight Committee (comprising the Cabinet Secretary and the Secretaries of Legal Affairs and Electronics and Information Technology) and remains valid for six months. Further, a court may order the disclosure of an individual's Aadhaar number, photograph, and demographic information. A separate, detailed discussion on the issues involved in the Aadhaar Act, particularly regarding the disclosure of information, is present in later sections of this case comment, where the reasoning of the court in upholding the Act as constitutionally valid while reading down some of its provisions is discussed in greater detail. The Act aimed at targeted delivery of subsidies, benefits, and services by providing unique identity numbers based on an individual's demographic and biometric information. It tasks the UIDAI with serving as the administrator and regulator of the Aadhaar ecosystem, making its functioning integral to the success of the entire system.

After the passage of the Act, five different regulations were notified by the UIDAI in September 2016. These are:

1. The Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations, 2016, which govern the transaction of business at UIDAI's meetings by specifying, for instance, the number of meetings that have to take place in a financial year, the quorum required, the role of the Chief Executive Officer, and the decision making process.
2. The Aadhaar (Enrolment and Update) Regulations, 2016, which govern the process of enrolment, the generation of Aadhaar numbers and its delivery to residents, update of information, appointment of registrars and enrolling agencies, omission and deactivation of the Aadhaar numbers, and grievance redressal. These Regulations also prescribe a Code of Conduct (in Schedule V), which requires service providers to make 'best efforts' to protect the interests of the residents (Rule 1).
3. The Aadhaar (Authentication) Regulations, 2016 detail the different modes of authentication, namely demographic, OTP, biometric, and multi-factor authentication; the procedure for appointing requesting entities and authentication service agencies; and the storage and access of transaction data and authentication records. These Regulations also introduced an e-KYC authentication facility, which is not specified in the Act.

---

[13] *Id.*, S. 29.

[14] *Id.*, S. 33.

4. The Aadhaar (Data Security) Regulations, 2016 provide for the specification of an information security policy, emphasises confidentiality, prescribe the security obligations of service providers and personnel, and provide for audit and inspection. To the best of the authors' knowledge, no such information security policy has been specified till date.
5. The Aadhaar (Sharing of Information) Regulations, 2016, which regulate how identity information association with the Aadhaar number holder can be shared with third parties. Interestingly, while the regulations incorporate the principle of purpose limitation for Aadhaar numbers via Regulation 6(5),13 no such principles limit the use of biometric or demographic information of Aadhaar number holders. Regulation 3 currently follows section 29(1)(a) of the Act by stipulating that core biometric information, namely fingerprints and iris scans, shall not be shared with anyone for 'any reason whatsoever.[15]

Under the Aadhaar system, every time an Aadhaar holder seeks a subsidy, benefit, or service, they must provide their biometric information to a designated agency, which then authenticates it through a central authority. This process records and stores the authentication request in the Central Identities Data Repository (CIDR). While the Aadhaar number is primarily used for the purposes outlined in Section 7 of the Aadhaar Act (mandatory proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc.), it can also be utilized for other purposes under Section 57, *allowing its use by the State or private entities for identity verification*.

Petitioner's Contentions

The Aadhaar scheme was challenged before the Supreme Court by Justice K.S. Puttaswamy. He claimed that Aadhaar infringes upon fundamental rights guaranteed by the Constitution. Broadly, his objections included:

1. The government has not put in place adequate privacy safeguards. Any private entity may request authentication by Aadhaar for any reason subject to regulations by the UIDAI. There are no checks on the power of the government to use the biometric data collected.
2. Entitlements granted to the individuals by the State's social sector schemes are themselves a fundamental right. They cannot be limited for any reason, including the failure to produce an Aadhaar Card/Number when applying for benefits

Section 7 of the Act which mandates proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc. was also challenged as unreasonable. Justice Chandrachud has pointed out how mandating Aadhaar for benefits and services under Section 7 would enable a scenario where citizens will not be able to live without Aadhaar. Therefore, he called Section 7 of the Aadhar Act arbitrary and

---

[15] Vrinda Bhandari, and Renuka Sane, *A Critique of Aadhaar Framework*, 31 (1) NLSIR 76-77 (2019).

unconstitutional in his dissent. Section 33 of the Aadhaar Act, which allowed for the sharing of an individual's information on a district judge's order and stated that a hearing shall be held before doing the same, was challenged as, even, arbitrary. Section 33 (2) was challenged as unconstitutional as it gave the State arbitrary powers to share an individual's information in the name of 'national security grounds' since this consideration was to be decided by a Joint Secretary as per this section of the Aadhaar Act. Section 57 of the Aadhaar Act was also challenged and held as unconstitutional which allowed for private parties to mandate Aadhar.

The petitioners argued that the Aadhaar system poses a grave risk to citizens' constitutional rights and liberties. *They asserted that the mandatory collection of biometric data intrudes upon individual privacy and opens the door for the State to evolve into a 'surveillance state'*. The process requires citizens to repeatedly submit their biometric information, which is stored and potentially accessible to both government and private entities. *The petitioners emphasize that this ongoing collection and storage of personal data could enable the profiling of citizens, tracking of their movements, and monitoring of their activities, thereby influencing behaviour and stifling dissent.*

Furthermore, the petitioners' expressed concerns about the potential misuse of data by private agencies involved in the enrolment and authentication processes. *They argue that the Aadhaar Act diminishes the status of citizens by making their rights and entitlements conditional on the surrender of biometric information, which is controlled by the State and private operators.* The risk of data breaches and the lack of robust data protection mechanisms further compound these concerns, leading to fears that citizens' personal information could be exploited by non-state actors.

