REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: Revised: Accepted:

Research Paper on Right to Privacy and Biometrics Guidelines

Mr. Yougesh[1*], Dr. P. K. Goyal[2]

[1*]Research scholar, Department of Law, Apex University, Jaipur
[2]Supervisor, Department of law, Apex university

ABSTRACT

The rapid evolution of biometric technologies has sparked significant concerns regarding the safeguarding of individuals' privacy rights. Biometrics, which entail utilizing distinct physical or behavioural traits for identification and authentication, have witnessed widespread adoption across various domains, including law enforcement, border security, and commercial sectors. While biometric systems promise heightened security and convenience, the potential for misuse or unauthorized access presents serious threats to personal privacy.

This abstract explores the intricate relationship that exists between the use of biometric criteria and privacy rights. It looks into the moral and legal standards that govern the gathering, storing, and use of biometric data, highlighting how crucial it is to have robust privacy safeguards in place to prevent any infractions. The abstract looks at how difficult it is to strike a compromise between the fundamental right to privacy guaranteed by both domestic and international human rights treaties and the justifiable aims of safety and efficacy.

Furthermore, the abstract underscores the importance of establishing comprehensive guidelines for biometrics that address key issues like data minimization, purpose limitation, data retention policies, and robust access control measures. These guidelines should cover the entire lifecycle of biometric data, including collection, storage, processing, and eventual disposal. Special emphasis is placed on transparency, accountability, and the involvement of independent oversight bodies to ensure adherence to privacy protection standards. By delving into these crucial aspects, the abstract seeks to contribute to the ongoing discussion on the responsible utilization of biometric technologies while safeguarding the fundamental right to privacy, fostering public trust, and promoting ethical conduct in the digital era.

Keywords:
Biometrics, Privacy Rights, Data Protection, Ethical Guidelines, Security and Privacy Balance.

1. INTRODUCTION

The discourse surrounding 'biometric data' has surged in public discussions lately, yet there seems to be a lack of clarity on its definition. Simply put, biometric data pertains to information about a living organism. Examples include facial images, iris scans, or fingerprints. Due to its potential for identifying individuals, it's crucial to establish mechanisms and safeguards for its handling.

Indian courts have acknowledged the inherent combination of several personal characteristics in biometric data, highlighting the necessity for strong regulation. To protect people's basic rights, several nations have put laws into place restricting the gathering and use of biometric data. For example, the newly implemented European Union General Data Protection Regulation defines biometric info as evidence obtained by specialised technological methods that utilise a person's anatomy, physiological, or behavioural features. Individual identification of people is made possible by such data, underscoring the necessity of safeguarding its usage and preservation.

The Information Technology Act of 2000 (IT Act) and its implementing regulations control the gathering, storing, and handling of biometric information in India. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 (Privacy Rules) define the specific standards for confidential info, delicate private details, and biometric data. A variety of other legislation cover specialised use of biometric data, such as confirming an individual's identification via the Aadhaar card system.[1]

2. DEFINITION OF RIGHT TO PRIVACY

The concept of privacy rights is broad and encompasses the right of individuals to protect their own affairs, choices, and spaces from unjustified intervention. This includes safeguarding private information, individual liberty, informational confidentiality, and bodily autonomy. Many international legal frameworks, such the International Covenant on Civil and Political Rights and the United Nations Declaration on the Rights of the Dead, recognize the right to privacy as a fundamental component of human rights.

[1] Shah, Jayminkumar. “Biometric Technology: Spreading Its Footprint in India.” Forbes, available at: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2020/03/26/biometric-technology-spreadng-its-footprint-in-india/?sh=1e60ca3d765b. (last visited on: May 24, 2024).

3. THE RIGHT TO PRIVACY: A FUNDAMENTAL RIGHT

A cornerstone of personal freedom and autonomy, the basic right to privacy is firmly established in a number of international human rights agreements. In 2017, the Apex bench in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India rendered a historic ruling that explicitly recognized this right as basic in India. In its ruling, the Court affirmed privacy as a constitutionally safeguarded right, expanding the scope of personal data security to encompass physical integrity and autonomy.

