ISSN: 3048-8702(O)

LLRJ

LEX LUMEN RESEARCH JOURNAL

VOLUME 2 - ISSUE 3

2026

LEX LUMEN RESEARCH JOURNAL-ISSN:3048-8702
Open Access, Double blind-Peer Reviewed Law Journal, Licensed by-CC BY-NC-SA.
Editor-in-Chief: Prof. (Dr). Razit Sharma, Publisher: Mrs. Rachana

Volume-2, Issue-3 ***Pages: 500-541***

DIGITAL IDENTITY, AADHAAR, AND THE ARCHITECTURE OF THE INDIAN SURVEILLANCE

By- **Ananya Mishra**[1]

ABSTRACT

Digital identity systems have brought a paradigm shift in governance, welfare delivery, and citizen-state relationships in the contemporary era[2]*. India's Aadhar scheme, pioneered by the Unique Identification Authority of India, is considered to be the world's largest biometric identity scheme*[3]*. Although Aadhar has earned laurels due to its contribution to efficient welfare delivery and economic empowerment through financial inclusion, it has also brought with it several concerns related to privacy, surveillance, cybersecurity, and freedom. This research aims at analysing the impact of Aadhar scheme on digital identity and surveillance in general. The analysis will focus on various aspects of this system, including its legal and constitutional ramifications, along with the implications of the landmark judgment in* ***Justice K.S. Puttaswamy v. Union of India*** *case*[4]*. This paper asserts that there exists a threat of a surveillance state owing to the techno-legal infrastructure established through Aadhar scheme.*

KEYWORDS: Aadhaar, Digital Identity, Surveillance, Privacy, Data Protection

[1]**Student, Atal Bihari Vajpayee School of Legal Studies, Chhatrapati Shahuji Maharaj University, Kanpur.**

[2] World Bank, Digital Identity Toolkit (2018)

[3] Unique Identification Authority of India, Aadhaar Overview.

[4] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

Volume-2, Issue-3 *Pages: 500-541*

INTRODUCTION:

Background of the Study

The rise of technological innovations has changed the way in which states interact with their citizens. One such innovative aspect that has been developed in the realm of state-citizen interaction is that of digital identification systems, whereby a method of creating a unique and verified identity can be developed. Digital identification systems have been employed for several reasons including governance, financial inclusion, service delivery, and the improvement of national security architecture.

In India, the development of a digital identification system through Aadhaar marks a revolutionary step in the development of identity systems. It is a unique biometric identification system in India which assigns every citizen or resident a 12-digit unique number based on their biometric information such as fingerprints and iris scanning[5]. As per the records, Aadhaar has more than 1.17 billion unique numbers assigned to citizens of India.[6]

Though Aadhaar was initially developed to streamline welfare delivery and reduce duplication of identities, its application today has made it almost a mandatory requirement in many other fields as well including banking, telecommunication, and taxation.[7]

However, the universal application of social credit systems has led to various legal, constitutional, and moral issues. The storage of huge volumes of personal data makes one question the privacy of individuals and their protection against any misuses[8]. In addition, the possibility to monitor and verify the identity of people has raised a debate on a surveillance-based approach to government.[9]

Statement of the Problem

[5] Unique Identification Authority of India, Aadhaar Technology and Architecture
[6] Unique Identification Authority of India, Aadhaar Dashboard Statistics
[7] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[8] Usha Ramanathan, "Aadhaar and the Surveillance State", 32 National Law School of India Review 45 (2014)
[9] David Lyon, Surveillance Studies: An Overview (Polity Press, 2007)

Volume-2, Issue-3 *Pages: 500-541*

While Aadhaar has received much acclaim for streamlining administrative processes and minimizing leakages in welfare programs, it comes with serious implications for civil liberties and democratic norms. The construction of an integrated data bank housing highly sensitive personal and biometric details has raised concerns over possible misuse and abuse of the same by both governmental and non-governmental entities.

This concern becomes more worrisome when we consider the growing dependence on Aadhaar for accessing vital services. Even though the program began as a voluntary exercise, its mandatory use for financial transactions, tax payments, and even mobile communication services renders it almost mandatory for users. In effect, citizens might be forced to provide their personal information to gain access to necessary services. A third concern that emerges from this program pertains to surveillance. The repeated use of Aadhaar cards to authenticate one's identity produces a wealth of metadata, which could expose an individual's behavioral patterns and transaction history.[10] The cumulative effect of such metadata collection allows for profiling and surveillance and transaction history.[11] The cumulative effect of such metadata collection allows for profiling and surveillance of individuals. In the context of the above, the central issue under investigation in this paper is whether the Aadhaar digital identification system plays any role in building a surveillance state in India, as well as whether

there are enough protections in law for individual rights.

Objectives of the Study

The central aim of this research paper is to provide a critical analysis of the position occupied by Aadhaar within the wider context of digital identity and surveillance. This research paper attempts to critically evaluate both the advantages and

[10] Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019)
[11] Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019)

Volume-2, Issue-3 *Pages: 500-541*

disadvantages of Aadhaar with specific reference to its constitutional and legal dimensions.

The objectives of the research paper can be listed as follows:

- To comprehend the meaning of digital identity and its development
- To understand the nature and operation of Aadhaar along with its intended purpose
- To explore the constitutional legitimacy of Aadhaar in relation to privacy rights
- To evaluate the degree of surveillance facilitated by Aadhaar
- To determine whether existing laws are adequate in addressing the problems raised by Aadhaar.
- To suggest reforms for ensuring a balance between governance efficiency and individual rights

Research Questions

The study will aim to answer the following key research questions so as to meet the stated objectives:

- **Does the Aadhar system set up an environment that makes possible the surveillance activities by the state?**
- **To what degree is the Aadhar system consistent with the fundamental right to privacy according to the case of Justice K.S. Puttaswamy v. Union of India[12]?**
- **Are the current laws adequate enough in protecting Aadhar information from misuse?**
- **What is the impact of Aadhar on the citizen-state relationship in a democracy?**

Research Methodology

[12] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1

Volume-2, Issue-3 *Pages: 500-541*

The research will follow a doctrinal approach involving an analysis of various issues in relation to the topic being discussed. The research mainly relies on secondary sources of data such as legislation, court rulings, literature and scholarly publications. An analysis of the provisions of certain legislations, especially the **Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016**, would be carried out in order to analyze the law relating to the issue. Rulings of the judiciary, especially the rulings of the Supreme Court of India, will be critically analyzed in the process of analyzing the constitutional dimension of Aadhaar[13].

Furthermore, this research will also employ a comparative approach where different perspectives from theoretical studies of surveillance and digital governance shall be analyzed.

Scope and Limitations of the Study

The scope of the current research is confined to the study of Aadhaar, as a digital identity management system, in India. In particular, the study will analyze the legal, constitutional, and ethical considerations of Aadhaar in connection with privacy and surveillance. Even though global digital identity management systems will receive some attention from the perspective of comparison, an extensive investigation of international considerations will not form a part of this study. The same applies to the technical issues concerning data encryption and cyber security. The scope of the analysis will also be constrained by the accessibility of data and judgments in this regard. With rapid development of digital governance, not all changes in this area can be included into the present study.

Significance of the Study

The importance of the current study lies in its efforts to critically address the issue of one of the most significant innovations in modern Indian governance. In its essence, Aadhaar reflects a remarkable fusion of law, technology, and public policy, which

[13] K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1

Volume-2, Issue-3 *Pages: 500-541*

raises important issues that go beyond administrative effectiveness. Addressing Aadhaar from the perspectives of surveillance and privacy, the current study will contribute to a wider discussion about the nature of governance in a modern digital society. As part of the research into these topics, it becomes critical to consider ways of ensuring that state policies do not undermine people's rights as part of a well-functioning democratic society.