Respondent's Counter-Arguments

The respondents asserted that the Aadhaar system collects only minimal biometric information, which is stored in the Central Identities Data Repository (CIDR) solely for authentication purposes. They also emphasized that no other personal data, such as religion, caste, tribe, language, entitlements, income, or medical history etc. is collected through Aadhaar enrolment. The respondents further argued that the Aadhaar enrolment process is secure, as biometric data is encrypted and transmitted to the CIDR within seconds, making it inaccessible to the enrolling agency. Similarly, during authentication, the requesting agency does not retain the biometric data, and the Authority only matches the biometrics without storing any information about the purpose, location, or nature of the transaction. Therefore, the respondents contend that there is no basis for concerns about profiling.

Decision

The Supreme Court upheld the constitutionality of the Aadhaar Act and the Regulations, by upholding the passage of the Act as a Money Bill. The Act was not unconstitutional on the grounds of facilitating surveillance, for violating the right to privacy, or for causing any exclusion under Section 7 of the Act. The Court also endorsed the Aadhaar project, as it had evolved from 2009, prior to the enactment of the Aadhaar Act in 2016. Apart from this, the Supreme Court upheld Section 139AA of the Income Tax, making Aadhaar linking mandatory with the PAN number for the payment of taxes.[16] The doctrine of proportionality, which is used to check whether the nature and extent of State interference with the rights of citizens is in proportion to the purpose of the legislation, was applied by the bench in examining the constitutional validity of the Aadhar Act. The majority judgement held that the Aadhar Act passes the test of proportionality.

However, the Court struck down amendments made to the Prevention of Money Laundering Rules, which required linking of Aadhaar number with one's bank account; and the Circular dated March 23, 2017, which amounted to mandatory linking of mobile connections with Aadhaar. The Court also struck down section 33(2) of the Act which authorised disclosure of information in the interest of national security, which had far-reaching effects on the status of surveillance law, as well as, section 57, insofar as it related to body corporates and individuals seeking authentication. In addition, various provisions were read down, including those pertaining to the disclosure of an individual's information without affording her an opportunity of hearing (section 33(1)); archiving of authentication records for five years (Regulation 27(1) of Authentication Regulations); and storage of metadata (Regulation 26 of Authentication Regulations).

The reading down of the above-mentioned sections was only a partial win as the overall functioning of the machinery of Aadhar Act is still a major threat to the safety of personal and sensitive data.

II

Key Issues for Consideration: Justifying State Surveillance

Proportionality as a Dilution of Rights

The balancing approach adopted by the Apex Court in its Aadhar judgement is, in essence, a dilution of privacy rights. The Court manifestly tried to balance the rights of privacy on the one hand as against the interest of and right to access to and

[16] *Id.*

mandatorily providing welfare schemes[17] by the State to citizens on the other. This was done, it is argued, without considering a proper evaluation-criteria; without due weightage to which rights of the citizens are to be weighed against another competing rights and deciding upon what matrix.

Under the German constitutional law, there is a key concept called 'balancing,' which is just one part of a bigger idea known as the principle of proportionality.[18] This principle has three parts: suitability, necessity, and proportionality in a narrow sense. All three parts aim to optimize outcomes. Constitutional rights are seen as guidelines for optimization. That is, the requirement that something be achieved to the fullest extent possible within legal and factual limits.[19] Ultimately, the proportionality principle requires a careful assessment of whether the significance of upholding one right justifies the necessary compromise or limitation of the other, thereby ensuring that the balance struck between competing rights is both reasonable and justifiable.

The objections often raised in this approach refer to the consequence leading to the cancellation of a right in order to achieve a certain objective. As Habermas argues, the balancing method weakens the importance of constitutional rights and also when we balance them against other (rights), rights are downgraded to the level of goals, policies, and values. Rights, thereby, lose the 'strict priority' that is characteristic of 'normative points of view'.[20] Habermas also maintains that the balancing approach takes legal rulings out of the realm of defined concepts like right and wrong, correctness and incorrectness, and justification and into a realm defined by concepts like adequate and inadequate, and discretion.[21] The point put forth, as is also seen in the concept of Aadhar being balanced against right to privacy, is that while weighing certain competing interests, values can help determine an outcome. However, they do not necessarily justify *that* outcome according to principles of rightness or correctness. *This* is the theoretical premise upon which the proportionality as applied in the Aadhar ruling has to be viewed and the article aims to discuss the same.

At its centre, the issues in the Aadhaar ruling revolved around the nature of the Aadhaar Act in negating the fundamental right to privacy of the citizens. The

---

[17] The right to access to schemes is inhibited by making Aadhar the most convenient form of identification to claim benefits from various livelihood, food, healthcare schemes all of which are constitutionally guaranteed rights. Privacy has been well-established as a fundamental right.

[18] Moshe Cohen-Eliya, Iddo Porat, *American balancing and German proportionality: The historical origins*, 8(2) Int. J. Const. Law, 263-286 (2010).

[19] Robert Alexy, A THEORY OF CONSTITUTIONAL RIGHTS 47 (2002).

[20] Jürgen Habermas, BETWEEN FACTS AND NORMS 256 (1996).

[21] Robert Alexy, *Balancing, constitutional review, and representation*, 3(4) INT. J. CONST. LAW 572-581 (2005).

Supreme Court in in *Justice K.S. Puttaswamy* v. *Union of India*[22] had declared the 'Right to Privacy' as part of the fundamental rights under Article 21(Right to Life and Personal Liberty) as enshrined in Part III of the Constitution of India.[23] The dissenting opinion of Justice Chandrachud forms the basis of discussion over privacy laws in this comment.

