# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

**ISSN: 2582-6433**

# DISCLAIMER

ISSN: 2582-6433

# ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

# *PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT*

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

# BIOMETRIC IDENTITY SYSTEM AND CONSTITUTIONAL LIBERTY: THE AADHAAR MODEL AND GLOBAL PRIVACY IMPLICATIONS CONSTITUTIONAL TO MANDATORY BIOMETRIC IDENTIFICATION SYSTEM

AUTHORED BY - S SEBASTIN KISHORE
LAW STUDENT
VISTAS CHENNAI

CO-AUTHOR - MR.MATHANACHANDIRAN B
ASSISTANT PROFESSOR
VISTAS CHENNAI

## ABSTRACT

The rapid rise of digital identity systems has transformed the relationship between the State and its citizens, bringing both opportunities and challenges. In India, the Aadhaar system stands as one of the most ambitious biometric identification programs in the world. It was introduced with the aim of providing a unique identity to every resident and improving the delivery of government services. While Aadhaar has helped in reducing fraud, increasing efficiency, and promoting financial inclusion, it has also raised serious concerns about privacy, surveillance, and constitutional freedoms.

This study focuses on examining the Aadhaar model through a constitutional and legal lens, particularly in relation to the right to privacy and individual liberty. The collection and storage of biometric data—such as fingerprints and iris scans—pose significant risks if not properly regulated. Unlike other forms of identification, biometric data is permanent and deeply personal, making its protection extremely important. The fear of data misuse, unauthorized access, and potential surveillance has led to widespread debate about the limits of State power in a digital society.

The constitutional dimension of Aadhaar became more prominent after the landmark judgment in Justice K.S. Puttaswamy v. Union of India, where the Supreme Court recognized the right

ISSN: 2582-6433

to privacy as a fundamental right. This decision laid down important principles, stating that any interference with privacy must be lawful, necessary, and proportionate. Building on this, the Court in K.S. Puttaswamy v. Union of India (Aadhaar) upheld the validity of Aadhaar but imposed key restrictions to prevent misuse and protect individual rights. These judgments highlight the judiciary's role in maintaining a balance between governance and liberty.

The study also explores the growing concerns around surveillance. When Aadhaar is linked to multiple services such as banking, welfare schemes, and communication systems, it creates the possibility of tracking an individual's activities. This raises important questions about autonomy, consent, and the risk of creating a surveillance- driven society. Additionally, issues such as data breaches, lack of awareness, and technological failures further complicate the effectiveness and safety of the system.

In conclusion, this research emphasizes that Aadhaar is not just a technological tool but a constitutional issue that directly impacts fundamental rights. While it offers clear administrative benefits, its long-term success depends on strong legal safeguards, transparency, and accountability. The study highlights the need for a balanced approach—one that embraces innovation while firmly protecting the privacy and dignity of individuals. Only through such a balanced framework can biometric identity systems function in a way that supports both development and constitutional values.

Biometric Identity System and Constitutional Liberty: The Aadhaar Model and Global Privacy Implications Examining Constitutional Challenges to Mandatory Biometric Identification Systems

The rapid growth of digital technology has transformed the way governments interact with citizens, especially in the area of identity and public service delivery. One of the most significant developments in this context is the introduction of biometric identity systems, which use unique physical traits such as fingerprints, iris scans, and facial recognition to verify an individual's identity. In India, the Aadhaar system has emerged as one of the largest biometric identification programs in the world, aiming to provide a universal identity to residents and streamline access to welfare schemes and services. While the system promises efficiency, transparency, and inclusion, it also raises serious concerns about privacy, data protection, and constitutional liberty.

ISSN: 2582-6433

At its core, Aadhaar was introduced as a tool for good governance. By assigning a unique identification number linked to biometric and demographic data, the government sought to eliminate duplication, reduce fraud, and ensure that benefits reach the intended recipients. For millions of people, especially those from economically weaker sections, Aadhaar has made it easier to access subsidies, open bank accounts, and establish identity in situations where documentation was previously lacking. In this sense, the system has played a role in promoting financial inclusion and administrative efficiency.