The rule of law requires maintaining a certain balance between the interests of the state and citizens.[14]

CONCEPTUAL FRAMEWORK OF DIGITAL IDENTITY AND SURVEILLANCE:

Meaning and Nature of Digital Identity

In the modern world, digital identity is defined as the virtual manifestation of one's identity, formed by a set of attributes in a digital database[15]. While traditional identity systems depend on physical documents, like passports or voter identification cards, digital identities involve databases containing personal information about the individual.

A typical digital identity includes:

- Biometric information, such as fingerprint scans, iris recognition, and facial recognition technology
- Personal details, such as full name, birthday, gender, and current residence
- Log-in information, such as passwords, PIN numbers, and one-time passwords (OTPs)
- Data regarding transactions and behavioral patterns

The main difference between traditional and digital identities is that the latter enables real-time authentication and verification processes[16]. Therefore, the use of digital

[14] Maneka Gandhi v. Union of India, (1978) 1 SCC 248
[15] World Bank (2018)
[16] Unique Identification Authority of India, Aadhaar Technology and Architecture

Volume-2, Issue-3 *Pages: 500-541*

identities can improve the efficiency of service delivery by governments. Additionally, the state will be able to verify citizens' identities more accurately, increasing the effectiveness of governance systems.

At the same time, the use of digital identities carries many risks. Physical documents can be lost or stolen, but their use does not depend on centralized systems. Digital identities, on the other hand, are dependent on databases, which can be hacked or accessed without authorization. Moreover, the combination of several different types of data in a single digital identity can lead to excessive profiling and surveillance.[17]

Evolution of Digital Identity Systems

Identity management has undergone tremendous changes over time. In traditional identity management schemes, there was no centralization or integration of identities. Multiple documents were required for individuals, each issued by an authority.

There have been various motivations for countries around the world to develop their digital identity management systems, including effective governance, enhanced national security, and improved financial inclusion.[18] The Aadhaar system in India is considered a unique example of a digital identity management scheme due to its massive size and biometric verification.[19]

The emergence of digital identity management systems is a part of the wider process of the development of data-driven governance[20], where decisions are made based on data analysis. It increases efficiency but simultaneously gives more power to those who control the infrastructure of data.

Concept and Dimensions of Surveillance

Surveillance is the process of systematically observing people, communities, or events to obtain information.[21]Traditionally, surveillance was performed using physical

[17] Daniel J. Solove, Understanding Privacy (Harvard University Press, 2008)
[18] World Bank (2018)
[19] Unique Identification Authority of India, Aadhaar Overview
[20] OECD, Digital Government Studies (2020)
[21] David Lyon, Surveillance Society: Monitoring Everyday Life (Open University Press, 2001)

Volume-2, Issue-3 *Pages: 500-541*

methods by law enforcement agencies. But in today's modern world, surveillance has evolved significantly, with the use of advanced techniques and equipment for information collection.

There are various types of modern surveillance:

- State surveillance, which is done by government authorities for national security and governance
- Corporate surveillance, in which private firms gather and analyze user information for their benefit
- Mass surveillance, which is large-scale surveillance of citizens[22]

Digital surveillance works on the principle of collecting data created by people in their day-to-day activities with digital devices. Such data includes communication records, geographic coordinates, financial transactions, and social media usage.

Theoretical Perspectives on Surveillance

There have been various scholarly studies on the phenomenon of surveillance, offering significant insights regarding the effects of such technologies on society.

Perhaps the most widely recognized theory is the Panopticon proposed by Michel Foucault[23]. The idea behind this term involves a prison design wherein criminals could be seen at all times without necessarily being monitored, which would force them to self-regulate their behavior[24]. Applying this metaphor to the issue of digital identities, the Panopticon refers to the way people modify their behavior when they know that it is possible to be under surveillance.

Moreover, the phenomenon of Surveillance Capitalism put forward by Shoshana Zuboff[25] needs to be noted. In essence, the theory assumes that the modern world relies heavily on data, which represents an economic value in itself. According to Zuboff, corporations and governments collect personal data for behavioral

[22] David Lyon (2001)
[23] Michel Foucault, Discipline and Punish: The Birth of the Prison (Vintage Books, 1977)
[24] Ibid
[25] Shoshana Zuboff, The Age of Surveillance Capitalism (PublicAffairs, 2019)

Volume-2, Issue-3 *Pages: 500-541*

predictions, which is one more perspective in regard to surveillance as a means of influencing people. It is necessary to understand these theoretical backgrounds to examine how technology like Aadhaar may operate as a system of control.

Relationship Between Digital Identity and Surveillance

Surveillance and digital identity are related in very many ways. As much as the primary role of digital identity management system is identification and providing services, there is always a surveillance aspect associated with it[26]. There are several factors that bring out the link between the two as follows:

To start with, digital identities make it possible to keep track of behavior. Each and every time someone uses his/her digital identity to authenticate him/herself, information is kept somewhere for future analysis.

Secondly, it allows for data aggregation where information from different areas such as banking sector, health care facilities and telecommunication companies, among others can be linked to the individual. This builds up a detailed profile which increases surveillance possibility.

Lastly, they increase government capability for surveillance. Through aggregation, government can be able to monitor people at a much larger scale due to availability of information.[27]

Digital Identity, Power, and Governance

The use of digital identity systems completely changes the dynamics between the state and its citizens. While previously identity has been a means of recognition, in the digital age, identity is also an instrument for control and management.[28]

Some aspects that change the dynamic of governance when using digital identity systems include:

- Control over data due to centralization of the information

[26] David Lyon (2007)
[27] OECD (2020).
[28] Julie E. Cohen, Between Truth and Power (Oxford University Press, 2019)

Volume-2, Issue-3 *Pages: 500-541*

- Loss of autonomy when dependent on technological systems
- Automation of the decision-making process due to data analytics

These dynamics raise concerns about accountability and transparency when using data analysis to make decisions, especially since it makes challenging those decisions by individuals difficult.

Risks and Challenges of Digital Identity Systems

While there are many advantages to using digital identity systems, it does come with some risks such as:

- Increased privacy issues because of breaches and abuse of data
- Data breaches resulting from inadequate cybersecurity[29]
- People left out of services because they cannot verify their identity
- Overreach of the use of the system

These challenges highlight the need for robust legal and regulatory frameworks to govern the use of digital identity systems.

EVOLUTION AND DEVELOPMENT OF AADHAAR:

Genesis of Aadhaar

Aadhaar has its roots in the issues related to identity verification and wastage of resources in the welfare schemes. Without an identity verification system prior to the implementation of Aadhaar, there were cases of fraud, leakages in welfare measures such as the Public Distribution Scheme, etc.[30] Taking these issues into consideration, the Government of India decided to create the Aadhaar project in the year 2009 by forming the Unique Identification Authority of India. Nandan Nilekani is the leader of the Aadhaar scheme, who believed that Aadhaar should act as a platform which provides a unique identity to every individual residing in India.

The key goals that Aadhaar had at its outset included:

[29] Privacy International, Digital Identity Report (2019)
[30] Government of India, Public Distribution System Reports

Volume-2, Issue-3 *Pages: 500-541*

- Elimination of duplicate and fictitious identities
- Enhancing the precision of subsidies and welfare programs
- Creation of a valid identity for every resident of the nation

Institutional Framework

The Aadhaar project is overseen by the Unique Identification Authority of India, which operates under the Ministry of Electronics and Information Technology[31]. The tasks of the UIDAI include:

- Enrolment and allocation of Aadhaar numbers
- Maintenance of the Central Identities Data Repository (CIDR)
- Authentication
- Data protection and management

The Central Identities Data Repository[32] forms the backbone of the Aadhaar system[33]. It holds the biometric and demographic information of citizens and responds to authentication queries from different agencies.