One possible method to understand such a viewpoint is undertake an analysis that aims at bringing into light what we presuppose when we resolve cases by balancing? The other way to grasp this idea is to examine what we assume when we balance different rights or interests in legal cases?

For example, we can consider a *decision*[24] by German Federal Constitutional Court about health warnings on cigarette packages. The Court decided that requiring tobacco companies to put health warnings on their products only *slightly* limits their freedom to do business. On the other hand, completely banning all tobacco products would be a much greater limitation. Between these two extremes, there are actions that cause moderate restrictions. This helps us create a scale with three levels of interference: light, moderate, and serious.

In the case of health warning labels, the health dangers of smoking are very high. This means that the reasons for requiring the warnings are very important[25]. We know, how smoking poses significant health risks. Therefore, the reasons for implementing these warnings are very strong. When we balance the low level of interference (just adding warning labels) against the high importance of protecting health, we can clearly see how the principle of proportionality works in this context and the approach helps us better understand that appropriate measures should be proportionate to the importance of the objective they aim to achieve.

In the *Aadhar case,* the Supreme Court was presented with a unique issue wherein the only reasonable way out was the use of proportionality principle and weighing the varied competing interests. The Aadhar Act brought with it technological incursions affecting constitutional rights of citizens. The doctrine of proportionality, which is used to check whether the nature and extent of State interference in the rights of citizens is in proportion to the purpose of the legislation,[26] was applied by the bench in examining the constitutional validity of the Aadhar Act. The majority

---

[22] (2017) 10 SCC 1.

[23] *Id*.

[24] BVerfG, decision of the Second Senate of January 22, 1997 - 2 BvR 1915/91 -, Rn. 1-70, *available at:* https://www.bverfg.de/e/rs19970122_2bvr191591.html.

[25] Robert Alexy, *Constitutional Rights, Balancing, and Rationality* 16 (2) RATIO JURIS 131–140 (2003).

[26] Aditya AK, *Proportionality Test for Aadhaar: The Supreme Court's two approaches*, BAR AND BENCH, *available at:* https://www.barandbench.com/columns/proportionality-test-for-aadhaar-the-supreme-courts-two-approaches (last visited May 13, 2023).

judgement held that the Aadhar Act passes the test of proportionality. The criteria[27] considered by the majority judgement was the same as decided by the Supreme Court decision in *Modern Dental College* v. *State of Madhya Pradesh,*[28] which summarised the doctrine as follows:

> *a) A measure restricting a right must have a legitimate goal (legitimate goal stage).*
> *b) It must be a suitable means of furthering this goal (suitability or rationale connection stage).*
> *c) There must not be any less restrictive but equally effective alternative (necessity stage).*
> *d) The measure must not have a disproportionate impact on the right holder (balancing stage).*[29]

In Aadhar judgement the majority held for the first condition *i.e.,* a legitimate aim and purpose of the legislation in question, (Aadhar Act):

> It is, thus, of some significance to remark that it is this Court which has been repeatedly insisting that benefits to reach the most deserving and should not get frittered mid-way. We are of the opinion that purpose of Aadhaar Act, as captured in the Statement of Objects and Reasons and sought to be implemented by Section 7 of the Aadhaar Act, is to achieve the stated objectives. This Court is convinced by its conscience that the Act is aimed at a proper purpose, which is of sufficient importance.[30]

On the point of suitable means of furthering the goal of the legislation, the Court observed:

> 'We are also of the opinion that the measures which are enumerated and been taken as per the provisions of Section 7 read with Section 5 of the Aadhaar Act are rationally connected with the fulfilment of the objectives contained in the Aadhaar Act'.[31]

On the point of finding a less restrictive but equally effective alternative, the judgement reads:

> 'No doubt, there are many other modes by which a person can be identified. However, certain categories of persons, particularly those living in abject poverty and those who are illiterate will not be in a position to get other modes of identity like Pan Card, Passport etc…[32]'
> The manner in which malpractices have been committed in the past leaves us to hold that apart from the system of unique identity in Aadhaar and authentication of the

---

[27] Justice A. K. Sikri, in the judgement, relies upon the works and observations of Justice Aharon Barak (former Chief Justice of the Supreme Court of Israel), Aharon Barak. *See* Aharon Barak, PROPORTIONALITY CONSTITUTIONAL RIGHTS AND THEIR LIMITS (2012).

[28] (2016) 7 SCC 353.

[29] *Id*., para 125.

[30] *Id.* para 276.

[31] *Id.* para 277.

[32] *Id*., para 277.

> real beneficiaries, there is no alternative measure with lesser degree of limitation which can achieve the same purpose.[33]

The fourth criterion is of crucial importance to the discussion on privacy laws since it discusses the balancing of the Right in question (privacy) being interfered with against the new legislation on Aadhar which, as the central government also stated in its arguments, entitles the citizens in availing certain benefits. The court's majority judgement justifies the Aadhaar Act having attained a balanced situation with respect to interference in the rights of the citizen, particularly, the Right to Privacy. The court, in its reasoning on the fourth aspect of proportionality, focuses on two issues:

- Whether, 'legitimate state interest' ensures 'reasonable tailoring'? … Here the Act is to be tested on the ground that whether it is found on a balancing test that the social or public interest and the reasonableness of the restrictions outweigh the particular aspect of privacy. …
- There needs to be balancing of two competing fundamental rights, right to privacy on the one hand and right to food, shelter and employment on the other hand.[34]

To answer the first query, the Court relied on the 'reasonable expectation of privacy' test and the judgment of the Court of Appeal in *R. Wood* v. *Commissioner*[35]. Justice Sikri writes: 'therefore, when a claim of privacy seeks inclusion in article 21 of the Constitution of India, the Court needs to apply the reasonable expectation of privacy test. It should, inter alia, see:

- What is the context in which a privacy claim is set up?
- Does the claim relate to private or family life, or a confidential relationship?
- Is the claim a serious one or is it trivial?
- Is the disclosure likely to result in any serious or significant injury and the nature and extent of disclosure?
- Is disclosure related to personal and sensitive information of an identified person?
- Does disclosure relate to information already disclosed publicly? If so, its implication?