However, alongside these benefits, Aadhaar has sparked intense debates about the limits of state power and the protection of individual freedoms. One of the primary concerns is the issue of privacy. Biometric data is extremely sensitive, as it is permanent and cannot be changed like a password. The collection, storage, and use of such data raise questions about how securely it is handled and whether individuals have meaningful control over their own information. The fear of data breaches, surveillance, and misuse of personal information has led to widespread criticism from activists, scholars, and legal experts.

The constitutional dimension of this debate became particularly significant with the recognition of the right to privacy as a fundamental right under Article 21 by the Supreme Court in Justice K.S. Puttaswamy v. Union of India. This landmark judgment established that privacy is intrinsic to the right to life and personal liberty, thereby placing limits on how the State can collect and use personal data. It emphasized that any infringement of privacy must meet the tests of legality, necessity, and proportionality. This ruling laid the foundation for evaluating the Aadhaar system from a constitutional perspective.

Subsequently, the validity of Aadhaar itself was challenged before the Supreme Court in K.S. Puttaswamy v. Union of India (Aadhaar). The Court upheld the constitutionality of Aadhaar but imposed certain restrictions to safeguard individual rights. It allowed Aadhaar to be used for welfare schemes and taxation purposes but struck down its mandatory use in areas such as private services, including mobile connections and bank accounts. This judgment reflects an attempt to strike a balance between the State's interest in efficient governance and the individual's right to privacy and autonomy.

Despite these judicial safeguards, concerns remain about the practical implementation of biometric identity systems. Issues such as authentication failures, exclusion of vulnerable

ISSN: 2582-6433

populations, and lack of awareness continue to affect the effectiveness of Aadhaar. For instance, individuals who face difficulties in biometric verification—due to age, manual labor, or technical errors—may be denied access to essential services. This raises questions about whether a system designed to promote inclusion might, in some cases, lead to unintended exclusion.

From a global perspective, India's Aadhaar model has attracted both interest and caution. Many countries are exploring similar biometric systems to improve governance and security. However, the Indian experience highlights the importance of strong legal safeguards, independent oversight, and robust data protection frameworks. Without these, biometric systems risk becoming tools of surveillance rather than instruments of empowerment.

International discussions on digital identity increasingly stress the need to balance technological advancement with respect for human rights and democratic values.

Another important concern is the potential for mass surveillance. When biometric data is linked with various aspects of an individual's life—such as banking, healthcare, and communication—it creates the possibility of profiling and tracking. This concentration of data in the hands of the State or private entities can undermine personal freedom and autonomy if not properly regulated. The absence of a comprehensive data protection law for a long time in India further intensified these concerns, though recent legislative efforts indicate a move toward addressing this gap.

In conclusion, the Aadhaar system represents both an opportunity and a challenge. It demonstrates how technology can be used to improve governance and expand access to services, but it also underscores the risks associated with large-scale data collection and surveillance. The debate surrounding Aadhaar is ultimately about finding the right balance between innovation and constitutional liberty. Ensuring this balance requires not only strong legal frameworks and judicial oversight but also a commitment to protecting the dignity, privacy, and rights of every individual.

## Evolution and Legal Framework of Aadhaar:

The evolution of Aadhaar reflects India's journey toward building a modern, technology-driven system of governance while trying to ensure that every individual has a recognized identity.

ISSN: 2582-6433

Before Aadhaar, many people—especially those from rural or economically weaker sections—struggled to prove their identity. This made it difficult for them to access basic services like opening a bank account, receiving government subsidies, or even obtaining official documents. The idea behind Aadhaar was simple yet powerful: to provide every resident with a unique identity that could be verified anywhere in the country.