Legislative Development

At first, there was no statute governing the implementation of Aadhaar scheme[34]. Lack of legislation had created issues of legality as well as constitutional validity of the scheme. To overcome the above problems, the Parliament passed the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act in 2016[35]. Under the Act, Aadhaar is made legal and a legal framework governing the usage of Aadhaar for providing subsidies, benefits and services from Consolidated Fund of India is made[36].

Main features of the Act are as follows:

[31] Government of India, Allocation of Business Rules
[32] Unique Identification Authority of India, CIDR Overview
[33] UIDAI, Aadhaar Architecture
[34] Usha Ramanathan (2014)
[35] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[36] Constitution of India, Art. 110

Volume-2, Issue-3 *Pages: 500-541*

- Employing a provision for enrollment and issuing of Aadhaar numbers
- The use of Aadhaar for purpose of authentication
- Core biometric information is kept confidential
- Punishment for unauthorized disclosure of data

But making the Aadhaar Act a Money Bill had been criticized by many people.

Judicial Scrutiny and Constitutional Challenges

The Aadhaar scheme has faced intense judicial review, especially concerning its consistency with fundamental rights.[37] The Indian Supreme Court, in the landmark case of Justice **K.S. Puttaswamy v. Union of India**, upheld the right to privacy as a fundamental right under Article 21 of the Indian Constitution. The judgment laid down the principle that any state action dealing with personal information must meet the standards of legality, necessity, and proportionality[38]. It had far-reaching implications on the ongoing controversy about Aadhaar. Later, in **K.S. Puttaswamy v. Union of India** (Aadhaar case), the Supreme Court validated the constitutionality of Aadhaar, although under certain restrictions. The court ruled that:

- The Aadhaar scheme is legal for welfare programmes and benefits
- Mandatory linking with the Permanent Account Number (PAN) card is legal
- The private sector cannot make Aadhaar verification mandatory
- Some provisions in the Aadhaar Act are invalid

It tried to strike a balance between the utility of the Aadhaar scheme and the need to ensure individual privacy. But there was still some ambiguity.

Expansion and Integration of Aadhaar

Since its beginning, the usage of Aadhaar has extended much beyond its initial use for welfare delivery. The scheme has been incorporated in various fields, thereby making it a vital part of the country's digital ecosystem[39].

[37] Gautam Bhatia, The Transformative Constitution (HarperCollins, 2019)
[38] Modern Dental College v. State of Madhya Pradesh, (2016) 7 SCC 353.
[39] World Bank (2018)

Volume-2, Issue-3 *Pages: 500-541*

The areas where Aadhaar has been incorporated include:

- Banking and financial sector, which requires Aadhaar for verification purposes such as Know Your Customer[40]
- Telecommunications sector, which used Aadhaar initially for verifying SIM card details
- The tax department, especially regarding the link-up of PAN cards[41]
- The welfare sector, especially Public Distribution System, LPG subsidy schemes, and MNREGA

These integrations of Aadhaar have made it possible to implement the Direct Benefit Transfer system through which the subsidy money will be transferred to the bank account of the beneficiaries directly. This has helped reduce leakages significantly. But along with that, there are concerns regarding the over-dependence on Aadhaar and exclusion due to authentication problems.

Technological Architecture of Aadhaar

The Aadhaar project is based on a technologically advanced framework[42] that facilitates data gathering, storage, and identification.

Some of the major elements of this framework are:

- Gathering of biometric data, such as fingerprints and iris scanning
- CIDR – the central database that keeps all the identity details
- Identification techniques like biometric identification and One Time Password based authentication
- Application Programming Interface (APIs) facilitating integration with multiple service providers

[40] Reserve Bank of India, KYC Master Directions
[41] Income Tax Act, 1961 (as amended)
[42] UIDAI, Aadhaar Technology Architecture

Volume-2, Issue-3 *Pages: 500-541*

Thanks to this framework, it becomes possible to verify people's identities in real time; however, the centralization of data poses significant problems of data protection and possible monitoring by governmental agencies.[43]

Aadhaar and the JAM Trinity[44]

The JAM Trinity refers to the combination of:

- Jan Dhan bank account
- Aadhar identity proof
- And mobile phone connection

The idea behind the JAM Trinity is to develop an inclusive digital network that can deliver financial services efficiently. The role of Aadhar in this network is very important since it provides a solid base for the system through identification proof.

The positive aspects of the JAM Trinity are many; however, there are some negative aspects too regarding increased linkage of personal information on various platforms.

Criticisms and Challenges in Implementation

However, there have been a number of criticisms surrounding the Aadhaar project:

- Exclusion, whereby people are refused services due to problems in the authentication process
- Security issues relating to leakage of data[45]
- Consent as people do not necessarily know how their data will be used
- Functional creep[46] as the Aadhaar project gets used for purposes other than originally intended

These issues highlight the need for stronger safeguards and more accountable governance mechanisms.

AADHAAR AS A GOVERNANCE TOOL:

[43] Usha Ramanathan (2014)
[44] Government of India, Economic Survey of India (2015–16)
[45] Privacy International, Aadhaar Report (2019)
[46] Privacy International (2019)

Volume-2, Issue-3 *Pages: 500-541*

Aadhaar and Welfare Delivery

One of the key goals of Aadhaar is to enhance the efficacy of the welfare delivery mechanisms in India.[47] The traditional welfare schemes have been plagued by several problems, including duplicity of beneficiaries, corruption, and leakage in the process of delivering benefits. To counter these difficulties, Aadhaar provides an effective solution by offering a unique and authentic identity to all beneficiaries.

With the help of Aadhaar authentication, the government can ensure that the welfare schemes are provided to the right individuals. This mechanism has helped reduce fraud and ghost beneficiaries in various welfare schemes, including the PDS, mid-day meals, and pension schemes. With the introduction of Aadhaar verification into the database of these schemes, the government can remove duplicate identities and clean up the list of beneficiaries.

Additionally, Aadhaar has played an instrumental role in the roll-out of the direct benefit transfer (DBT) scheme[48]. Through DBT, all subsidies are credited directly to the beneficiaries' bank accounts. This makes the delivery of welfare schemes much more efficient and prevents any corruption in the process. Use of Aadhaar card by the government for welfare purposes, however, has raised questions regarding exclusion. The failure to authenticate an individual due to reasons such as biometric mismatch, poor internet connectivity, or other technical problems may result in denying access to eligible persons of certain benefits.[49]

Direct Benefit Transfer (DBT) and Efficiency

The Direct Benefit Transfer is another example of the successful use of Aadhaar technology for improving governance. In this case, the subsidies provided by the government to people will be deposited directly into the beneficiary's bank account without involving any intermediary.

[47] World Bank, Digital Identity Toolkit (2018)
[48] Government of India, Direct Benefit Transfer Mission.
[49] Usha Ramanathan, "Aadhaar and the Surveillance State", 32 National Law School of India Review 45 (2014).

Volume-2, Issue-3 *Pages: 500-541*

Aadhaar technology facilitates the operation of the DBT system in terms of providing proper identification of the beneficiary in order to transfer money. With the use of an Aadhaar number, the government will easily identify who should be a recipient of benefits. Thus, there will be no leakages or corruption, which will result in huge financial savings for the government.