It is important to note here that the '*reasonable expectation of privacy test*' was discussed by the United States Supreme Court, in 1967, in its decision of *Katz* v. *United States.*[36] The test has two components: a *subjective* one and an *objective* one. The subjective component deals with the question of whether the person whose right is violated actually expected privacy in such a situation? If the answer is in the

---

[33] *Id*., para 280.

[34] *Id*., para 285.

[35] (2010) 1 WLR 123, para 292.

[36] (1967) 389 U.S. 347.

affirmative, the Court would further inquire whether, objectively, the society would find the expectation of privacy reasonable?[37]

The Court's application of 'reasonable expectation of privacy test,' with due respect to the Court, is flawed in the context of the Aadhar issue. The usage of this test has been discouraged by Justice Nariman in the *Puttaswamy*[38] while referring to the judgment of the apex court in *District Registrar and Collector* v. *Canara Bank*,[39] and thereby holding that the 'reasonable expectation of privacy test' has no plausible foundation under Articles 14, 19, 20, and 21 of the Constitution of India.[40] Therefore, the application of the test by the apex court, when it was rejected earlier on the grounds of constitutional values, is puzzling. Instead of focusing on the extent of interference in the rights of the citizens and balancing the same against State objectives, the Court engaged in , it seems, reasonable expectation of privacy test to dilute requirement of justifying the fourth criterion of proportionality for the Act.

The Court finds the basis of its reasoning on the ground that if the petitioner has no reasonable expectation of privacy, she is outside the protective scope of article 21 of the Indian Constitution. This is not a very satisfying premise.[41]

On the second aspect of the balancing exercise, the Court tried to consider the right to privacy on the one hand and the right to food, livelihood, and social welfare benefits on the other. Based on the balancing of the two, it concluded that the invasion on the right to privacy is nominal. The majority judgement reads:

> '*Let us advert to the second facet of balancing, namely, balancing of two fundamental rights. As already pointed out above, the Aadhaar Act truly seeks to secure to the poor and deprived persons an opportunity to live their life and exercise their liberty. By ensuring targeted delivery through digital identification, it not only provides them a nationally recognized identity but also attempts to ensure the delivery of benefits, service and subsidies….*[42]
> '*In the aforesaid backdrop, this Court is called upon to find out whether Aadhaar Act strikes a fair balance between the two rights… To reiterate some of the important features, it is to be borne in mind that the State is using Aadhaar as an enabler for providing deserving section*

---

[37] Mariyam Kamil, *The Aadhaar Judgment and the Constitution – II: On proportionality (Guest Post)*, (September, 2018) *available at*: https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/. (last visited Jan.19, 2022).

[38] (2017) 10 SCC 1.

[39] (2005) 1 SCC 496.

[40] Nishith Desai, *Supreme Court Holds That The Right To Privacy Is A Fundamental Right Guaranteed Under The Constitution Of India*, MONDAQ (September 2017) *available at:* https://www.mondaq.com/india/privacy-protection/629084/supreme-court-holds-that-the-right-to-privacy-is-a-fundamental-right-guaranteed-under-the-constitution-of-india#:~:text=Justice%20Nariman%20has%20also%20discussed,United%20States22%20. (last visited Jan. 19, 2022).

[41] *Supra* at 22.

[42] *Id.*, para 295.

> *of the society their right to food, right to livelihood, right to receive pension and other social assistance benefits like scholarships etc. thereby bringing their right to life to fruition. This necessity of Aadhaar has arisen in order to ensure that such benefits are given to only genuine beneficiaries. The Act aims at efficient, transparent and targeted delivery of subsidies, benefits and services… As against the above larger public interest, the invasion into the privacy rights of these beneficiaries is minimal.'*[43]

Approach of Dissenting Opinion:

Justice Chandrachud offers his dissenting opinion on the issue of interference with the Rights of Citizen and provides, in my opinion, a much better constitutional perspective on the Aadhaar Act when it comes to the infringement of rights of a citizen by the same. Justice Chandrachud identifies an apt consideration and describes how such state action is highly disproportionate to the welfare being provided to the people by the Act The idea of state surveillance in the garb of providing food, shelter, social security etc., through Aadhaar, is a petrifying one and highly preposterous. The Judge pointed out how mandating Aadhaar for benefits and services under Section 7 would enable a scenario where citizens will not be able to live without Aadhaar. Therefore, he calls Section 7 of the Aadhar Act arbitrary and unconstitutional. He declared:

> '…by collecting identity information, the Aadhaar program treats every citizen as a potential criminal without even requiring the State to draw a reasonable belief that a citizen might be perpetrating a crime or an identity fraud. When the State is not required to have a reasonable belief and judicial determination to this effect, a program like Aadhaar, which infringes on the justifiable expectations of privacy of citizens flowing from the Constitution, is completely disproportionate to the objective sought to be achieved by the State.'[44]

Surveillance: Monitoring of citizens under the garb of 'benefits'

The petitioners, in their arguments, had submitted that by associating every citizen with an identification number and attaching that number to provide access to a plethora of services and activities, the State creates a surveillance system that can be used to actively monitor the activities, transactions or exchanges its 'subjects' indulge in. Such 'body tagging' of the citizens gives the State, the capability and in certain processes even the authority, to gain all knowledge of the citizens' activities concerned with their State-generated social identity *i.e.,* Aadhaar.[45]

The mechanism of Aadhaar, as the UIDAI explains, brings into play the 'uniqueness' of the identity of individuals by using their biometrics *i.e.,* fingerprints and iris scan.