The Aadhaar project was launched in 2009 under the Unique Identification Authority of India (UIDAI). It aimed to assign a 12-digit unique identification number to residents based on their biometric and demographic data. What made Aadhaar different from earlier identity systems was its reliance on biometrics such as fingerprints and iris scans, which are unique to each individual. This reduced the chances of duplication and fraud, making the system more reliable. Over time, Aadhaar grew rapidly and became one of the largest biometric identification systems in the world, covering a vast majority of India's population.

As the system expanded, the government began linking Aadhaar to various welfare schemes and services. The intention was to ensure that benefits reached the right people without leakage or corruption. For example, subsidies for food, gas, and pensions were connected to Aadhaar to prevent duplication and ghost beneficiaries. This helped improve transparency and efficiency in the delivery of public services. However, as Aadhaar became more widely used, concerns also started to emerge regarding privacy, data security, and the possibility of misuse.

To give Aadhaar a proper legal foundation, the government enacted the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. This law provided the framework for the collection, storage, and use of Aadhaar data. It also defined how Aadhaar could be used for authentication and verification purposes. Importantly, the Act aimed to ensure that Aadhaar would be used primarily for welfare schemes and not for unnecessary surveillance. However, critics argued that the law did not have enough safeguards to fully protect individual privacy.

The constitutional validity of Aadhaar was challenged in court, leading to important judicial decisions. In the landmark case of Justice K.S. Puttaswamy v. Union of India, the Supreme Court recognized the right to privacy as a fundamental right under Article 21. This judgment had a major impact on the Aadhaar debate, as it set clear limits on how personal data could be collected and used by the State. It emphasized that any intrusion into privacy must be lawful,

ISSN: 2582-6433

necessary, and proportionate.

Following this, the Supreme Court delivered another significant judgment in K.S. Puttaswamy v. Union of India (Aadhaar). The Court upheld the constitutionality of Aadhaar but introduced important restrictions to protect individual rights. It allowed Aadhaar to be used for government welfare schemes and income tax purposes but struck down its mandatory use for private services such as mobile SIM cards and bank accounts. This decision aimed to strike a balance between the benefits of Aadhaar and the need to protect personal liberty.

Over time, the legal framework of Aadhaar has continued to evolve. Amendments and policy changes have been introduced to address concerns related to data protection and misuse.

There has also been a growing emphasis on strengthening cybersecurity measures and ensuring that individuals have more control over their data. At the same time, discussions around a comprehensive data protection law have gained importance, highlighting the need for stronger safeguards in the digital age.

In conclusion, the evolution and legal framework of Aadhaar show how India has tried to balance technological progress with constitutional values. While Aadhaar has made identity verification easier and improved access to services, it has also raised important questions about privacy and state power. The legal developments surrounding Aadhaar reflect an ongoing effort to ensure that innovation does not come at the cost of individual rights and freedoms.

## Judicial Review and Key Judgments:

Judicial review has played a central role in shaping the legal and constitutional understanding of Aadhaar and biometric identity systems in India. As Aadhaar expanded in scope and became linked to various aspects of everyday life, concerns about privacy, surveillance, and individual freedom led to multiple legal challenges. The judiciary, particularly the Supreme Court, stepped in to examine whether the system aligned with constitutional principles such as the right to equality, dignity, and personal liberty. Through a series of landmark judgments, the courts have attempted to strike a balance between the State's objective of efficient governance and the protection of fundamental rights.

The foundation of this constitutional debate was laid in the landmark case of Justice K.S.

ISSN: 2582-6433

Puttaswamy v. Union of India. In this historic judgment, a nine-judge bench of the Supreme Court unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The Court held that privacy is intrinsic to life and personal liberty and is essential for the exercise of other freedoms. This judgment was not limited to Aadhaar alone but had far-reaching implications for all forms of data collection and surveillance. It established that any restriction on privacy must satisfy the tests of legality, necessity, and proportionality, thereby setting a constitutional standard for evaluating biometric systems.