So far, DBT has been introduced in various programs related to LPG subsidies, scholarships, and even social security pensions. The benefits of DBT in this context are obvious: money transfers become more effective and faster due to the lack of bureaucracy and intermediaries involved in the process. However, the DBT system faces certain problems. These may include delays in transfers, incorrect linking of an Aadhaar number with the bank account of the beneficiary, and lack of banking infrastructure in the rural part of India. The use of Aadhaar for authentication also involves some risk associated with exclusion from the program.

Aadhaar and Financial Inclusion

There have been instances whereby the Aadhaar card has helped promote financial inclusion within India. Individuals, especially those from vulnerable communities, have been able to use this universally accepted form of identity to access banks. The association of this card to the banking sector has made it possible for one to open an account at any given bank since it can help in Know Your Customer (KYC) procedures. In other words, this has promoted banking in areas that were not covered by banks. Aadhaar cards have been incorporated into the Jan-Dhan-Aadhaar-Mobile (JAM) Trinity framework whereby people use their bank accounts linked to the Aadhaar card to get governmental benefits, pay their bills, and transact within the bank. Individuals have also found it easy to conduct their banking operations due to the introduction of the Aadhaar Enabled Payment System (AePS), which allows one to conduct transactions through biometric recognition. The adoption of Aadhaar cards in promoting financial inclusion also poses several challenges. The mandatory nature of linking these cards to one's bank accounts violates individual privacy and

Volume-2, Issue-3 *Pages: 500-541*

freedom[50]. Besides, technical errors may hinder the process of accessing financial services.

Aadhaar in Digital Governance

The Aadhaar card has emerged as an important part of India's digital governance regime. This facility allows government departments to link different systems and databases, thus ensuring the creation of one seamless system that facilitates the process of service delivery and administration. By adopting the Aadhaar card, government departments are able to authenticate the identities of people instantly without the requirement of any physical documents or authentication processes. This has simplified administrative processes and increased the effectiveness of services offered by the government. The Aadhaar card is also used for many e-governance measures including digital locker, online verification system, and e-KYC procedure. Such uses have enhanced the convenience of accessing government services by making them accessible online from remote locations. However, the linking of various government databases with the Aadhaar number poses serious risks with regard to data concentration and surveillance.

Challenges and Criticisms

However, there have been many criticisms of the system. First, one of the major problems associated with Aadhaar is that of exclusion. Those who fail to authenticate themselves using their biometric identification features may be excluded from the system[51]. This means they will be deprived of the opportunity to access basic services. Moreover, there is an issue related to the security of information. As the Aadhaar database is centralized, it. it becomes easier to attack it through cybercrime. Although several security measures have been adopted, data leaks continue to occur, casting doubt on the effectiveness of these measures. Consent is another problem faced by the Aadhaar system. People may not be aware of what their personal information will be

[50] Gautam Bhatia, The Transformative Constitution (HarperCollins, 2019)
[51] Jean Drèze et al., "Aadhaar and Food Security", Economic & Political Weekly (2017)

Volume-2, Issue-3 *Pages: 500-541*

used for. Moreover, since Aadhaar is necessary to access important services, people cannot say no. Finally, the use of the Aadhaar system beyond its original intention can pose a threat to privacy.

Balancing Efficiency and Rights

The usage of Aadhaar as an instrument of governance reveals the conflict between efficiency and the right of individuals. While on the one side there have been several improvements in service delivery, on the other side, many significant issues come up in terms of privacy, autonomy, and possible overreach by the government. There should be an effective balance struck in order to take advantage of the benefits that Aadhaar may offer without infringing upon individual rights.

CONSTITUTIONAL AND LEGAL ANALYSIS OF AADHAAR:

Evolution of the Right to Privacy in India

There is no explicit provision in the Indian Constitution with regards to the right to privacy. Nevertheless, through judicial interpretation by the Supreme Court, the right to privacy has emerged as a fundamental right as an inherent aspect of the right to life and personal liberty as guaranteed by

Article 21 of the Constitution. In earlier cases like **M.P. Sharma v. Satish Chandra (1954)**[52] **and Kharak Singh v. State of Uttar Pradesh (1962)**[53], privacy had not been declared to be a fundamental right. With the passage of time, a new meaning has been attributed to Article 21 and the facets of personal liberty have been recognized by the Supreme Court of India. Finally, with respect to the judgment in the case of Justice **K.S. Puttaswamy v. Union of India**, it was observed by a nine-judge bench that the right to privacy is a fundamental right and is covered under Part III of the Constitution.

Aadhaar and the Right to Privacy

[52] AIR 1954 SC 300
[53] AIR 1963 SC 1295

Volume-2, Issue-3 *Pages: 500-541*

The Aadhaar scheme includes the collection of both biometric and demographic information and, therefore, poses serious threats with regard to informational privacy issues. The centralization of the data collected can lead to abuse by various parties, ranging from unauthorized access and surveillance to other potential uses.

The right to privacy is affected in many ways within the framework of the Aadhaar project:

- Data collection involving biometric information
- Data storage and processing using central databases
- Authentication procedures creating additional metadata

In its judgement in the case relating to the Aadhaar case, the Supreme Court recognized that Aadhaar affected the right to privacy but did not automatically breach it if sufficient measures were taken.

The Aadhaar Judgment (2018)

The constitutionality of the Aadhaar scheme was directly attacked in **K.S. Puttaswamy v. Union of India (Aadhaar Case)**. The Supreme Court, through a five-judge bench, gave a lengthy judgment analysing the legality and proportionality of the Aadhaar scheme. The Supreme Court upheld the validity of the Aadhaar scheme on a majority opinion and recognized the significance of the scheme in facilitating targeted distribution of welfare benefits. However, certain important restrictions were put into place to protect individual rights.

The main decisions of the Supreme Court are as follows:

- Aadhaar scheme is constitutionally valid for the implementation of welfare schemes that are funded from the Consolidated Fund of India
- Forced linking of Aadhaar number with PAN is allowed
- Compulsory linkage of Aadhaar number for accessing facilities such as mobile phone services and bank accounts is not allowed
- Private entities shall not use Aadhaar numbers for authentication purposes

Volume-2, Issue-3 *Pages: 500-541*

- Some sections of the Aadhaar Act have been declared invalid or unconstitutional

The decision shows an effort to reconcile between the needs of the state and individual rights.

Doctrine of Proportionality[54]

One of the crucial parts of the analysis made by the Court in the Aadhaar case is the use of the doctrine of proportionality to determine the justifiability of the restriction of a fundamental right. The following four factors make up the proportionality test:

1. **Legitimate Aim** - The measure in question must be aimed at a legitimate purpose of the State
2. **Rational Connection** - There must be a rational connection between the two
3. **Necessity** - The measure must be necessary and there must be no alternative less restrictive measures
4. **Balancing** - There should be more benefit from the measure than harm done to the right

The Court ruled that Aadhaar passes the test of proportionality especially in regard to the delivery of welfare schemes because the system served as an effective way to ensure that subsidies reached their targets and avoided leakages. Nonetheless, one of the weaknesses of the Court's approach is that it did not apply the proportionality principle rigorously, especially concerning the necessity of the system and the existence of other options.

Informational Privacy and Data Protection

Informational Privacy in Justice **K.S. Puttaswamy v. Union of India** is of critical importance when discussing Aadhaar. Informational privacy pertains to the right of an individual to control the gathering, usage, and
distribution of their personal information.

