The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

PRIVACY IN THE AGE OF AADHAR: A CRITICAL ANALYSIS OF INDIAN JURISPRUDENCE

Aditi Raikwar

INTRODUCTION

In the digital age, the collection, storage, and use of individual information by the state have become the focal point of constitutional controversy in those jurisdictions that aim to reconcile the provision of welfare and civil liberties. In India, the Aadhaar programme has been envisioned as the largest biometric identity programme of the world that has emerged as the fulcrum of this conflict. Initially envisioned as a voluntary programme to facilitate the delivery of subsidies and benefits, Aadhaar has increasingly evolved into a mandatory requirement for accessing a variety of government and private services. This monumental expansion has generated serious concerns regarding informational privacy, data protection, and the potential for state surveillance.

The constitutional discourse on privacy in India saw a major change after the historic judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[1], wherein a nine-judge bench of the Supreme Court of India unanimously held the right to privacy as a fundamental right that resides in the ambit of Article 21[2] of the Constitution. The declaration brought about a re-examination of the constitutional validity of the Aadhaar scheme, subsequent to which a five-judge bench pronounced the following judgment in Puttaswamy v. Union of India (2018)[3]. The majority judges who opined that the constitutional validity of Aadhaar was maintained imposed stringent limitations on the use of Aadhaar. The dissenting judges, particularly Justice Chandrachud's,

1 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.
2 INDIA CONST. art. 21.
3 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2018 SC 1841.

critically assailed the scheme as amounts to a breach of constitutional protection and allows for the creation of a surveillance state that is antithetical to democratic values.

This research paper critically examines the Aadhaar scheme from the constitutional perspective of the right to privacy. It attempts to examine whether the design and implementation of the Aadhaar system meet the proportionality test established in the Puttaswamy case and if the judicial logic has addressed the system risks involved in centralizing biometric data in full. The paper examines the adequacy of the Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act of 2016[4] in safeguarding individual privacy and places the scheme in international perspective with respect to data protection and digital governance.

This paper considers Aadhaar in the context of India's evolving constitutional jurisprudence on privacy, mindful of the delicate balance between technological advancement and the protection of basic rights. For this purpose, it tries to contribute to the new scholarship that examines the dual character of the state as a protector and potential violator of privacy rights in the age of the digital.

CONSTITUTIONAL RIGHT TO PRIVACY

PRE-PUTTASWAMY JURISPRUDENCE: MP SHARMA AND KHARAK SINGH

Before the landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Indian constitutional scheme did not have the recognition of privacy as a fundamental right. Two landmark cases are MP Sharma v. Satish Chandra (1954)[5] and Kharak Singh v. State of Uttar Pradesh[6] (1962) that shaped early jurisprudence formation and created limited conceptions of privacy within the Indian Constitution.

In MP Sharma, an eight-judge bench held that the right of privacy was not a constitutional right under Article 20(3)[7] but upheld the right of the state to search and seize the documents in criminal cases. The Court did not accept the idea of a general right of privacy on the rationale that the Constitution had no express provisions for the same.

In the case of Kharak Singh, the bench in majority upheld that the surveillance by police was not against any of the fundamental rights, with the exception of domiciliary visits, which were

4 The Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
5 MP Sharma v. Satish Chandra, AIR 1954 SC 300.
6 Kharak Singh v. State of Uttar Pradesh, AIR 1962 SC 1295.
7 INDIA CONST. art. 20(3).

declared to be unconstitutional as against the 'personal liberty' as contemplated under the Article 21 of the constitution. The judgment, however, squarely negated the existence of a fundamental right of privacy, although against a powerful dissenting opinion presented by Justice Subba Rao, who was inclined toward an expansive understanding of liberty encompassing the right to privacy.

Early cases created a narrow and fragmented understanding of privacy, leading to varying interpretations in the following years. But as technology advanced, it fueled government surveillance and data aggregation issues, and demands for re-examining privacy in the context of the Constitution intensified.

JUSTICE K.S. PUTTASWAMY V. UNION OF INDIA (2017): A MILESTONE IN PRIVACY JURISPRUDENCE

The historic moment was in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), when the nine-judge bench of the Supreme Court by a unanimous ruling declared that privacy is a fundamental right of the Constitution, that is, under Part III, namely Articles 14, 19, and 21 of the constitution. The reference was made in the aftermath of questions being raised over the Aadhaar scheme, which raised serious questions of biometric data collection and implications of surveillance.