Building upon this, the Supreme Court directly addressed the validity of Aadhaar in K.S. Puttaswamy v. Union of India (Aadhaar). This case involved a detailed examination of the Aadhaar Act, 2016, and the manner in which biometric data was collected and used. The Court upheld the constitutionality of Aadhaar, recognizing its role in ensuring efficient delivery of welfare benefits and preventing leakages in government schemes. However, it also imposed important limitations to safeguard individual rights. For instance, the Court ruled that Aadhaar could not be made mandatory for private services such as mobile connections or bank accounts, as this would lead to excessive intrusion into personal privacy.

Another important aspect of this judgment was the Court's emphasis on data protection and security. It highlighted the need for strong safeguards to prevent misuse of biometric information and stressed that individuals must not be subjected to unnecessary surveillance. The Court also struck down certain provisions of the Aadhaar Act that allowed private entities to access Aadhaar data, thereby reinforcing the principle that personal information must be handled with strict accountability.

Earlier, in interim orders during the Aadhaar litigation, the Supreme Court had also clarified that Aadhaar should not be made mandatory for accessing essential services. These temporary directions reflected the Court's cautious approach while the matter was under consideration. They recognized the risk of exclusion, especially for vulnerable populations who might face difficulties in biometric authentication.

Judicial review has also brought attention to the issue of exclusion caused by technological failures. Courts have acknowledged that individuals should not be denied basic rights or services due to authentication errors or lack of access to technology. This highlights an important dimension of constitutional law—ensuring that technological systems do not

ISSN: 2582-6433

undermine social justice and equality.

Overall, the role of the judiciary in reviewing Aadhaar demonstrates the importance of constitutional checks and balances in a digital age. The courts have neither completely rejected nor fully endorsed biometric identification systems. Instead, they have adopted a balanced approach, allowing the use of Aadhaar for legitimate state purposes while placing necessary restrictions to protect individual freedoms.

1. Government of India, *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*, which provides the legal framework for Aadhaar and regulates the use of biometric identity for welfare delivery.
2. Justice K.S. Puttaswamy v. Union of India, where the Supreme Court recognized the right to privacy as a fundamental right under Article 21 of the Constitution.
3. K.S. Puttaswamy v. Union of India (Aadhaar), which upheld Aadhaar's validity but restricted its mandatory use to protect individual privacy.
4. Constitution of India, Article 21, which guarantees the right to life and personal liberty, including the right to live with dignity and privacy.

## Aadhaar and Surveillance Concerns:

The legal framework surrounding Aadhaar and privacy in India has developed over time in response to rapid technological growth and increasing concerns about data protection. As biometric systems like Aadhaar became widely used, it became necessary to create laws that not only regulate their functioning but also safeguard individual privacy and constitutional liberties. These laws reflect an ongoing effort to balance the benefits of digital identity with the protection of personal information.

The primary legislation governing Aadhaar is the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. This Act provides the legal basis for the collection and use of biometric and demographic data by the Unique Identification Authority of India (UIDAI). It allows the government to use Aadhaar for ensuring that subsidies and welfare benefits reach the intended beneficiaries. The Act also includes provisions related to data security and confidentiality, stating that biometric information cannot be shared publicly. However, concerns have been raised about the scope of data collection and the potential for misuse, especially in the absence of strong oversight mechanisms in its early stages.

ISSN: 2582-6433

The constitutional protection of privacy received a major boost through the landmark judgment in Justice K.S. Puttaswamy v. Union of India. In this case, the Supreme Court declared that the right to privacy is a fundamental right under Article 21 of the Constitution. This decision had a direct impact on how laws related to Aadhaar and data protection are interpreted. It established that any collection or use of personal data must be lawful, necessary, and proportionate, thereby setting clear limits on State action.

Following this, the Supreme Court further examined the Aadhaar framework in K.S. Puttaswamy v. Union of India (Aadhaar). While upholding the constitutionality of the Aadhaar Act, the Court imposed several restrictions to protect privacy. It ruled that Aadhaar could be made mandatory only for certain government welfare schemes and income tax purposes, but not for private services such as mobile connections or bank accounts. This judgment played a crucial role in limiting the scope of Aadhaar and ensuring that it does not become a tool for excessive surveillance.