[54] Modern Dental College v. State of Madhya Pradesh, (2016) 7 SCC 353

Volume-2, Issue-3 *Pages: 500-541*

Some of the issues surrounding the introduction of Aadhaar include:

- The lack of an adequate law on data protection during the implementation of the project
- The dangers posed by the centralization of data
- The potential for misappropriation of authentication data

While the Aadhaar Act does contain provisions that limit the disclosure of biometric information, they have been widely regarded as inadequate. In response to these issues, the Digital Personal Data Protection Act, 2023 was enacted subsequently. The efficacy of this regulation in governing the handling of data related to Aadhaar has been debated.

Aadhaar and Other Fundamental Rights

Apart from privacy, Aadhaar is also relevant to some of the following fundamental rights:

- **Rights to equality (Article 14)**: Discrimination based on authentication failure would result in unequal enjoyment of welfare entitlements
- **Rights to life and personal dignity (Article 21)**: Inaccessibility of basic necessities because of problems with Aadhaar could impact survival
- **Rights to freedom of expression (Article 19(1)(a))**: The potential for surveillance might act as a deterrent to exercising freedom of speech

The relationship between Aadhaar and the above-mentioned rights necessitates a comprehensive constitutional approach.

Criticism of the Aadhaar Judgment

However, there have been some noteworthy critiques of the Aadhaar ruling, including:

- Dependence on the advantages of Aadhaar, while failing to address its disadvantages
- Failure to consider data privacy and surveillance issues sufficiently

Volume-2, Issue-3 *Pages: 500-541*

- Acknowledgment of the Money Bill procedure used to pass the Aadhaar Act
- Failure to take into account mass surveillance capabilities

Moreover, there were dissenting opinions in the ruling which highlighted serious objections to the use of Aadhaar as a surveillance tool.

AADHAAR AND THE ARCHITECTURE OF THE SURVEILLANCE STATE:

Understanding the Surveillance State

Surveillance state is described as a situation where the government closely watches the actions, behaviors, and data collected about people. Historically, surveillance was a limited process requiring considerable resources. However, developments in digital technology have made surveillance easy and ubiquitous. In contemporary societies, surveillance is usually integrated within the governance framework for purposes of security, administration, or provision of welfare. The development of digital identities like Aadhaar helps in this regard because it makes possible monitoring and analysis of the data collected. The notion of the surveillance state is connected with the capability of the state to watch over the actions of individuals and analyze their activities in order to influence their behavior.

Aadhaar as Surveillance Infrastructure

In essence, Aadhaar has the capability of building a technological framework which could be used to engage in activities of surveillance[55]. Some characteristics of this technological framework include the following:

- The centralized database which allows storage of biometrics and demographic data of users
- The creation of authentication logs every time an individual uses his or her unique identifier

[55] UIDAI, Aadhaar Act, 2016

Volume-2, Issue-3 *Pages: 500-541*

- The linking of different sectoral databases to each other including those of welfare programs, telecoms, banking and others

The capability of collecting information from various sectors means that one can build a comprehensive profile of an individual based on this information. This capability is very useful for effective governance but is also
capable of being abused.

Metadata and Profiling

One of the most important issues related to Aadhaar is that of the creation and usage of metadata. Metadata means data about transactions or communication, such as the time, place, and kind of authentication performed. Even without accessing the actual content of transactions, metadata can expose the pattern of behavior. For instance, authenticating oneself repeatedly from particular places will give away an individual's travel patterns, habits, and socioeconomic activities.

With time, the cumulative data collected in metadata can be used to profile people based on their behavior, leading to potential issues such as:

- Anonymity lost
- Surveillance targeted
- Discrimination likely

This capacity to profile people on a large scale signifies a paradigm shift in the interaction between the government and its citizens.

Function Creep and Expansion of Aadhaar

The term "function creep" describes the process through which a system begins to operate outside of its initial scope. While Aadhaar was created to help distribute welfare benefits, its functions have grown to span different industries.

Instances of function creep are seen in:

- The association of Aadhaar with banking systems and PAN numbers
- Aadhaar's application within telecommunication and digital services
- Incorporation into e-governance systems

Volume-2, Issue-3 *Pages: 500-541*

Such developments lead to an increase in the number of data points attached to one identity, thus increasing the possibilities for surveillance. Moreover, it poses the issue of unclear restrictions regarding the use of Aadhaar.

The Panopticon and Digital Surveillance

One such theoretical framework which can prove to be useful for the study of Aadhar is that of Panopticism formulated by Michel Foucault. In the panopticism model of control, the individual is aware of the fact that he might be under observation at all times even though he is not really under any active scrutiny. This is bound to influence the behavior of individuals to such an extent that they become self-regulating. The fear of being watched, especially in the case of Aadhar, can influence people's behavior to such an extent that it leads to a chilling effect on individual freedom.

Surveillance Capitalism and Data Economy

Another crucial perspective is that of surveillance capitalism, which was proposed by Shoshana Zuboff. This theory concentrates on the importance of data as an economic asset and on the way that both government and corporations use data in order to predict people's behavior and influence it. Even though the Aadhaar system itself is created by the government, its interaction with the private sector makes it problematic from the perspective of using personal information in order to achieve certain financial benefits. Such interaction increases the level of problems connected with surveillance.

Legal Safeguards Against Surveillance

The Aadhaar system comes with some legal measures designed to protect against any misuse of personal data. For example, the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act,
2016[56] prohibits the sharing of core biometric data and establishes penalties for breaches.

[56] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

Volume-2, Issue-3 *Pages: 500-541*

Furthermore, judgments by the judiciary, especially in **K.S. Puttaswamy v. Union of India (Aadhaar case)**, have placed some limitations on the Aadhaar system, including making its use optional for private organizations.

Nevertheless, these legal protections are deemed insufficient because there are still some issues to consider:

- Insufficient mechanisms for independent monitoring
- Excessive authority granted to the state in accessing data
- Inadequate transparency in data processing

The effectiveness of legal safeguards depends on their implementation and enforcement, which continues to be a subject of debate.

Risks of a Surveillance State

Incorporation of the Aadhaar system into various aspects of governance poses a number of threats connected with the rise of the surveillance state:

- **Mass surveillance**: Monitoring of masses of people using electronic devices
- **Privacy issues**: Data gathering eliminates individuals' freedoms
- **Chilling effect**: Fear of being watched causes individuals to limit their actions
- **Power concentration**: Accumulation of data increases government power

This threat is another reason why the Aadhaar system needs regulation.

Critical Evaluation

Aadhaar, although capable of enabling surveillance, must be separated from its actual use. While the availability of surveillance technology cannot necessarily be equated to the use of surveillance technology, the lack of proper security measures will increase the possibility of abuse. The convergence of information technology and centralization of data makes it possible to convert the system into one that enables surveillance if there is no appropriate regulation. Thus, the problem is not whether the Aadhaar system is currently being used as an instrument of surveillance, but whether it has been designed to be used for such purposes.

Volume-2, Issue-3 *Pages: 500-541*

DATA PROTECTION AND PRIVACY FRAMEWORK IN INDIA:

Evolution of Data Protection Laws in India

The approach adopted by India towards data protection has been a gradual one. Before the declaration of privacy as a fundamental right, the data protection regime in India was mostly characterized by sector-specific legislation and statutory provisions[57]. The Information Technology Act, 2000 along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[58] constituted the basis for protecting sensitive personal information. Nevertheless, these statutory provisions were not extensive and applied mainly to corporations but not the state. The landmark case of Justice K.S. Puttaswamy v. Union of India is an important watershed in the journey of developing data protection laws in India. In this judgment, it was stated that there should be a proper legal framework to protect the personal data of citizens and also regulate its use by the state and non-state agencies.