The Court categorically overruled MP Sharma[8] and Kharak Singh[9] and held that they no longer represented the correct legal position. The majority opined that privacy is a part of the right to life and liberty of person under Article 21 of the Indian Constitution and is also enshrined in other rights like freedom of expression and dignity. The court gave a broad definition of privacy, including decisional autonomy, bodily integrity, and informational privacy.

Justice Chandrachud, writing for the majority, established the right to privacy on the basis of the principle of 'constitutional morality', contending that the Constitution had to adapt to safeguard individual freedom in a contemporary democratic state. The Court was adamant that privacy went beyond elitist notions, being a necessary component of the dignity and autonomy that constituted the birthright of every individual.

8 MP Sharma v. Satish Chandra, AIR 1954 SC 300.
9 Kharak Singh v. State of Uttar Pradesh, AIR 1962 SC 1295.

Notably, the ruling set out the 'three-pronged proportionality test' for ascertaining state actions that violate privacy rights:

1. There must be a legitimate state purpose;
2. The techniques used must be proportionate and necessary to the aim.
3. It is necessary to have adequate procedural safeguards.

This ruling gave a foundation for reassessing Aadhaar and other government-funded data collection regimes. Moreover, it acted as a catalyst for additional constitutional scrutiny in areas like sexual autonomy, surveillance, and data protection. Lastly, Puttaswamy (2017)[10] revolutionized the Indian constitutional rights landscape by elevating privacy from a presumed claim to a robust, enforceable right. Not only did it reverse decades of precedent, but it also provided a principle-based framework for future adjudication in the age of the digital world.

THE AADHAR SCHEME

THE AADHAR INITIATIVE

I. Objectives and Operation

The Aadhaar concept came into being in 2009 by the Government of India as a significant endeavor to provide every citizen of the country with a unique identification number. It was being run by the Unique Identification Authority of India (UIDAI), an administrative organization functioning under the Planning Commission, which has now been reorganized as NITI Aayog. The core purpose of the project was to enhance efficiency, transparency, and accountability in the implementation of government welfare schemes by eliminating the existence of duplicate and non-existent beneficiaries.

The Aadhaar number is issued after recording the demographic information, including name, gender, age, mobile number, and mobile address, and biometric information, including fingerprints, photographs, and iris scans. The number, after being issued, is used for verification in numerous services. Such services as bank account opening, obtaining mobile SIM cards, receiving subsidies under schemes like LPG and PDS, and filing income tax returns are some among numerous.

10 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.

Even as Aadhaar was kept voluntary, its application to core services and many sectors has made it de facto mandatory for broad sections of society. The ubiquity of Aadhaar has also raised intense controversies about the role of the state in data management and the limits of techno solutions in governance.

II. Regulatory Framework

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016[11] then provided legislative backing for the project. It passed as a Money Bill under Article 110 of the Constitution, the act avoided the scrutiny stage of the Rajya Sabha, something that was later challenged in the Supreme Court but ultimately affirmed by a narrow majority in Puttaswamy judgement(2018).

The Aadhaar Act made UIDAI a legal body and authorized it to assign Aadhaar numbers to residents voluntarily submitting their demographic and biometric information. The Act authorizes UIDAI to make policy, set standards, regulate authentication processes, and offer guarantees of identity information security.

Major provisions are:

1. Section 7[12] which mandates Aadhaar authentication to claim subsidies and benefits drawn from the Consolidated Fund of India. This is essentially the foundation architecture of the welfare delivery system that has been initiated with the Aadhaar model.
2. Section 29[13] which prevents sharing of key biometric data and Aadhaar identifiers without consent.
3. Section 33[14] permits disclosure of information for national security purposes, but with very few safeguards, raising the fears of untrammeled executive discretion.

11 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).

12 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 7, No. 18, Acts of Parliament, 2016 (India).

13 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 29, No. 18, Acts of Parliament, 2016 (India).

14 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 33, No. 18, Acts of Parliament, 2016 (India).

4. Section 57[15] (since struck down) originally permitted private parties to authenticate using Aadhaar. This was deemed to be unconstitutional in Puttaswamy (2018) due to the misuse of information and the absence of proportionality.