4. REGULATION OF BIOMETRIC DATA IN INDIA

Under current Indian legislation, it is mandated that the protocols for managing sensitive personal information also cover the possession, processing, or handling of biometric data. Biometric data is governed by the IT Act since it may be gathered and used using computer resources and so qualifies as personal information. The Privacy Rules define 'personal data' as anything about somebody that, alone or in connection with other freely publicly available data, can be used to identify that individual (Personal Data). Furthermore, a subset of Personal Data known as "sensitive personal data or information" includes very private information about an individual, including passwords, some financial details like bank account or card information, and biometric data (Sensitive Data).[2]

Privacy regulations require adherence to stricter protocols and heightened levels of protection when processing, managing, or handling any data classified as Sensitive Data. Biometric data falls within this category, necessitating specific safeguards to be implemented. Key conditions for the handling of biometric data encompass:

1. Collection: When acquiring biometric data, a body corporate (Entity) must seek written authorization from the data subject concerning the collection and utilisation of such information. There must be a choice in this authorization for the data subject to decline providing the necessary biometric information. Biometric data is sensitive, hence it can only be obtained for authorized purposes that are directly related to and required for the Entity's responsibilities.
2. Retention: The Entity must stop keeping the biometric data after the reason it was gathered has been satisfied.
3. Disclosure: The sharing of biometric information with third parties necessitates the explicit consent of the individual concerned, which can be obtained through a contractual agreement between the Entity and the data subject. Furthermore, disclosure is allowed when mandated by law, when governmental entities need data for identification verification, or when it's necessary to stop, look into, prosecute, and penalize illegal activity.
4. transmission: The express agreement of the person whose data is being transferred is required for the transmission of biometric data to any party, inside or outside of India. On the other hand, if the transfer is necessary to fulfill a legal agreement between the entity and the data subject, it may take place. In these situations, it is crucial that the party receiving the data provide a comparable degree of data security as the party that sent the data.

Entities entrusted with the handling of biometric data are required to establish and uphold appropriate security protocols and guidelines. If a company refuses to implement these safety precautions and creates harm to the data tied or undue profit for the organisation or any individual, the party that is impacted shall be paid by the organisation. The IT Act has a clause that significantly deviates from the standard guidelines regulating damages in India. The data subject does not need to provide evidence of any particular harm brought about by the entity's carelessness in handling biometric data if it can be shown that the business profited unjustly. Despite the absence of judicial precedents illustrating the application of this provision in India, its significance remains undeniable.[3]

5. BIOMETRIC DATA AND PERSONAL DATA PROTECTION BILL

In July 2018, the Indian government received the 'Personal Data Protection Bill, 2018' (the Bill) from a group of experts headed by Justice B. N. Srikrishna. The purpose of this bill is to replace the current data protection framework in India with a new one. The Bill, which is still in draft form, classifies biometric data as "sensitive personal data" and establishes the need for express consent prior to processing such data.

The Bill suggests changing the Privacy Rules that now govern the sharing of biometric data across international borders. It argues that model contract provisions, subject to approval by the Data Protection Authority created by the Bill, should regulate such transfers. at addition, the Bill requires that a copy of the supplied biometric data be kept at a data center in India. The deliberate, knowing, or careless collection, disclosure, transfer, or sale of biometric data, as well as breaches involving its processing, are described with severe consequences.

6. BIOMETRIC DATA AS AN AUTHENTICATION MECHANISM

In the case of Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, the Supreme Court of India made a significant ruling on the topic of biometric data collecting and its use by commercial non-government businesses for authenticating purposes. This decision was a component of a larger evaluation of the Aadhar (Targeted Delivery of

[2] *Available at*: https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar/usage-of aadhaar.html#:~:text=Aadhaar%20system%20provides%20single%20source,as%20the%20case%20may%20be. (last visited on: May 20, 2024)