The Aadhaar Act and Data Protection

There are provisions related to data protection and privacy under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. Provisions made by the Aadhaar Act are aimed at regulating the gathering, storage, and use of the personal information.

Some of the key features of the Aadhaar Act include:

- No sharing of sensitive biometric identifiers including fingerprints and iris scans
- Prohibiting the use of any information collected from the citizens for anything but what has been stated by the law

[57] Ministry of Electronics & IT, Govt. of India

[58] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Volume-2, Issue-3 *Pages: 500-541*

- The requirement of seeking prior consent before carrying out any authentication procedure
- Imposing penalties for any kind of unauthorized access or disclosure
- However, the Act has been faced with criticism on various grounds due to some issues:
- In the absence of an independent body to monitor the actions
- Aadhaar has been providing a lot of power to the state
- Limited redressal measures have been provided for the citizens

Judicial Interpretation and Privacy Safeguards

The Supreme Court, in K.S. Puttaswamy v. Union of India (Aadhaar Case), analysed the data protection aspects of the Aadhaar regime. While upholding the constitutional validity of Aadhaar, the Court placed some limitations to ensure the protection of privacy rights.

In particular, the Court:

- Concluded that private parties were not permitted to utilize Aadhaar authentication services
- Curbed the extent of data storage
- Underlined the importance of comprehensive data protection measures

This decision reiterates the requirement that any violation of privacy should be proportional to its ends and must have suitable security measures in place.

Even so, issues persist about the execution of these policies and the possibility of data misuse.

Digital Personal Data Protection Act, 2023

The passing of the Digital Personal Data Protection Act, 2023 marks an important milestone[59] in formulating a data protection regime in India. This Act aims to regulate personal data processing and provide individuals with more power over their data.

[59] Digital Personal Data Protection Act, 2023.

Volume-2, Issue-3 *Pages: 500-541*

Some important aspects of the Act are:

- The concept of "data principal" as a right holder
- The responsibility of "data fiduciary" to process data legally and securely
- The necessity of obtaining consent before data processing
- The formation of the Data Protection Board for enforcement
- The imposition of penalties for data leaks

It is worth noting that this Act applies not only to governmental but also private organizations.

Limitations of the Data Protection Framework

Although the Act has immense significance, it has come under criticism for certain deficiencies. Some of the major drawbacks include the following:

- Loose exemption provision provided to the government based on factors such as national security and public order
- Lack of adequate independence of the Data Protection Board
- Lack of clarity regarding data localization and cross-border data flows
- Inadequate provisions for surveillance

This makes one wonder about the adequacy of the act as far as regulating systems such as the Aadhaar system is concerned.

Data Security and Risks

The issue of the safety of information is an important part of protecting data. The centralized system used by Aadhaar can be viewed from two perspectives - it has certain benefits, as well as drawbacks.

For example, while on the one hand, centralization helps manage data and verify identities easily, on the other, this very quality makes it susceptible to breaches, which could result in significant consequences, like the loss of identity and financial

Volume-2, Issue-3 *Pages: 500-541*

problems. Cases of data leakage[60] have demonstrated that there are certain gaps in the system and there might be some problems with current security procedures.

Balancing Innovation and Privacy

The difficulty in regulating Aadhaar is how to balance its advantages with its potential dangers. While there are numerous benefits that can be derived from the use of technology, such as efficiency in government services and inclusion of citizens in the financial system, there are also considerable threats associated with its implementation.

A good regulation must ensure:

- Comprehensive laws
- Accountability processes
- Trials on how data are processed
- Power to the people through their rights

This will ensure that technology does not undermine basic liberties.

COMPARATIVE ANALYSIS OF DIGITAL IDENTITY SYSTEMS:

Estonia: A Model of Secure Digital Identity

Another example of an innovative digital ID program is the Estonian digital identity system, which has earned recognition worldwide due to its unique characteristics.

Firstly, it has been developed using the principles of decentralization and security. Privacy, transparency, and citizen control are among the core principles underlying this project.

Accordingly, Estonians receive a digital ID giving access to various services, such as financial transactions, voting, healthcare, and taxes. Contrary to Aadhaar, the Estonian system does not depend much on biometrics and uses crypto methods and smart cards to identify users.

[60] Privacy International, Aadhaar Data Concerns Report (2019).

Volume-2, Issue-3 *Pages: 500-541*

Secondly, Estonia has the infrastructure called X-Road, which enables communication between databases without centralized storing of the information. This approach helps avoid any breaches and makes mass surveillance impossible. Finally, the Estonian data protection legislation is consistent with **the General Data Protection Regulation (GDPR)**[61], and people can easily gain access to the data collected about them and monitor who has used this information. Thus, the Estonian approach to digital IDs proves that this issue could be managed successfully while maintaining strong privacy.

Surveillance-Oriented Digital Identity System

Another model can be found in China, where digital identity systems are deeply intertwined with the country's surveillance apparatus. The digital identity scheme in China utilizes national identity databases and advanced technologies like facial recognition, artificial intelligence, and big data analytics. One of the key distinguishing aspects of this scheme is its use of the social credit scoring system to reward or punish individuals according to their conduct. Scores received by individuals through this system determine whether an individual will benefit from certain services, job positions, and monetary rewards. For that reason, digital identity is not simply used as a means of identification. It serves as an instrument of behavioral regulation and monitoring facilitated by the connection of identity systems and surveillance technologies.

Overall, this example highlights the dangers that could emerge with digital identity if it was integrated into a comprehensive surveillance system. This is a scenario different from Aadhaar, as it does not employ the mentioned characteristics yet, which does not mean that it cannot occur in the future.

United Kingdom: Rights-Based Approach

[61] Regulation (EU) 2016/679 (General Data Protection Regulation)

Volume-2, Issue-3 *Pages: 500-541*

Approach to digital identity in the United Kingdom can be characterized as prudent and focused on citizens' rights. Unlike India and Estonia, United Kingdom has not developed mandatory identification procedures at the national level. On the contrary, it uses decentralized approaches to verification, tailored to specific industries.

In particular, initiatives like GOV.UK[62] Verify enable the verification of one's identity online using private providers approved by the government. The system focuses on users' consent, data minimization, and privacy protection measures.

In general, the United Kingdom's approach to digital identity can be described as being highly dependent on data protection legislation, namely GDPR and Data Protection Act, 2018[63]. In this regard, it places strict obligations on data controllers. Contrary to India's approach to the problem, the British experience shows a prudent and user-focused approach.

Comparative Analysis with Aadhaar

Comparison of these models with Aadhaar reveals some of their significant distinctions in terms of structure, goals, and protections:

- **Centralized versus Decentralized Model:** Aadhaar employs a centralized database, whereas Estonia employs a decentralized one
- **Biometric Dependence:** Aadhaar uses biometric data extensively, but Estonia and the UK use digital certificates
- **Data Privacy:** European models focus on stringent data privacy legislation, whereas India is yet to develop its approach
- **Surveillance Threats:** The Chinese model is one of a high surveillance state, whereas that of Aadhaar is moderate

Aadhaar is unique in its size and effectiveness, but it carries a risk because of its centralization and increasing coverage.