The Aadhaar Amendment Act, 2019 reinstated private sector utilization of Aadhaar on a voluntary basis, subject to approval from the individual. Even though the amendment brought more oversight, its structure still does not have independent regulatory oversight and judicial protection according to the critics.

III. Privacy Concerns: Data Collection, Storage, and Profiling

For all of its declared goals, the Aadhaar scheme has always raised basic questions about the privacy, autonomy, and informational control of citizens. These questions are threefold:

1. Data collection and consent

The scope and character of the information gathered under Aadhaar are unprecedented. Biometric details as opposed to cards or passwords are permanent and irrevocable. They cannot be altered once compromised. While Aadhaar asserts itself to be consent based, the linking of Aadhaar to critical services like food rations, pensions, and mobile connectivity makes consent illusory or coercive.

There have been instances of people being deprived of their rights based on biometric differences or system errors, leading to exclusion and digital illiteracy, especially for vulnerable groups.

2. Risk of Surveillance and Data Retention

Although the Aadhaar Act prohibits the storage of authentication transaction data, the UIDAI holds onto authentication metadata, such as time, location, and mode of authentication. This allows for the reconstruction of personal behavior patterns and thus eases mass surveillance. The uncertainty regarding retention policies, third-party access, and auditing mechanisms only adds to the problem. Most importantly, there is no prior judicial sanction required for law enforcement or intelligence agencies accessing data under national security exceptions.

3. Profiling and Function Creep

The depth of Aadhaar penetration across various sectors banking, telephony, health, taxation, education has generated an interlinked data ecosystem that can create rich behavioural profiles. This type of function creep, where data gathered for one use is used for another, is a severe threat

15 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 57, No. 18, Acts of Parliament, 2016 (India).

to informational self-determination. Centralized storage of sensitive personal information increases the risk of data leaks. There have been a number of cases of Aadhaar data leaks from government websites, such as the release of millions of records of beneficiaries, students, and pensioners. Furthermore, the absence of viable solutions and institutional remedies for redress reinforces the power imbalance between the state and the individual.

JUDICIAL SCRUTINY OF AADHAR

Constitutional validity of the Aadhaar scheme was examined in Justice K.S. Puttaswamy (Retd.) v. Union of India (2018)[16], after acknowledgement of the right to privacy as a fundamental right in Puttaswamy (2017)[17]. The main questions before the five-judge Constitution Bench were whether the Aadhaar Act, 2016[18] infringed the right to privacy, facilitated surveillance, and whether its enactment as a Money Bill was within the Constitution.

I. Majority Opinion (Justice Sikri)

The majority judgment, written by Justice A.K. Sikri (on behalf of himself, CJI Dipak Misra, and Justice Khanwilkar), confirmed the constitutional validity of the Aadhaar Act, with Justice Bhushan did agree in separate terms. The Court held that the Aadhaar project aimed to advance a legitimate state interest of ensuring the smooth delivery of social welfare benefits and weeding out fake or duplicate identities from government databases. It ruled that Aadhaar was not violating the fundamental right to privacy in an unconstitutional way.

The Court held that the Aadhaar Act contained adequate protection against misuse of data. Biometric verification was minimally intrusive and did not lead to collection of intrusive personal data. Section 7[19], requiring Aadhaar authentication in order to receive subsidies and welfare benefits, was upheld as a constitutional way of securing targeted delivery.

The Court read down or struck down some provisions, however section 33(2)[20], which permits disclosure of information on national security grounds by executive action, was struck down for

16 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2018 SC 1841.
17 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.
18 The Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
19 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 7, No. 18, Acts of Parliament, 2016 (India).
20 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 32(2), No. 18, Acts of Parliament, 2016 (India).

the absence of judicial supervision. Also, section 57[21], which permits private companies to make use of Aadhaar for authentication, was declared unconstitutional, for reasons of disproportionate invasion of privacy and facilitating commercial exploitation. Sections requiring Aadhaar linking with bank accounts and mobile numbers were invalidated for absence of legislative support and for being overly wide.

II. Dissenting Opinion (Justice D.Y. Chandrachud)

Justice D.Y. Chandrachud delivered a forceful and comprehensive dissenting judgment which differed with the majority on procedural as well as substantive constitutional bases.