[3] *Ibid*

Financial and Other Subsidies, Benefits and Services) Act, 2016's legality. When an Aadhar number is issued, people contribute biometric information that is used for Aadhar-based authentication. One specific authentication method, referred to as e-KYC authentication, involves the sharing of authenticated personal details from the Aadhaar database with any authorized agency. This method was permitted for use by both government and private non-government entities.[4]
The widespread adoption of a particular authentication mechanism by private entities has sparked its use across various sectors, including digital platforms and the issuance of e-wallets. This surge in utilization has been fueled by the development of innovative technologies, particularly those involving biometric data collection, which has expanded the scope of applications for this authentication method. The Supreme Court has investigated this tendency, noting that it has resulted in the commercial use of personal information by private corporations. The Supreme Court's decision highlighted the intrinsic relationship between biological data and human qualities, emphasising the significance of such information. Consequently, the Supreme Court has mandated that both government agencies and private entities must justify their use of biometric data by demonstrating a compelling and legitimate interest in its collection, analysis, and storage.
The Aadhaar Act's provisions that allow private companies to collect people's biometric data for commercial authentication have been limited by the Supreme Court's intervention. This action shows that private organizations using biometric data for profit-driven endeavors are not approved.[5]

7. AADHAAR: OBJECTIVES AND IMPLEMENTATION

A. The Aadhaar System

The emergence and progress of inventions need additional legal scrutiny of privacy rights. New technological techniques, such as monitoring, targeting, and data collecting, have the potential to jeopardise personal privacy. Countries are increasingly relying on modern technology in reaction to global terrorist attacks and rising security issues.[6]
Digital footprint analysis and large-scale data collecting have the ability to uncover complex patterns, trends, and correlations, especially when it comes to human behavior and relationships. Although there are many benefits to these technical developments, there are also worries about how governments will handle and handle such sensitive data, particularly as algorithms continue to be improved and processing capacity increases.
"An essential component of the debate over data collecting is the Aadhaar card. Aadhaar is a 12-digit identity number that was introduced in 2009 and is given to Indian residents by the Unique Identification Authority of India (UIDAI). It is free and open to everyone, irrespective of age or socioeconomic standing. Candidates must provide biometric data (fingerprints, iris scans, and face photos) in addition to personal data (name, date of birth, age, gender, address, cellphone number, and email)."[7]

Aadhaar serves as a significant policy mechanism for boosting social and economic diversity, restructuring public sector service delivery, controlling fiscal funds, and fostering easy, people-centric governance. It assists in the economic empowerment of impoverished and weaker parts of society, providing hassle-free utilisation of services and benefits.[8]
Aadhaar aims to establish a cohesive national identity system capable of transcending state, linguistic, and database limitations. Its primary objective is to provide an identity to the most disadvantaged and marginalized individuals in India. This initiative is crucial as millions of impoverished citizens in the country currently lack officially recognized identities. Consequently, they face significant barriers in accessing essential services such as mobile phones, financial assistance, banking facilities, and government welfare programs.[9]

The introduction of Aadhaar ID has revolutionized access to essential services for individuals lacking proper identification. Through bank account transfers facilitated by Aadhaar, people can now directly avail housing subsidies, healthcare, and food assistance. Aadhaar plays a pivotal role across various sectors, including food distribution, employment, education, social security, banking, and healthcare. Service providers can easily use the central Unique Identification database to

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India (Puttaswamy II), (2018) 1 SCC 809.
[5] Soutik Biswas, "Right to Privacy a Fundamental Right, Says Supreme Court in Unanimous Verdict", The Wire, Aug. 24, 2017, available at: https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy/ (last visited on May 24, 2024).
[6] See Justice K.S. Puttaswamy (Retd.) v. Union of India (Puttaswamy I), Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1, 7 (Kaul, J., concurring).
[7] *Ibid*
[8] UIDAI, "About Aadhaar", available at: https://uidai.gov.in/your-aadhaar/about-aadhaar.html (last visited on May 20, 2024).
[9] Caroline E. McKenna, India's Challenge: Preserving Privacy Rights While Implementing an Effective National Identification System, 38 Brooklyn Journal of International Law 729, 731 (2013).

confirm the identity of recipients. At the moment, over 1.09 billion people in India have obtained an Aadhaar identification, which makes it easier for them to get essential services and advantages. [10]