Lessons for India

[62] Government of UK, GOV.UK Verify System
[63] Data Protection Act, 2018 (UK)

Volume-2, Issue-3 *Pages: 500-541*

The comparison provides various lessons that could be used to improve Aadhaar[64]:

- Consider decentralization wherever feasible to reduce dependence on a centralized database
- Mandate the enactment of legislation for data protection to conform to international practices
- Empower the citizenry to monitor their personal data
- Prevent function creep, and restrict the uses of Aadhaar to its intended purpose
- Constitute regulatory bodies for overseeing data usage

Such recommendations will go a long way towards safeguarding against the dangers of Aadhaar and keeping it within constitutional bounds.

ETHICAL AND SOCIAL IMPLICATIONS OF AADHAAR:

Privacy and Ethical Concerns

One of the most critical ethical problems surrounding Aadhaar involves the violation of people's privacy. The gathering and storing of biometric and demographic data involve the creation of an ecosystem in which people are always identified and verified.

In **K.S. Puttaswamy v. Union of India**, the landmark case in which privacy was recognized as a basic right by the Supreme Court of India, it became clear that the notion of informational self-determination must be included in the concept of privacy. Informational self-determination is a person's right to regulate the processing of his or her personal data.

This becomes problematic when it comes to Aadhaar, however, because of the volume of data gathered and the danger of data leakage. No matter how many precautions

[64] OECD, Digital Government Studies (2020)

Volume-2, Issue-3 *Pages: 500-541*

are taken, there will always be some risk of a data breach. Ethical governance entails giving people authority over their personal information.

Exclusion and Marginalization

Although Aadhaar contributes to inclusion, there are cases of exclusion as well, especially for marginalized people. Problems during authentication such as mismatch of biometrics, connectivity problem, or technical problem may lead to denial of access to important services, such as ration, pension, and health services.

The problem of such a situation has significant ethical implications since people's right to their basic needs cannot depend on technology that sometimes fails. Vulnerable communities such as the elderly, workers doing manual labor, and rural populations are more likely to experience the problem. As stated by experts like Usha Ramanathan, Aadhar does not contribute to the removal of disparities but may worsen them. From the ethical perspective, justice should be ensured by the application of any service system.

Digital Divide and Inequality

The efficiency of Aadhaar is directly proportional to access to the digital infrastructure. Unfortunately, there is still a very strong digital divide in India[65] where inequalities exist when it comes to the access to the Internet, technology, and digital infrastructure.

Residents living in rural and isolated regions can experience problems while accessing Aadhaar-enabled services because of poor connectivity or inadequate knowledge about digitization. It means that the advantages of digital governance are not available to everyone who needs them.

The problem of the digital divide brings up several important ethical considerations. Since access to rights and services can become possible only through digital technologies, people unable to use the Internet are disadvantaged.

[65] World Bank, World Development Report: Digital Dividends (2016)

Volume-2, Issue-3 *Pages: 500-541*

Autonomy and Informational Self-Determination

Another ethical issue related to the use of Aadhaar is that of autonomy. The concept of informational self-determination is based on an individual's freedom to control their personal information and exercise discretion regarding its usage. However, in reality, there have been numerous instances when Aadhaar has been mandated for receiving various essential services, which has resulted in individuals feeling forced into giving their personal information. According to Daniel J. Solove's theory, the concept of privacy should not be limited to secrecy but control over one's personal information. Ethically, it becomes difficult to legitimize the collection of such information.

Human Dignity and Constitutional Values

Human dignity is one of the essential values that form the basis of fundamental rights. There have been controversies over the potential for technology-based programs to undermine human dignity, especially where people do not get access to welfare benefits on account of failure in authentication processes.

In **Maneka Gandhi v. Union of India**[66], the apex court noted that the right to life in Article 21 guarantees the right to live with dignity. Any system that denies people basic amenities on account of technical glitches may be in violation of the same. The ethical dilemma here is ensuring that technology does not undermine human dignity.

Function Creep and Expansion of Use

The concept of function creep describes the process whereby an application grows in scope from what it was originally designed to be used for. Aadhaar started off as a method for delivering social welfare services, but is currently being used for a wide range of sectors like banking, telecommunications, and taxation. There are significant dangers associated with the expansion of the system and how easily data can be abused, leading to a loss of privacy. With each new service tied into Aadhaar, the

[66] (1978) 1 SCC 248

Volume-2, Issue-3 *Pages: 500-541*

network grows and becomes a potential surveillance tool. Privacy International has pointed out some of the dangers of function creep when it comes to digital identity applications, especially since there are no limits to its capabilities.

Ethical Governance and Accountability

Ethical issues surrounding Aadhaar call for strong governance structures. The principles of transparency, accountability, and supervision should be embraced to ensure that the operation of digital ID systems is in accordance with the Constitution and ethics.

Strong regulation needs independent supervisory institutions, proper legal provisions, and avenues for redress. It is imperative that individuals can contest any decision, access data, and get remediation in the event of violations.

The passage of the Digital Personal Data Protection Act, 2023 is a positive move towards enhancing data privacy in India. Nevertheless, its success will rely on implementation and enforcement.

FINDINGS AND ANALYSIS:

Aadhaar as a Tool for Governance Efficiency

One of the key findings of this study is the significant improvement in the efficiency of governance due to Aadhaar. The introduction of a unique and verified identification system for citizens has allowed the state to enhance the efficiency of welfare schemes and minimize duplicate registrations and fraudulent activities.

Aadhaar has been instrumental in facilitating direct benefit transfers (DBT) where the transfer of subsidies to citizens takes place without any middlemen. This has helped prevent corruption in the public distribution system and improve the mechanisms of governance. Nonetheless, although these findings are highly significant, they need to be assessed considering their wider impact on individual liberties.

Centralization of Data and Structural Risks

Volume-2, Issue-3 *Pages: 500-541*

One of the major issues found from the study is related to the centralization of the data infrastructure of Aadhaar. The use of central databases that store the biometric information as well as personal information increases the vulnerability of data theft, unauthorized access to data, and misuse of information. Centralization gives more power to the state, thus posing questions regarding accountability and control. As opposed to decentralized databases, where there are several points or nodes where data is stored, Aadhaar becomes more vulnerable to cyber-attacks.

Aadhaar and the Right to Privacy

There were several implications of the Supreme Court's decision in K.S. Puttaswamy v. Union of India concerning the fundamental right to privacy for the use of Aadhar. This decision determined that in case of violation of the right to privacy, the requirements of legality, necessity, and proportionality should be satisfied. There are a number of issues related to the Aadhaar system that are raised by this judgment. Despite being based on law, there are doubts about the necessity and proportionality of collection and processing of such an amount of personal information. There is always a risk of using this data incorrectly, and people cannot fully control their own personal data.

The subsequent Supreme Court's decision regarding Aadhaar proved the validity of the program, but under certain conditions.

Surveillance Potential and Data Profiling

Another important insight from the study is that Aadhaar can facilitate surveillance as a consequence of the data generation and collection process. Each authentication results in a record, and with repeated use, the records combine to form patterns regarding behavior and activity. While Aadhaar does not itself serve as a surveillance mechanism, the link between various services through Aadhaar forms the foundation of a surveillance mechanism. The idea is consistent with the theory of surveillance and how it operates, particularly with regard to data usage. Risks of abuse go beyond the

Volume-2, Issue-3 *Pages: 500-541*

misuse of Aadhaar data by the state for surveillance purposes, and can include misuse by corporations as well.

Exclusion and Implementation Challenges

It was also noted that the use of Aadhaar has contributed to cases of exclusion, especially when it comes to providing welfare services. Technical problems, including mismatch of biometric data and lack of connectivity, have caused people to be denied access to their basic services.

These problems illustrate the difference between policy intentions and their execution on the ground. Although the purpose of using Aadhaar is to promote inclusion, the fact that it is based on technology means that it can lead to exclusion of those who cannot prove their identity.