---

[43] *Id.,* para 307, 308.

[44] *Id.,* para 217.

[45] *Supra* at 4.

It is, no doubt, true that biometrics are unique to each individual; however, their uniqueness does not ensure their security by itself. The Court's observation was:

> 'When Aadhaar is seeded into every database, it becomes a bridge across discreet data silos, which allows anyone with access to this information to reconstruct a profile of an individual's life. It must be noted while Section 2(k) of the Aadhaar Act excludes storage of individual information related to race, religion, caste, tribe, ethnicity, language, income or medical history into CIDR, the mandatory linking of Aadhaar with various schemes allows the same result in effect. For instance, when an individual from a particular caste engaged in manual scavenging is rescued and in order to take benefit of rehabilitation schemes, she/he has to link the Aadhaar number with the scheme, the effect is that a profile as that of a person engaged in manual scavenging is created in the scheme database. The stigma of being a manual scavenger gets permanently fixed to her/his identity. What the Aadhaar Act seeks to exclude specifically is done in effect by the mandatory linking of Aadhaar numbers with different databases, under cover of the delivery of benefits and services.'[46]

It is also interesting to note how the majority judgement contradicts in its statements at different points. For example, the majority finds the Aadhar data collection scheme (of biometrics) a safe one.[47] The Court red down section 33 of the Aadhaar Act, which allowed for the sharing of an individual's information on a district judge's order and stated that a hearing shall be held before doing the same. It held section 33(2) unconstitutional as it gave the State arbitrary powers to share an individual's information in the name of 'national security', since this consideration was to be decided by a Joint Secretary as per the section of the Aadhaar Act. Section 57 of the Aadhaar Act was also held as unconstitutional as it allowed private parties to mandate Aadhar.

The majority judgement partially red down and disregarded sections 33, 33(2) and 57. It would have been seen a complete victory of the Constitutional principles and values had the Court considered the points raised by Justice Chandrachud in his dissenting opinion regarding the unconstitutional nature of the Aadhar Act.

While reading down and striking certain provisions of the Aadhar Act, the majority also removed the provision which facilitated the retention of authentication transaction data or metadata for five years as the original Bill provided for. Metadata refers to a set of data describing other stored data. In essence, Aadhar data collection stored metadata in the form of linking of mobile numbers, bank details, Pan Cards, etc., and the same could prove basis for a very sophisticated but effective surveillance mechanism without appearing to be one. The Aadhar Act originally also had the provision to retain this data for a period of five years as mentioned. The majority judgement however, struck down this provision and laid down that the

---

[46] *Supra* at 1, Chandrachud J.,para 274.

[47] *Supra* at 38, para 44.

transaction data (metadata) has to be deleted after a period of six months and did not find merit in letting UIDAI retain the data for five years. It also stated that the data may be retained by UIDAI for more than six months in case there is a dispute pending or ordered by a court. The Court observed:

> We do not find any reason for archiving the authentication transaction data for a period of five years. Retention of this data for a period of six months is more than sufficient after which it needs to be deleted except when such authentication transaction data are required to be maintained by a Court or in connection with any pending dispute. Regulations 26 and 27 shall, therefore, be amended accordingly[48].

The restriction over data retention in the context of time period is in contradiction to the Court's earlier statements regarding the safety and the 'uniqueness' of the biometric data stored with Aadhar. If the data is, indeed, as the Court found, obscure from threats like surveillance or body-tagging of citizens, the retention of data for longer periods, as the government earlier intended to, should not have been an issue.[49] Thus, the six-month limit as prescribed by the Court does not appear to have sound reasoning behind it.

The other point considered by the Court that, the data may be retained for more than six months in case a dispute arises or after a court order, assumes that six months is the appropriate time period where the dispute may arise[50] and, thereby, ignores the horrors of modern technology and its manipulative potential that come with the pace at which scientific progress takes place today. This scenario is one where the data protection laws of individuals come into play, however, a separate analysis is required to determine how the Court failed to address adequate protection regarding the data processing of individuals.

While discussing the storage mechanism of the data with Aadhar and the security of the same, it is of utmost importance that encryption of data collected by UIDAI must also be taken into account. The UIDAI claims that all the biometric data it collects is encrypted. Further, they also claim that the Aadhar enrolment system is full proof when it comes to hacking or other kinds of breach. The reasoning behind the same being, as argued by the government, that within a few seconds of collection the biometric data, by the concerned enrolling agency, the biometrics' data collected is sent to the Authorities (CIDR – Central Identities Data Repository) with encryption and it is then beyond the reach of the enrolling agency who collected it. Legally, however, sound safeguards are not present. There is no provisions in the Aadhar Act or any bylaws mandating encryption. This is a serious concern since

---

[48] *Supra* at 1, para 205.

[49] Anand Venkat, *The Aadhaar Judgment and Reality – III: On Surveillance (Guest Post)*, indconlawphil.wordpress.com, September, 2018. https://indconlawphil.wordpress.com/2018/10/02/the-aadhaar-judgment-and-reality-iii-on-surveillance-guest-post/ (last visited Jan. 31, 2022).