In response to growing concerns about data protection, India introduced a comprehensive legal framework through the Digital Personal Data Protection Act, 2023. This law focuses on regulating the collection, storage, and processing of personal data, including biometric information. It emphasizes the importance of obtaining consent from individuals before using their data and provides rights such as access to information, correction of data, and the ability to withdraw consent. The Act also imposes obligations on data handlers to ensure security and accountability, marking a significant step toward strengthening privacy protection in India.

Additionally, the Information Technology Act, 2000, along with its associated rules, has played an important role in addressing issues related to data security and cyber protection. It includes provisions for safeguarding sensitive personal data and penalizing unauthorized access or misuse. Although it was not originally designed for biometric systems like Aadhaar, it has been used to fill gaps in the legal framework before the introduction of more specific data protection laws.

Another important aspect of the legal framework is the role of regulatory authorities. The Unique Identification Authority of India (UIDAI) is responsible for managing the Aadhaar system and ensuring that data is handled securely. At the same time, new data protection authorities established under recent laws are expected to provide oversight and address

ISSN: 2582-6433

grievances related to privacy violations.

Despite these legal developments, challenges remain in ensuring effective implementation. Issues such as data breaches, lack of awareness among citizens, and difficulties in enforcing accountability continue to raise concerns. There is also an ongoing debate about the extent to which the State should be allowed to collect and use personal data in the interest of governance and security.

In conclusion, the laws related to Aadhaar and privacy in India reflect a continuous effort to adapt to the challenges of the digital age. While significant progress has been made in recognizing and protecting privacy as a fundamental right, the effectiveness of these laws depends on their proper enforcement and public awareness. Striking a balance between technological advancement and individual liberty remains essential to ensure that systems like Aadhaar serve as tools of empowerment rather than instruments of control.

Here are **humanized footnotes** for your topic on *Aadhaar, Privacy, and Surveillance*. These are written in a **clear, simple academic tone** and can be directly used in your project:

1. Constitution of India, Article 14, ensuring equality before law and protection against arbitrary State action.
2. Government of India, *Digital Personal Data Protection Act, 2023*, which introduces safeguards for handling personal data and strengthens privacy protection in the digital era.
3. Information Technology Act, 2000 and related rules, which provide legal provisions for data security and protection against unauthorized access to personal information.
4. Unique Identification Authority of India (UIDAI), official guidelines on Aadhaar data protection and authentication processes.
5. Reports by Unique Identification Authority of India explaining the functioning and objectives of Aadhaar in improving service delivery.

## REAL INCIDENT HAPPENED IN TAMIL NADU:

### Tamil Nadu Aadhaar Data Leak (2021)

A major incident highlighting privacy and surveillance concerns occurred in Tamil Nadu in 2021, when a massive data breach exposed the personal information of millions of residents. The breach was linked to the Public Distribution System (PDS), where sensitive details such

ISSN: 2582-6433

as Aadhaar numbers, addresses, mobile numbers, and family information of nearly 50 lakh people were leaked online and reportedly made available on hacker forums. (MEDIANAMA) This incident raised serious concerns about how Aadhaar-linked data is stored and protected by government systems. Although Aadhaar is intended to improve welfare delivery, the leak showed that when such data is connected across multiple platforms, it increases the risk of misuse and unauthorized access. The fact that such a large amount of personal data could be exposed indicates weaknesses in data security and monitoring mechanisms.

From a constitutional perspective, this breach directly affects the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India. When sensitive personal information is leaked, individuals lose control over their identity, making them vulnerable to identity theft, fraud, and digital exploitation. It also raises concerns about surveillance, as such data can potentially be used to track and profile individuals without their consent.

This incident clearly shows that while Aadhaar aims to promote efficiency and inclusion, the lack of strong data protection measures can lead to serious violations of fundamental rights. It highlights the urgent need for better cybersecurity, stricter accountability, and stronger legal safeguards to ensure that citizens' data is not misused.