Adequacy of Legal and Regulatory Framework

The legal regime for Aadhaar is not static, but has developed over time through the introduction of the Aadhaar Act and the affirmation of the right to privacy by the judiciary. The most recent development in this regard is the Digital Personal Data Protection Act, 2023, which sets out a comprehensive data protection regime in India. Nevertheless, the findings of this research suggest that current legal safeguards might not be adequate to resolve all the problems related to Aadhaar. Problems like data minimization, purpose limitation, and independent supervision need to be reinforced. Legal safeguards can only be effective if they are not only well-designed, but also effectively enforced.

Balancing Efficiency and Fundamental Rights

One of the core themes that emerge from this paper is the issue of balancing governance efficacy and the preservation of fundamental rights. The example of the Aadhaar system demonstrates how such a system can provide huge benefits but at the same time pose threats to privacy and autonomy. The idea of proportionality can be considered a useful tool for dealing with such issues. This concept implies that any interference with the exercise of fundamental rights should be justified, proportionate,

Volume-2, Issue-3 *Pages: 500-541*

and adequately secured. In the context of the Aadhaar system, finding this balance still seems challenging. Although some measures have already been taken to regulate it, the work on the matter is far from over.

Overall Assessment

It follows that the use of Aadhaar may be categorized as that of a dual technology that has benefits as well as downsides. In the first place, Aadhaar improves efficiency, facilitates inclusion, and minimizes corruption. In the second place, however, the technology poses risks as regards privacy and exclusion.

It is up to the manner in which Aadhaar is utilized whether the contribution it makes to the construction of a surveillance state will be limited or not.

CONCLUSION AND SUGGESTIONS:

Summary of Key Findings

It can thus be seen from the above analysis that there is a dual purpose behind Aadhaar.

Firstly, Aadhaar has been extremely beneficial in improving governance efficiency. This is because of better management and distribution of welfare schemes, prevention of duplication, and provision of direct benefits. Aadhaar has promoted financial inclusion, in addition to making the functioning of the public administration more transparent.

Secondly, the centralized design of the Aadhaar system leads to inherent risks. These include data leakage, unapproved access, as well as abuse of the information available.

Thirdly, the recognition of the right to privacy as a fundamental right in **K.S. Puttaswamy V. Union of India** imposes constitutional constraints on the application of the Aadhaar scheme. Despite upholding the legal validity of the scheme, the Court stressed the importance of proportionate measures in dealing with privacy issues.

Volume-2, Issue-3 *Pages: 500-541*

Fourthly, although the Aadhaar project was not aimed at surveillance, the collection and aggregation of data provide the foundation for such activities.

Lastly, the study has revealed that there is a danger of exclusion in the operation of the Aadhaar scheme. The inability to access technology could prevent vulnerable groups from accessing certain basic services.

Aadhaar and the Surveillance State Debate

One of the important concerns addressed in this study is whether or not Aadhaar serves as part of the structure of a surveillance state. From the results, it is clear that Aadhaar cannot be considered a surveillance system as of now. However, it certainly contains the structural elements that make it possible for such an evolution to take place.

Surveillance states have always been dependent on the capacity of governments to monitor their citizens. Since Aadhaar leaves behind a data trail whenever its verification process is carried out, patterns of behavior can easily be established, making surveillance possible.

However, this threat is more a possibility than a reality since history is proof of how administrative technologies have ended up being used for other purposes.

Need for a Rights-Based Approach

In this context, this essay highlights the need for a rights-based approach to be incorporated within digital identification systems. It calls for a system whereby people's rights, such as privacy, dignity, and autonomy are respected and protected as technology is made use of for the benefit of the citizens.

The decision in the case of **K.S. Puttaswamy v. Union of India** serves as the basis for determining whether the Aadhaar scheme is legal under the Constitution. The principle of legality, necessity, and proportionality must be used in designing and implementing digital identification systems.

Moreover, a rights-based approach entails transparency, accountability, and informed consent among others.

Volume-2, Issue-3 *Pages: 500-541*

Recommendations for Reform

Based on the above findings, the following recommendations can help to ensure that the Aadhaar is used as a means of empowerment rather than surveillance:

1. **Improve Legal Framework for Protecting the Privacy and Security of Data**
   The implementation of the Digital Personal Data Protection Act, 2023 needs to be improved via regulation.
2. **Decentralize Data Architecture**
   One should make efforts to move away from using centralized database architecture to avoid security problems.
3. **Restrict the Function Creep of Aadhaar**
   The application of Aadhaar must be limited to certain purposes, and any change in its function requires careful legal consideration and approval from Parliament.
4. **Promote Inclusivity and Accessibility**
   Alternative systems must be introduced to guarantee that an individual is able to enjoy essential services despite any technical difficulties.
5. **Introduce Accountability Mechanism**
   There is a need to introduce a mechanism to enable individuals to monitor the use of their data and bring authorities to account if needed.
6. **Establish an Independent Regulatory Body**
   There is a need to establish an independent regulatory body to control the functioning of the system and address concerns related to privacy issues.

Future of Digital Identity in India

The future of digital identity in India will be determined by the extent to which the issues highlighted in this analysis are tackled. The evolution of technology is bound to make digital identity even more pervasive.

India stands at a great chance of developing an effective system that protects individuals' rights while ensuring efficient service delivery. By learning from global

Volume-2, Issue-3 *Pages: 500-541*

experiences and putting in place effective safeguards, Aadhaar will be a role model for other countries without compromising privacy.

REFERENCES:

1. **Books**
    - Gautam Bhatia, **The Transformative Constitution: A Radical Biography in Nine Acts** (HarperCollins India, New Delhi, 2019).
    - Upendra Baxi, **The Future of Human Rights** (Oxford University Press, New Delhi, 3rd edn., 2008).
    - Shoshana Zuboff, **The Age of Surveillance Capitalism** (PublicAffairs, New York, 2019).
    - Daniel J. Solove, **Understanding Privacy** (Harvard University Press, Cambridge, 2008).
2. **Articles and Journals**
    - Usha Ramanathan, "Aadhaar: A Biometric History of India's 12-Digit Revolution," (2014) **Economic and Political Weekly**.
    - "Privacy and Data Protection in India," **Journal of the Indian Law Institute**.
3. **Cases**
    - **Justice K.S. Puttaswamy (Retd.) v. Union of India**, (2017) 10 SCC 1.
    - **Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India**, (2019) 1 SCC 1.
    - **Maneka Gandhi v. Union of India**, (1978) 1 SCC 248.
    - **M.P. Sharma v. Satish Chandra**, AIR 1954 SC 300.
    - **Kharak Singh v. State of Uttar Pradesh**, AIR 1963 SC 1295.
    - **Modern Dental College & Research Centre v. State of Madhya Pradesh**, (2016) 7 SCC 353.
4. **Statutes**
    - The Constitution of India, 1950.

Volume-2, Issue-3 *Pages: 500-541*

- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- The Digital Personal Data Protection Act, 2023.
- The Information Technology Act, 2000.
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

5. Reports and Online Sources

- Unique Identification Authority of India (UIDAI), available at: **https://uidai.gov.in**
- Supreme Court Observer, "Puttaswamy v. Union of India (Aadhaar Case)," available at: **https://www.scobserver.in**
- Government of India, Direct Benefit Transfer Reports, available at: **https://dbtbharat.gov.in**
- World Bank, "Digital Identity Systems," available at: **https://www.worldbank.org**
- Privacy International, Reports on Surveillance and Digital Identity, available at: **https://privacyinternational.org**