His main criticisms were money Bill classification, he was of the opinion that the Aadhaar Act could not have been enacted as a Money Bill under Article 110[22], since the majority of provisions of the Act did not directly relate to the Consolidated Fund of India. Its enactment in this way was a travesty of the Constitution's basic structure and parliamentary practice.

Justice Chandrachud cautioned that Aadhaar established a ‘concentration of personal data in the hands of the State without adequate accountability’, setting the stage for surveillance and profiling of data. He dismissed the contention that biometric authentication was proportionate, considering the danger of data leaks, function creep, and exclusion. He commented that Aadhaar, while presented as being voluntary, had become coercively compulsory in reality, eroding personal autonomy and the constitutional value of dignity. Chandrachud's dissent is still widely respected in policy and academic circles for its focus on constitutional morality, federalism, and individual rights in the digital age.

III. Application of the Proportionality Test

The Court's examination of the constitutionality of Aadhaar was informed by the proportionality test, as set forth in Puttaswamy (2017)[23], which entails four prongs, i.e., the Court recognized welfare delivery and administrative effectiveness as legitimate.

- Rational connection: It was determined that biometric authentication was rationally connected to weeding out duplicate beneficiaries.
- Necessity: The Court held that no less intrusive alternatives existed for targeting welfare.

21 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, § 57, No. 18, Acts of Parliament, 2016 (India).

22 INDIA CONST. art. 110.

23 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2017 SC 4161.

- Balancing of rights: Invasion of privacy was considered justified when balanced against the public interest of effective subsidy distribution.

Nonetheless, this application has been criticized by scholars as weak and formalistic with too little examination of less intrusive alternatives, errors of exclusion, and the absence of meaningful consent.

The Aadhaar judgment is a balancing act between state interests in governance through the digital medium and the constitutional guarantee of privacy. Though the majority affirmed Aadhaar's essence, it tried to construct guardrails around its use. The dissent was a constitutional alert against the undermining of civil liberties in the wake of technological growth. With India's digital state becoming more entrenched, the jurisprudential tensions revealed in Puttaswamy (2018)[24] continue to define debates on surveillance, consent, and informational autonomy.

LEGISLATIVE AND REGULATORY FRAMEWORK

The path of privacy laws in India particularly in the wake of the decision like in Justice K.S. Puttaswamy (Retd.) v. Union of India, is a regime model attempting to reconcile the competing imperatives of digital rule, national security, welfare dispensation and constitutional safeguards of privacy. At the heart of the model are two key pieces of legislation: the Aadhaar Act of 2016 and the Digital Personal Data Protection Act of 2023. Though these acts together attempt to establish frameworks for the protection and processing of personal data, their passage and implementation reveal significant lacunae in responsibility, enforcement, and institutional independence.

The Aadhaar Act 2016, enacted as a Money Bill, granted the legislative cover to the Aadhaar project, such as the issuance of a 12-digit unique identification number to Indian residents on the basis of their biometric information. The overarching principle of the Act was to facilitate the delivery of subsidies and benefits paid out of the Consolidated Fund of India on a targeted basis. Section 7 of the Act made Aadhaar-based authentication mandatory for the delivery of such welfare benefits. The Act, however, contained provisions such as Sections 57 and 33(2) which permitted private actors to utilize Aadhaar and disclosed information on the basis of national security, with insufficient checks. These provisions were being subject to test in the Puttaswamy

24 K.S. Puttaswamy (Retd.) v. Union of India, AIR 2018 SC 1841.

judgment, where the Supreme Court upheld the substance of the Act but struck down or read down provisions which were found to violate the right to privacy.

In the wake of the Supreme court's judgment, the Aadhaar and Other Laws (Amendment) Act, 2019[25] was enacted. The amendments were meant to reinforce the voluntariness of Aadhaar and remove concerns about the use of biometric data by private enterprises. Significantly, the amendment addressed voluntary Aadhaar authentication by telecommunications firms, banks and other service providers, subject to the informed consent of the user and the consent of the UIDAI. The legislation also introduced offline authentication processes and set up oversight mechanisms, such as the Appellate Tribunal and the Aadhaar Adjudicating Officer. Critics, however, are of the opinion that the amendments de facto reinstalled the commercial exploitation of Aadhaar under the cover of voluntariness and thus violated the Puttaswamy judgment. In addition, the UIDAI, which is also the operator and regulator of the Aadhaar system, has been accused of failing to be transparent and independent and thus undermining critical institutional checks and balances.