B. Pros of the Aadhaar System

Prime Minister of India, Narendra Modi, has outlined a key policy objective centered on the universal enrollment of Aadhaar for all citizens of India. The goal of this project is to make Aadhaar the most widely used identity identification technique in the country, which would simplify access to financial and governmental services.[11]

The Aadhaar system serves as a beacon of hope for India's most vulnerable communities, granting them unrestricted access to essential government services. These services include vital services including food grains, financial help, job pay, educational perks, healthcare assistance, and the delivery of LPG (cooking fuel). It successfully tackles the persistent problem of corruption caused by intermediaries who use false identities to manipulate welfare databases and siphon off money meant for the poor by creating direct distribution routes.[12]

Individuals facing poverty often struggle to acquire crucial documents such as proof of residence or birth certificates. As a solution, a new initiative has been launched to provide access to telecommunication services and facilitate passport applications for this demographic. The primary goal is to improve their ability to travel and connect with others throughout the country. As a result, those at the bottom of the socioeconomic scale will have more resources to engage in the market and seize possibilities provided by having a valid government identity card.[13]

Additionally, Aadhaar cards are set to play a crucial role in advancing banking services and fostering entrepreneurial endeavors. In especially in rural regions, the Unique Identification Authority of India (UIDAI) is dedicated to improving financial transactions by enabling safe transactions using MicroATMs and mobile devices. By enabling banks to effortlessly link Aadhaar numbers with permanent account numbers (PANs), this program seeks to streamline the process of opening bank accounts by lowering the need for substantial identity documents.[14]

Connecting a bank account to Aadhaar has many benefits. It decreases instances of tax evasion, removes bogus beneficiaries, and facilitates smooth and transparent transfers of subsidies. For companies and entrepreneurs, Aadhaar is a trustworthy verification instrument that makes market transactions easier and more safe. For example, people may use their Aadhaar credentials—such as ID numbers or fingerprints—to make purchases, guaranteeing the effectiveness and dependability of payment procedures.[15]

The Reserve Bank of India has implemented a new initiative aimed at enhancing financial access in rural regions by establishing service centers within local grocery stores and other small businesses. These locations are equipped with cellphones and portable fingerprint readers, enabling retailers to connect their Aadhaar numbers to their bank accounts. Simply insert their bank account information and Aadhaar number into the smartphone and scan their fingerprint for identification when they visit these facilities. As a result, the required sum is sent to the merchant's bank account without any difficulty. This novel payment system encourages the integration of farmers and retailers into the formal banking industry while also streamlining transactions in rural regions. By using this method, people may build their credit history, which opens doors for future loan applications and general financial empowerment.[16]

C. Cons of the Aadhaar System

Serious privacy concerns are raised by the extensive gathering, combining, and usage of an individual's biometric and demographic data, particularly in India where there are noticeably inadequate privacy regulations and no independent monitoring body.[17]

[10] State Govt to Transfer Scholarship Funds to Students' Accounts, The Tribune, Mar. 13, 2015, available at: http://www.tribuneindia.com/news/punjab/state-govt-to-transfer-scholarshipfunds-to-students-accounts/68619.html (last visited on May 20, 2024).

[11] Vikas Dhoot, UIDAI Tightens Norms for Aadhaar-Bank Account Linking, The Hindu, Mar. 9, 2018, *available at:* http://www.thehindu.com/news/national/uidai-tightens-norms-for-aadha-ar-bank-account-linking/article21938183.ece (last visited on May 20, 2024).

[12] Saurabh Kumar, Why Aadhaar is India's Unique Innovation for a Digital Economy, YOUR STORY *Available at:* https://yourstory.com/2017/01/AAD HAAR-DIGITAL-ECONOMY/. (last visited on: May 20, 2024)

[13] Vidhi Doshi, A Security Breach in India Has Left a Billion People at Risk of Identity Theft, WASH. POST *Available at:* https://www.washingtonpost.com /news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billionpeople-at-risk-of-identity-theft/?utm_term=.147fb681aeb1. (last visited on: May 20, 2024)