[50] *Id*.

encryption provided the little hope public had when it came to the safety and privacy of their biometric data. The minority judgement clearly highlights the issue.[51]

III

Judicial Perspectives on Privacy and Privacy Jurisprudence in India

Privacy in India has been the central issue in several litigations over the time and the Courts of this country have done a remarkable job in giving due importance to the rights guaranteed to prisoners as citizens[52], people under trial[53] etc. As discussed previously, privacy was recognised as a fundamental right in *Puttaswamy*[54] and its interpretation by the nine-judge bench was in a manner that had never been previously done by any court of law in India. There are, however, many past incidents where the importance of privacy as an integral part of human lives has been highlighted by the Judiciary. It is important to refer to some of such judicial pronouncements and literary works which highlighted the significance of privacy in such a manner that is relevant to the context of the Aadhaar Act in India. To begin with, we can consider the prominent judgement of *Selvi* v. *State of Karnataka*[55], where the Supreme court discussed the rights of the accused person with respect to her right to privacy against neuroscientific investigative techniques and declared that such technique violated the accused's right against self-incrimination and also infringed the mental privacy of the accused person. The court stated:

> 'In conceptualising the `right to privacy' we must highlight the distinction between privacy in a physical sense and the privacy of one's mental processes…We must recognise the importance of personal autonomy in aspects such as the choice between remaining silent and speaking. An individual's decision to make a statement is the product of a private choice and there should be no scope for any other individual to interfere with such autonomy, especially in circumstances where the person faces exposure to criminal charges or penalties. Therefore, it is our

---

[51] *Supra* at 1, para 143.

[52] *See generally T.V. Vatheeswaran* v. *State of Tamil Nadu (1983) 2 SCC 68, State Of Andhra Pradesh* v. *Challa Ramkrishna Reddy (*2000) 5 SCC 712.

[53] *See generally Sunil Batra* v. *Delhi Administration* 1980 SCC (3) 488, *Nandini Satpathy* v. *P.L. Dani* AIR 1978 SC 1025.

[54] *Supra* at 22.

[55] AIR 2010 SC 1974, (2010) 7 SCC 263.

> considered opinion that subjecting a person to the impugned techniques in an involuntary manner violates the prescribed boundaries of privacy.[56]

Such sincere and profound interpretations of right to privacy have implications on the constitutionality of Aadhar Act. A country where clear distinctions are made between physical and mental spheres of privacy and due respect is given to both by the courts of law in a discrete manner, any mechanism, especially, a state-sanctioned one, that infringes or threatens to jeopardise the right to privacy of its citizens or treat the same with callousness can simply not be allowed. The judgement in *Selvi* is ultimately a vindication of the ideals expressed by Canadian Supreme Court's, Justice Claire L'Heureux-Dubè:

> 'Although the search of an individual's home is an invasion of privacy, and although the taking of fingerprints, breath samples or bodily fluids are even more private, there is no doubt that the mind is the individual's most private sanctum. Although the state may legitimately invade many of these spheres for valid and justifiable investigatory purposes vis-à-vis the accused, it is fundamental to justice that the state not be able to invade the sanctum of the mind for the purpose of incriminating that individual. This fundamental tenet is preserved, in its entirety, by the principle against self-incrimination.'[57]

Aadhar, though not directly interfering with the sanctum of one's mental or physical privacy, does the same to some extent through its body-profiling/body-tagging mechanism, whereby it has access to the person's details concerned with those transactions he indulges in, through his Aadhar. This is clearly a huge violation of the fundamental right to privacy at the most basic level.

At the end of the eighteenth century, an article titled *The Right to Privacy*[58] by American scholars Warren and Brandeis was probably the first to defend a 'right to seclusion' or 'right to be left alone' where a person was entitled to privacy at his home/personal sphere and this had ground-breaking repercussions in providing the basis to fight state-surveillance mechanisms to a great extent. The same concept also gained importance in legal thought by the US Supreme Court in the case of *Katz* v. *United States,*[59] where the issue of Federal Bureau of Investigation (FBI) eavesdropping on an individual had arisen. The FBI agents did so by attaching recording devices outside a phone booth. The court had to consider whether this amounted to unlawful search and seizure as prohibited by the Fourth Amendment of the US Constitution. The Supreme Court held that it did and also noted that the purpose of the Fourth Amendment was to protect people, not places:[60]

---

[56] *Id*.

[57] *R.* v. *S* (R.J.) (1995) 1 SCR 451, 605 (concurring opinion of Justice Claire L'Heureux-Dubè).

[58] Samuel D. Warren and Louis D. Brandeis, *'The Right to Privacy'*, 4(5) HARV.L.REV 193 (1890).

[59] 389 U.S. 347 (1967).

[60] *Id*.

> '…an enclosed telephone booth is an area where, like a home… and unlike a field…a person has a constitutionally protected reasonable expectation of privacy…As the Court's opinion states, 'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a 'place.'[61]

Such precedents must force the Indian legislature and the judiciary, as well, to think along the lines of private 'spheres' of citizens and protect the activities undertaken in the same and also ensure that nothing infiltrates the same. The Aadhar, in its very essence, goes completely in contradiction to the respect of privacy spheres of the citizens. As the above-discussed article and judgement conceptualise, any sort of tagging of bodies of people in pursuance of monitoring their activities and/or infiltration of the private spheres of the people amounts to unreasonable and unlawful surveillance. Aadhar Act attempts and authorise similar state actions when it links mobile phones, biometrics and other crucial data for availing of certain benefits or welfare schemes.