Meanwhile, the need for an effective data protection regime led to the enactment of the Digital Personal Data Protection Act (DPDP), 2023[26]. The Act was the product of multiple drafts of data protection bills since Puttaswamy (2017) is India's first legislation on the processing of digital personal data. The Act covers both public and private data fiduciaries and follows a rights-based framework of data protection with focus on the principle of consent. It gives data principals the right of access, correction, erasure, and grievance redressal and places obligations on data fiduciaries to provide lawful and secure processing. It also creates a Data Protection Board of India, which will hear concerns and impose penalties for defaults. But the DPDP Act has been subjected to widespread criticism for its wide-ranging State-friendly exemptions. Section 17 of the Act, for example, gives the Central Government the power to exempt any public agency or body from the Act on grounds of public order, sovereignty or friendly relations with foreign nations. Unlike the safeguards in Puttaswamy (2017) judgement which ensured that the principles of legality, necessity, and proportionality remained at the center, these exemptions are not reviewable by parliament or the courts. Something to be concerned about in terms of the

25 The Aadhaar and Other Laws (Amendment) Act, 2019, No. 14, Acts of Parliament, 2019.
26 The Digital Personal Data Protection Act (DPDP), 2023, No. 22, Acts of Parliament, 2023.

dangers of state surveillance gone unchecked, especially after earlier revelations about the use of Pegasus spyware and secret data collection by public authorities.

In addition, the Aadhaar system and the DPDP Act's enforcement mechanism is institutionally very weak. UIDAI has never established effective grievance redressal mechanisms. Citizens who have been incorrectly excluded from benefits based on technical glitches or biometric mismatch have limited legal recourse. The absence of an independent and well-funded watchdog institution also ensures low accountability for the data breaches. The Data Protection Board under the DPDP Act is wholly-appointed and executive-dominated, basically raising the question of its independence and impartiality in the case of government agencies.

Another issue is the absence of obligatory data localization provisions. Earlier versions of the data protection bill had contained stringent provisions for the storage and processing of sensitive personal data within India's territorial jurisdiction; the 2023 Act watered down these provisions substantially. The law allows the government to prescribe nations to which data can be exported without restriction, without clear criteria or public discussion. In a progressively integrated global digital economy with increasingly ubiquitous cross-border data flows, the lack of localization requirements erodes national sovereignty and puts the security of user data at risk. Moreover, this scenario makes it difficult to impose legal remedies and exercise jurisdiction over foreign actors in cases of data misuse or infringement.

Finally, the legal architecture still suffers from the absence of harmonization of sectoral regulation. The Aadhaar system, IT Rules, telecommunication regulations do not have proper coordination. This results in fragmentation of regulations, uncertainty in compliance, and differing levels of protection across industries. Despite the DPDP’s intention to have an integrated approach, its success lies in the subordinate legislation being accurate and the Data Protection Board's working efficiency. In short, while the Aadhaar Act and the DPDP Act are significant leaps forward in institutionalizing data protection in India, they fall short of constitutional ideals. The wide discretion given to the State, along with inadequate enforcement and oversight mechanisms, continue to imperil the privacy rights of Indian citizens. A good legislative framework need not be motivated merely by efficiency and innovation but by constitutional ethics, accountability, and human dignity in the digital age.

CRITICAL ANALYSIS

The Aadhaar programme, originally a tool for inclusive governance and fair redistribution of welfare has evolved into a complex system generating enormous constitutional and ethical issues especially in the wake of the Supreme Court's privacy jurisprudence. The decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) laid a foundation to safeguard the constitutional right to privacy based on principles of legality, necessity, proportionality, and procedural safeguards. The main challenge is to determine whether the Aadhaar system, particularly post-Puttaswamy and amendments to the legislation, actually complies with these principles or only seems to do so in theory but not in practice.