[14] *Ibid*

[15] *Ibid*

[16] *Ibid*

[17] Caroline E. McKenna, supra note 118, at 732; see Swati Shinde Gole, "Aadhaar Data Theft Hasn't Compromised UIDAI Server: Cops", The Times of India, May 4, 2017, *available at:* https://timesofindia.indiatimes.com/city/bengaluru/aadhaar-data-theft-hasnt-compromised-uidai-server-cops/articleshow/59963733.cms (last visited on May 22, 2024)

There is widespread concern regarding the implementation of a singular universal ID number, as it raises the potential for both governmental and private entities to gain access to sensitive demographic and biometric data. Indeed, instances of breaches in the UIDAI system, resulting in the theft of Aadhaar information, have already occurred. Notably, anonymous vendors have utilized the WhatsApp mobile application to offer unimpeded access to data from over one billion Aadhaar numbers.[18]

For a nominal fee of 500 rupees, or around eight dollars in US dollars, anyone can obtain a wide variety of personal data, such as name, address, date of birth, photo, PIN, phone number, and email address. The Aadhaar system, which was initially created by the government to combat corruption and improve security by offering a distinctive identifying method, is the subject of this data leak.

However, recent occurrences reveal a significant flaw in the system's security. Hackers exploit this vulnerability by accessing Aadhaar numbers, subsequently utilizing them to produce duplicate Aadhaar cards. These counterfeit cards are then used to link SIM cards to bank accounts, frequently without the victims' understanding, allowing for possible identity theft. Despite these disturbing disclosures, the Unique Identification Authority of India (UIDAI) asserts that biometric data is safely encrypted from the start, guaranteeing consumers of its confidentiality. Nevertheless, the prevalence of such breaches raises concerns regarding the efficacy of these security measures, as unauthorized access and leakage of personal data evidently persist.[19]

UIDAI has denied recent media stories that claim information hacking, claiming that these allegations are the result of inaccurate reporting. According to the authorities, biometric data associated with Aadhaar is completely safe. UIDAI claims that having an Aadhaar number by itself does not pose a risk since effective identification needs both the number and matching iris or fingerprints. Without biometrics, access to demographic data alone is considered inadequate for abuse.[20]

Recent revelations have debunked the notion that biometric authentication prevents identity fraud, as instances of such fraud persist. These counterfeit cards are then used to link SIM cards to bank accounts, frequently without the victims' understanding, allowing for possible identity theft. Despite these disturbing disclosures, the Indian Unique Identity Authority (UIDAI) asserts that biometric data is safely encrypted from the start, guaranteeing consumers of its confidentiality. These developments pose challenges to UIDAI's objective of universal Aadhaar coverage for every Indian citizen.[21]

8. PRIVACY CONCERNS AND DATA SECURITY

While the Aadhaar initiative was designed with the noble goal of streamlining governance processes and fostering transparency, it has been met with significant apprehension regarding privacy and data security. Critics have voiced concerns over the potential risks to individual privacy stemming from the collection and centralization of extensive biometric and demographic data, fearing it could pave the way for widescale surveillance. Furthermore, there are worries surrounding the security of the Aadhaar database, with fears of data breaches, identity theft, and unauthorized use of personal information.

Through a number of steps, the Unique Identification Authority of India (UIDAI) is unwavering in its commitment to protecting users and their data. These include restricting the collection of personal information (excluding details like religion, caste, community, class, ethnicity, income, or health) and maintaining a safe and encrypted database. They also include enforcing strict security protocols for data storage and enforcing penalties for any unauthorized access or tampering).

However, even with these guarantees, there is a clear legal vacuum concerning Aadhaar users' safety against any data breaches. India does not have a complete privacy legislation system; instead, industry-specific rules and the growing judicial precedents that interpret the right to privacy are used.[22]

The primary security and cybercrime legislation in India is the Information Technology (Amendment) Act of 2008. This act's essential provision protecting personal information privacy is found in Section 72A. The penalties for privacy infractions involving electronic data are covered in this section. It is imperative to emphasize, nonetheless, that these fines

[18] *Ibid*

[19] Richa Mishra, "The 12-Digit Conundrum", The Hindu Business Line, May 5, 2017, *available at:* http://www.thehindubusinessline.com/specials/india-file/aadhaar-the-12digit-conundrum/article9582271.ece (last visited on May 23, 2024).