IV

Data-Driven Monitoring and Surveillance by the State

A Panopticonin the Making[62]

In the present age, surveillance systems are driven by data-based surveillance reversing the legal axiom that it is better to let ten guilty men go free than one innocent man to go to jail. American political scientist Professor Virginia Eubanks explains:

> '…in new data-based surveillance, the target often emerges from the data. The targeting comes after the data collection, not before. Massive amounts of

---

[61] *Id*. (concurring opinion of Justice Harlan).

[62] A Panopticon is a prison system developed by English philosopher and social theorist Jeremy Bentham. The building with the prisoners is only one cell thick, and every cell has one open side facing the central tower. This open side has bars over it, but is otherwise entirely exposed to the tower. The guards can thus see the entirety of any cell at any time, and the prisoners are always vulnerable and visible. Conversely, the tower is far enough from the cells and has sufficiently small windows that the prisoners cannot see the guards inside of it.
The sociological effect is that the prisoners are aware of the presence of authority at all times, even though they never know exactly when they are being observed. The authority changes from being a limited physical entity to being an internalized omniscience- the prisoners discipline themselves simply because someone might be watching, eliminating the need for more physical power to accomplish the same task.

> information are collected on a wide variety of individuals and groups. Then, the data is mined, analyzed, and searched in order to identify possible targets for more thorough scrutiny. Sometimes this involves old-school, in-person watching and tracking. But increasingly, it only requires finer sifting of data that already exists. If the old surveillance was an eye in the sky, the new surveillance is a spider in a digital web, testing each connected strand for suspicious vibrations.'[63]

This modern day intricate and intrusive network of surveillance, extends far beyond the traditional scope of monitoring. It challenges the foundational principles of justice and liberty, where even the idea of presumption of innocence is at the risk of being overshadowed by data-driven suspicion. As the state increasingly relies on data to identify potential threats as a preventive action, the very notions of privacy and fundamental rights begin to fray. This abrasion is not merely a theoretical concern but a perceptible consequence of the modern surveillance apparatus, as seen in state machineries established by law of policies such as Aadhar.

Impact of Modern Data-Based Surveillance on Fundamental Rights

Modern-age data collection mechanisms, like Aadhar, affect the rights of individuals through the design collection and profiling and not their potential abuse in some imagined future. This is an argument the Supreme Court failed to consider in deciding the Aadhar judgement. This simple concept was left only to be pointed out by Justice Chandrachud in his dissent.[64] If a society allows for huge databases with the potential for intrusive surveillance because the courts consider such fears regarding breach of privacy far-fetched. The kind of mechanisms, ultimately, results into the system where the databases start functioning as means of predictive policing.

Predictive-policing is based on the idea of preventing crimes before it occurs by profiling citizens' past behaviour or the public at large. Such a scenario can only be termed as an absurd dystopia. Just like DNA data banks, as used in countries like the US, which becomes means of predictive policing, Aadhar holds, it is submitted, the same potential.

It is in such scenarios where the transformative nature of the Constitution, one which brings about changes for the public good with a liberal and socially beneficial interpretation of its provisions, comes into play. We see how courts apply this in cases like *Selvi*.[65] There are some things, some invasions of personal rights, some

---

[63] Virgina Eubanks, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR, (2018).

[64] Gautam Bhatia, THE TRANSFORMATIVE CONSTITUTION: A RADICAL BIOGRAPHY IN NINE ACTS (2019).

[65] *Supra* at 55.

exercises of state power that the Constitution simply does not allow, no matter what benefits they may be scientifically proven to have.[66]

Professor Ramachandra Siras's case[67] is a prime example of how a state's invasion in a person's autonomous choices ultimately manufactures paranoid citizens living in the fear of being gauged eternally by the watchful state. Data processing against wilful consent by the person whose data is being monitored/processed even in the name of administrative/investigating purposes is another mechanism which utterly disregards an individual's right to privacy. However, the regulatory mechanisms for this, as prescribed, under various data processing laws are beyond the scope of this case comment.

Another precedent that should be considered is the case of *Goldberg* v. *Kelly*[68] In this case, the US Supreme Court decided that a right to a full hearing exists before the termination of the concerned person's welfare benefits. Hence, while considering the Aadhar Act, which fixates biometric authentication as the basis for several welfare benefits, it is of paramount importance that the Supreme Court ought to take this into account and mandate the right to a fair trial before a citizen receiving benefits under a welfare scheme is discontinued under the Aadhar. This again, however, would put the onus on the individual to prove his identity which was not accepted/recorded by the machines in order to avail a fair trial or the welfare benefits. Moreover, even stronger judicial constraints would be required to surpass this horrid mechanism. In the age of automation, innocence becomes a treasured possession and subsequently even rarer to establish.

The solution to such problems is as complex and distant to achieve as the present technology-driven labyrinth systems are. One simple solution left to citizens would be the choice for self-identification which allows them to choose whether they would like any association with the technological mechanisms provided. Thus, citizens can choose whether they wish to be a part of such technological setups no matter how great the benefits one avails from such setups. The pre-existing identification, that is, government identification documents like PAN or Driving License do not incorporate biometrics or link storage mechanisms of data and serve

---

[66] Gautam Bhatia, *'Something of a Freedom is Yet to Come'*, THE TRANSFORMATIVE CONSTITUTION: A RADICAL BIOGRAPHY IN NINE ACTS, 2019.

[67] In 2010, Aligarh University suspended Professor Ramachandra Siras following an incident where three journalists, entered Siras' residence and recorded him engaging in a consensual intimate encounter with another man. Although the Allahabad High Court temporarily halted Professor Siras' suspension, it did not prevent the ongoing departmental investigation. Tragically, he took his own life a few days after the court's decision. *See* International Commission of Jurists, *SR Siras* v. *Aligarh Muslim University*, *available at:* https://www.icj.org/sogicasebook/sr-siras-v-aligarh-muslim-university-high-court-at-allahabad-india-1-april-2010/ (last visited Aug. 22, 2023).