To start with, a major issue with Aadhaar is its conformity to the proportionality test laid down in Puttaswamy judgement. The Supreme Court in Puttaswamy judgement upheld the constitutional validity of Aadhaar by a whisker, holding that the scheme was serving a legitimate aim viz., the targeted delivery of government subsidies and was justified by legislative authorization through the Aadhaar Act of 2016. The proportionality test, however, requires that not only is a measure, but also must be the least intrusive measure available, bear a rational relation to the purpose sought to be promoted, and have inbuilt safeguards against abuse. Critics argue that Aadhaar specifically fails on the latter two. The Aadhaar system has persistently been beset by problems of data breaches, information leaks, and unauthorized access. In spite of repeated assurances by the Unique Identification Authority of India (UIDAI), the vulnerabilities reflect inherent weaknesses in infrastructure of security and in regulation enforcement.

Secondly, the question of consent also becomes a central issue. Although the 2019 amendments ensured ‘voluntariness’ of Aadhaar usage by private parties subject to user consent and offline verification, these protection mechanisms are mostly illusory in practice. In any legal setting, consent must be informed, voluntary, and capable of being withdrawn. However, several reports and RTI queries suggest that Aadhaar has been made de facto compulsory, particularly in the domains of education, banking, employment and telecommunication. Public and private authorities prefer to demand Aadhaar details without making reasonable alternative arrangements. This effectively converts the so-called consent into compulsory, particularly among the economically weaker sections of society who are not in a position to exercise the bargaining power or legal acumen required to decline such demands. This sort of scenario runs counter to the autonomy and dignity embedded in the right to privacy.

One of the primary concerns pertains to the ability of Aadhaar to facilitate a surveillance state. The architecture of the Aadhaar system necessarily creates a demographically and biometrically rich centralized database. All authentication requests whether it is to receive rations, enter educational institutions, or avail healthcare services are logged and retained creating vast digital footprints. Though UIDAI claims that Aadhaar does not track movement or usage, the system architecture enables the intersection of different databases, facilitating profiling across sectors. The absence of independent audit and expeditious judicial review leads to a culture permitting possible misuse of surveillance, especially that of an unaccountable government. In the Puttaswamy judgement, the Supreme Court downplayed such risks, with heavy dependence given to the assurances of UIDAI; however, empirical data gathered subsequently show that the surveillance system is not a theoretical possibility but it is an operational reality.

The comparative analysis of constitutional and data protection paradigms unveils deep implications. The General Data Protection Regulation (GDPR) of the European Union is universally regarded as the gold standard of data privacy. The GDPR requires that consent be voluntary, clear and informed, while it equips individuals with a robust set of rights such as access, rectification, portability and imposes draconian fines for non-compliance. Crucially, the enforcement of GDPR is entrusted to independent supervisory authorities, which are outside the executive domain. By contrast, India's Digital Personal Data Protection Act of 2023 has been faulted for granting sweeping exemptions to state agencies on vaguely defined grounds like ‘national security’ and ‘public order’. Section 17 of this Act empowers the central government to exempt any department from the provisions of the Act, thereby threatening to render unregulated surveillance institutionalized in direct contravention of the principles announced by the Puttaswamy framework.

The United States, while not having a broad federal data protection law, provides a second comparative model in its post-Snowden law. The Snowden revelations prompted the USA FREEDOM Act, which limited bulk metadata collection and mandated disclosures and accountability. The U.S. also has a relatively strong civil society and judiciary that can be leveraged to combat unconstitutional surveillance. In India, the UIDAI is both the operator and regulator of Aadhaar, creating a conflict of interest. The Data Protection Board established under

the DPDP Act is not independent, as it is wholly appointed by the executive, which seriously calls into question its ability to act against government abuse.

One of the key structural defects is the absence of robust accountability mechanisms. No redressal mechanisms are transparent to the individuals whose data is being misused or are being denied benefits because of Aadhaar-linked errors. There have been several instances where the beneficiaries have been denied rations or pensions because of authentication failure, but compensation or relief has been meager or nil. This also raises doubt about the efficacy of procedural mechanisms and due process both which are necessary under the privacy doctrine set out in Puttaswamy. In summary, although Aadhaar may invoke constitutional validity based on the approval of the Supreme Court and amendments to the law, the reality on the ground is one of disquieting disharmony between principle and practice. The Puttaswamy judgment provided a constitutional protection to privacy, dignity, and autonomy in the digital world. Aadhaar, in its current form, erodes these values through coercive consent, lack of enforcement, and a possible surveillance state. Unless India institutes serious institutional reforms providing independent oversight, enhancing user empowerment, and making it transparent, Aadhaar can end up being a cautionary tale of digital stewardship unaccountable to the constitution.