[20] Samden Sherpa, Aadhaar Data Fully Safe, Cannot Be Breached or Leaked: UIDAI Responds, GIZBOT *Available at:* https://www.gizbot.com/news/aadhaardata-fully-safe-cannot-be-breached-or-leaked-uidai-responds-046950.html (last visited on: May 23, 2024).

[21] Aadhaar Data Allegedly 'Breached' for Rs 500: All Your Questions Answered, The Indian Express, Jan. 5, 2018, *available at:* http://indianexpress.com/article/technology/tech-news-technology/aadhaar-data-allegedly-breached-for-rs-500-hereseverything-to-know-5011205/ (last visited on May 24, 2024).

[22] *Ibid*

only apply to organizations operating in accordance with the Act and do not extend to individuals who may unlawfully get such information.[23]

Section 43 of the Information Technology Act requires companies to employ "justifiable security measures and protocols" to safeguard data against unauthorised access, destruction, use, change, release, or modification. This section, however, allows enterprises to pick the specific techniques they use to protect confidential information. As a result, there's a chance that businesses may go for lax data protection regulations, which might lead to a lack of external monitoring. This problem highlights the numerous shortcomings of the Aadhaar system, both in terms of its implementation and consequences for the right to privacy.

9. USE OF BIOMETRIC DATA, POST AADHAAR JUDGEMENT

“Following directives from the Supreme Court, the Government has implemented amendments to various legislations, including the 2005 Money Laundering Prevention (Maintenance of Records) Rules. The Aadhaar and Other Laws (Amendment) Act, 2019 was used to effect these changes, which were intended to guarantee adherence to the directives of the Supreme Court.” Clarifying the conditions and scope under which private companies can use biometric data for Aadhaar-based authentication is the main goal of these modifications.

“Furthermore, the Reserve Bank of India (RBI) has added new restrictions concerning the use of Aadhaar authentication procedures to the Master Direction - Know Your Customer Direction, 2016 (KYC Directions).” These KYC Directions outline the client identification protocols that banks, non-banking financial institutions, and payment system operators—all under RBI regulation—need to follow in order to create account-based relationships and track transactions.

As per the updated KYC Guidelines, banks are the only ones with the right to use the biometric data-based Aadhaar authentication system while creating client accounts. However, this practice is contingent upon customers voluntarily opting to use their Aadhaar numbers for authentication. Conversely, non-bank entities are restricted to employing verification methods that do not entail the collection of biometric data.

10. LANDMARK CASE LAWS ON RIGHT TO PRIVACY IN INDIA

1. The Supreme Court of India firmly maintained the right to privacy as a basic entitlement inherent within Article 21 of the Indian Constitution, which protects the Right to Life and Personal Liberty, in the historic ruling of Justice K.S. Puttaswamy (Retd.) versus Union of India (2017). The court emphasized that privacy includes fundamental elements including physical integrity, individual liberty, and data security.[24]
2. The Supreme Court highlighted in the landmark decision of R.M. Malkani v. State of Maharashtra (1973) how crucial privacy is to maintaining individual liberty, which is protected by Article 21 of the Constitution. The court made it clear that listening in on someone else's phone calls without permission violates their basic right to privacy.[25]
3. The People's Union for Civil Liberties (PUCL) v. Union of India case in 1996 established a significant legal precedent when the Supreme Court categorically ruled that the act of tapping phones constitutes a breach of an individual's right to privacy. This is subject to following legally mandated processes and proving need within the bounds of a democratic society.[26]

11. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

There has been much anticipation for the Data Protection Act to be passed in India. The Personal Data Protection Bill, 2018, which is the initial version of the data protection bill, was tabled in Parliament in 2018. The Ministry of Electronics and Information Technology established the Justice Srikrishna Committee, which created this first draft. Still, one particular element in the measure drew the most criticism. This clause required data fiduciaries to keep a minimum of one copy of their clients' data in India, presumably to make it easier for law enforcement to retrieve the information. Concerns were raised about the potential infringement on privacy rights, as this mandatory requirement could grant the state significant access to personal data. Additionally, criticisms were directed at the regulatory framework proposed by the bill, which was seen as lacking sufficient autonomy and potentially subject to excessive central government control.[27]

Two additional bills were presented in Parliament in 2019 and 2021; however, They were eventually removed because inadequate legal frameworks were put in place to protect Indian people' digital data. The Digital Personal Data Protection Act, 2023 (DPDP Act), which outlined a comprehensive policy for safeguarding persons' digital data, was subsequently passed on August 11, 2023.