[68] 397 U.S. 254 (1970).

the purpose of being the identity proofs of the person holding them. Aadhar differs from them in this.

Hence, for future legislations, an idea may be strongly considered where a choice is given to the citizens on whether they wish to be part of 'welfare' schemes in exchange for their personal data. This is the case because if the state does, in fact, work for the public good, offering a choice for the same, ought not to pose any setbacks for availing of services. The emerging technologies have the potential of redefining the idea of self-determination. 'Individuals have the right to engage with technological systems on their own terms, the right to opt into or opt out of such systems without suffering for it, and the right not to be subjected to technological intervention without being given meaningful choice. Technological self-determination is the right of every individual to determine how, on what terms, and to what extent, she will engage with technological systems.'[69]

On the requirement of consent, we may easily perceive as to how the state can manipulate consent by viewing consent not as a specific agreement to submit to a particular situation but as a general assumption of agreeableness to all situations unless expressly denied. We see such an approach in section 7 of the recently enacted 'Digital Personal Data Protection Act, 2023', which provides that:

> A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:-
> (a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, *and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.*[70] (emphasis added)

Such ideals must be given serious thought whenever any digital data collection mechanism is set up by any organisation within the country or by the State itself as they are in line with the constitutional principles this country strives to uphold.

V

Conclusion

When Aadhar was initially introduced, in 2010, by the Government of India, it involved a voluntary enrolment process, intended to improve individuals' access to government services and benefits by a smooth authentication system and was an

---

[69] Gautam Bhatia, *Under a Humane Constitution*, THE HINDU (Mar. 12, 2018, New Delhi) *available at*: https://www.thehindu.com/opinion/lead/under-a-humane-constitution/article23042046.ece (last visited Feb. 01, 2022).

[70] Section 7, Digital Personal Data Protection Bill, 2023.

alternate means to identify oneself. It was UIDAI's way of letting a citizen know that they are indeed 'who they claim they are'.[71] The issue of Aadhar became a bone of contention before the Supreme Court. It generated and caused the second-longest hearing only after the *Kesavananda Bharati*.[72] It invited engrossing debates from, both sides, petitioners and the Government.[73] Aadhar has, with time, come to be an almost indispensable tool in the life of every Indians. A range of services forced citizens to register with Aadhar in order to avail certain benefits integral to his/her life even if the state has not mandated them. Before the hearings in the Aadhar case, the Aadhar Act made it mandatory to hold the Aadhar card if one wanted to open a bank account, obtain a new Mobile SIM card, pay the income tax, etc. The outcome of the hearing was that mobile number linking, admission of children to schools and colleges, opening/linking of a bank account with Aadhar and allowing private companies to use Aadhar data, all were declared unlawful and the provisions of the Act authorising the same were struck down by the Supreme Court. Having said that, obtaining a PAN card, filing income tax returns still requires an Aadhar number. Recently, the central government mandated Aadhar for workers if they wished to avail social security benefits.[74] Such mandates leave millions vulnerable to threats of surveillance, monitoring and tracking against their wishes by unregulated access to their biometric data and reduce the nature of the right of privacy as a fundamental right to only a myth.

India finds its hope in Justice Chandrachud's dissenting opinion which will surely, in coming years, be given legislative importance, but for now, Aadhar is a dark chapter in the evolution of the concept of privacy in India. The dissenting opinion holds the potential to form the basis of future privacy regulations in the country and will probably prove to be the most formidable weapon in the fight when it comes to defending the rights of the public at large against tyranny in the concerned matters. The dissent acts as a crucial safeguard in upholding constitutional principles in the context of privacy legislation. Senior counsel Shyam Divan in his oral arguments in the Aadhar case remarked: *'The Constitution is not a charter of servitude'*. These words should leave an indelible mark on us, our minds, and as a nation whenever we are

---

71 *See* https://uidai.gov.in/contact-support/have-any-question/304-faqs/authentication/for-residents.html. (last visited Feb. 02, 2022).

72 *Kesavananda Bharati Sripadagalvaru* v. *State of Kerala* (1973) 4 SCC 225, AIR 1973 SC 1461.

73 Mehal Jain, *[Aadhaar Day-1 To 38] Here Is The Summary Of Supreme Court's Second-Longest Hearing*, LIVELAW, *available at*: https://www.livelaw.in/aadhaar-day-1-to-38-here-is-the-summary-of-supreme-courts-second-longest-hearing/ (last visited Jun. 16, 2023).

74 Yogima Seth Sharma, '*Aadhaar mandatory for all workers to avail social security benefits'*, ECONOMIC TIMES (May 05, 2021) *available at*: https://economictimes.indiatimes.com/news/economy/policy/aadhaar-mandatory-for-all-workers-to-avail-social-security-benefits/articleshow/82401711.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. (last visited Feb. 02, 2022).

put in a situation where the liberty and rights of the citizens are brought for unreasonable policing by the state. The ideas presented here are harmonious with Justice Chandrachud's recent remarks, *'technology must be understood as the facilitator of change, but the driver of change has been and must be the human mind.'*[75]

[75] PTI, *SC judge roots for tech to boost justice delivery*, THE TIMES OF INDIA (18 Jan., 2022, Ahmedabad) *available at*: http://timesofindia.indiatimes.com/articleshow/88961545.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. (last visited Feb. 02, 2022).