CONCLUSION AND SUGGESTION

The recognition of the right to privacy as a constitutional right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) was a major turning point in the development of Indian constitutional law. In holding that the privacy is a necessary part of life and liberty as conceived under Article 21, the Supreme Court had lay down a bedrock for a digital society that is attuned to individual freedoms. Nevertheless, the Aadhaar program has tested the strength of this right in an increasingly digitizing welfare state. While Aadhaar aims to facilitate the targeted delivery of services, remove inefficiencies, and make administration more effective, its implementation has generated critical questions regarding consent, proportionality, government surveillance, and safeguarding of personal data.

The Aadhaar programme has not completely ceased from abiding by the constitutional standards set in the Puttaswamy judgment. In spite of legislative backing and the partial endorsement of the judiciary in Puttaswamy judgement, ongoing practical issues in the form of implicit coercion, poor data protection measures, and potential surveillance continue to exist. The theoretical

recognition of privacy contrasts with the real situation, in which the use of welfare services often depends on the Aadhaar linkage, consent procedures are opaque or non-existent, and independent regulation is deficient or absent. Such concerns are aggravated by a decrease in legislation mostly under the Aadhaar Amendment Act, 2019[27], and the Digital Personal Data Protection Act, 2023[28] granted by the state with few protection mechanisms.

The comparative analysis brings India's data deficit in the global context of privacy norms into sharp focus. The GDPR of the European Union, for example, has consolidated robust individual rights, keeps purpose limitation central, and requires independent regulatory oversight. India's data protection regime, with the executive being given overarching powers with minimal checks, institutionalises a deficit. The Aadhaar programme, in the context of Puttaswamy, therefore, indicates a disjunct between constitutional normative commitments and arrangements brought into effect.

In light of these findings, several reforms are urgently required to align Aadhaar with privacy jurisprudence and constitutional values:

1. Strengthen Consent Mechanisms:

Consent should be explicit, specific, and revocable. There has to be clear communication of purpose, alternatives, and refusal consequences for all Aadhaar-based authentications. UIDAI should create a uniform consent architecture based on international best practices, like GDPR's ‘opt-in’ approach.

2. Independent Regulatory Oversight:

The UIDAI, as the implementing authority, cannot be the sole arbiter of privacy protection. A separate Data Protection Authority with financial and functional independence is urgently required to monitor compliance, rule on violations, and protect data subjects' rights. The current framework under the DPDP Act falls short of this need.

3. Limitation of Purpose and Minimisation of Data:

Aadhaar usage has to be limited to essential welfare purposes as originally envisioned. Aadhaar linking in the absence of regulation to services like banking, telecom, or education can lead to a surveillance state. Purpose limitation and data minimisation need to be enshrined and implemented to avert profiling.

---

27 The Aadhaar and Other Laws (Amendment) Act, 2019, No. 14, Acts of Parliament, 2019.

28 The Digital Personal Data Protection Act (DPDP), 2023, No. 22, Acts of Parliament, 2023.

4. Strong Data Security and Breach Redressal:

UIDAI needs to enhance cybersecurity measures, implement end-to-end encryption, and release transparency reports on data breaches. The citizens should be provided with an easily accessible grievance redressal mechanism in the form of the right to inform and the right to compensation.

5. Judicial Review and Legislative Safeguards:

Aadhaar's future applications need to be strictly tested by the courts under the Puttaswamy paradigm. The lawmaking authority needs to pass more specific interpretations of “reasonable restrictions” and remove ambiguous exemptions that help executive abuse.

6. Privacy by Design: Privacy needs to be integrated at the architectural level of the Aadhaar system. This involves decentralised storage, anonymisation of data, and technical protection against mass surveillance. Regular privacy impact assessments need to be made mandatory for all Aadhaar-related activities. In conclusion, Aadhaar is both a technological promise and a constitutional conundrum. Its ongoing application must be balanced through a privacy-friendly legal framework that protects individual agencies without sacrificing governance objectives. Puttaswamy cannot be an aspirational statement; it needs to be a living, enforceable fact. A constitutional democracy needs to ensure that technological progress serves civil liberties, not supersedes them.