Key Features of the Digital Personal Data Protection Act, 2023 -

[23] FAQs, Security in UIDAI System, UIDAI, *available at:* https://uidai.gov.in/youraadhaar/help/faqs.html (last visited on May 23, 2024).
[24] 2017 (10) SCALE 1
[25] 1973 AIR 157
[26] AIR 1997 SC 568 / (1997) 1 SSC
[27] *Available at:* https://scholarship.law.bu.edu/faculty_scholarship/1568/ (last visited on: May 22, 2024)

- Information pertaining to named or identifiable persons is defined by law as personal data.
- The laws controls the processing of digital personal data in India, whether it is gathered offline or online and then converted to digital form. Furthermore, it covers data processing operations carried out outside of India if they entail the provision of goods or services within of India.
- Data processing is the automated or semi-automatic management of digital personal data, encompassing tasks like gathering, storing, using, and disseminating the data.
- Consent is a foundational principle within the Data Protection Act. Processing of personal data is only permissible after obtaining the individual's consent. A notification describing the personal data to be gathered and the reasons for processing it must be given prior to requesting consent. Additionally, people are free to revoke their consent at any moment. Consent from a minor's parent or legal guardian is required in certain situations.
- Under certain circumstances, consent may not be required for lawful purposes, including but not limited to:

1. Instances where individuals have willingly provided their data for specific purposes.
2. Access to government benefits and services as mandated by law.
3. Emergency medical situations where obtaining consent is impractical or impossible.
4. Employment-related activities where data processing is necessary for contractual or regulatory obligations.

- With a few exceptions, the law authorizes the transmission of data outside of India. The Central Government will decide which countries are on this restricted list and notify those nations accordingly.[28]

12. IMPLICATIONS AND WAY FORWARD

The intersection of privacy rights and Aadhaar highlights the intricate challenges societies face in balancing individual privacy with governance, security, and technological progress. While Aadhaar holds promise for transforming governance and enhancing service delivery, Ensuring that the acquisition, retention, and application of Aadhaar data respect and protect people's right to privacy is crucial.

The ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India, handed out by the Supreme Court, has set important rules and norms for protecting Aadhaar privacy. It highlights the need for strong data protection protocols, strict steps to prevent data exploitation, and openness in the Aadhaar system's functioning.

CONCLUSION

The debate surrounding the Aadhaar system and the right to privacy encapsulates a nuanced discussion on balancing individual privacy with state interests in the digital era. While Aadhaar holds the potential to modernize governance and enhance service delivery, it is imperative to ensure that the collection, storage, and utilization of Aadhaar data are conducted with utmost regard for individuals' privacy rights.

The Supreme Court's historic ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India established important rules and standards for protecting Aadhaar-related privacy. It emphasized the need for strong data protection protocols, strict steps to prevent data exploitation, and openness in the Aadhaar system's functioning.

It is imperative that the government take into consideration the apprehensions expressed by opponents and interested parties, implement strong data security protocols, and ensure strict compliance with the directives issued by the Supreme Court in order to safeguard the right to privacy and utilize Aadhaar's potential for inclusive and efficient governance. Aadhaar is a big step toward simplified governance and digital inclusivity. Consequently, in order to protect people's right to privacy, the government must allay the concerns expressed by opponents and interested parties and guarantee that the Supreme Court's orders are followed without fail. As a vehicle for inclusive and sustainable development, Aadhaar can only live up to its promise by taking a well-rounded strategy that respects human rights.

[28] *Available at:* https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/magazine/beyond-gdpr-data-protection-around-world (last visited on: May 22, 2024).