VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

BIOMETRICS UNVEILED: CHARTING THE LEGAL CONUNDURUMS OF PRIVACY INVASION

- Renee Kundi[1]

ABSTRACT

This research discusses the multiple aspects of biometric technology and its concerns about privacy. The research starts by examiningbiometric technology's history and current status, including facial and fingerprint recognition. It discusses how biometric technology is widely being adopted and used globally. It then focuses on privacy concerns, especially regarding biometric data collection. The research explores the risks of mishandling and misusing data and emphasizes the need for strong laws to protect people's rights. It also examines how Indian laws govern biometric technologies, analyzing statutes and court rulings, such as the K.S. Puttaswamy v. Union of India case, which affirmed the right to privacy. The research ends by discussing ethical considerations in biometric data collection in India, covering topics like informed consent, data security, transparency, and social impact. Overall, it throws light on the relationship between legal frameworks, ethical issues, and technological advancements in the context of biometric privacy.

Key Words: Biometric Technology, Evolution, Privacy Concerns, Legal Framework in India, Biometric Data, Ethical Considerations.

INTRODUCTION

Biometrics are a part of all the identification and recognition procedures these days. Biometrics refers to using bodily features like fingerprints, face, and voice as special keys to confirm one's identity. They are used in various fields and applications for identity verification and access control. It is a safe and practical approach to gain access to items or to establish one's identity, and it functions similarly to a customized password based on a

[1] Student, Bharati Vidyapeeth (Deemed to be University), New Law College, Pune.

person's physical attributes. However, it is essential to note that while biometrics offer enhanced security and convenience, privacy and data protection concerns must be addressed when implementing these systems. Different levels of harm can result from the misuse or breach of biological or biometric data than from theft or improper use of other personal information.

Once obtained, biological and biometric data pose a real risk to an individual's online persona. If stolen or copied, biometric data can provide access to a person's most sensitive secrets, data, bank accounts, etc.

Laws about biometrics are essential because they help to protect our personal information. The enactment of laws relating to biometrics is also necessary due to the rapid advancement and widespread adoption of biometric technologies. Rigid legal frameworks are essential to balance protecting people's privacy rights and utilizing biometrics for efficiency and security. Additionally, biometric laws ensure that individuals give informed consent before collecting their biometric data.[2] Thus, having a detailed legal framework for biometrics and its privacy becomes important.

BIOMETRIC TECHNOLOGY AND IT'S EVOLUTION

Biometrics can be broken down into Greek words – "bio," which means life, and "metrics," which means to measure.[3] The measuring and examiningof an individual's distinct physical and behavioral traits is known as biometrics. This technology is used for identification and authentication procedures.[4] Global biometrics adoption has grown, with notable technological advances and an increasing understanding of the value of biometric data in improving security. Biometrics works in three significant steps: enrolling the data, storing it, and comparing it with the other data stored. Furthermore, any biometric system consists of three primary parts: A sensor that recognizes the trait that is used to identify secondly, a computer that reads this data and saves it; and lastly, a program that evaluates the attribute and presents it as a line of code or a graph and starts the comparative analysis.[5]

[2]Sterlin Miller, The Basics, usage and privacy concerns of Biometric data, Thomson Reuters, (https://legal.thomsonreuters.com, last visited 25/01/24, 12:56pm)
[3] The history of biometrics, Recfaces, (https://recfaces.com, last visited 25/01/24, 01:10pm)
[4] Mara Calvello, What Is Biometrics? How it Works, Types, & Pros and Cons, Learn hub G2 (https://learn.g2.com last visited 25/01/24, 1.30pm)
[5] ibid

Behavioral and physical biometrics are two distinct categories within biometric identification. Physical biometrics involves measuring and analyzing an individual's physiological characteristics such as fingerprints, iris patterns, facial patterns, or DNA. These traits are unique to each person and remain constant throughout life. On the other hand, behavioral biometrics focuses on studying an individual's behavioral patterns and actions, including keystroke dynamics, gait analysis, voice patterns, or even signature dynamics.[6]

The origins of biometric technology can be found in using handprints and fingerprints for identification in prehistoric societies. The first scientific method of fingerprint recognition appeared in the late 19th century. The 20th century saw the introduction of several biometric modalities, such as finger, iris, and face scanning, which laid the groundwork for the precise biometrics that we use today.[7]Currently, biometric technology has become widespread across various sectors globally. In finance, biometrics like fingerprint and facial recognition are commonly employed for secure access to mobile banking apps and payment authorization. Government initiatives, such as Aadhaar in India, showcase the integration of biometrics for citizen identification. Airports and border control agencies increasingly rely on biometrics, especially facial recognition, to enhance security and streamline passenger processing. Mobile devices commonly feature biometric authentication methods, contributing to user convenience and device security. Healthcare institutions leverage biometrics for patient identification, and the corporate sector uses it for secure access to buildings and sensitive information. However, the increased adoption of biometrics has raised concerns about privacy and data security.

PRIVACY INVASION CONCERNS: BIOMETRIC DATA

Biometric technologies have advantages like making things secure and easy. One can unlock their phone or access their bank account using their fingerprint or face, which is convenient. It's hard for someone else to copy these unique features, so it helps keep one's stuff safe. However, there are downsides, too. Sometimes, these systems might not recognize one correctly, causing frustration. Privacy is a concern because personal information, like fingerprints or face scans, is stored in databases. Personal and sensitive information could be

[6] Supra note 3
[7] The Evolution of Biometric Technology: Past, Present, And Future, TBS-Biometrics, (https://www.tbsbiometrics.com, last visited 25/01/24, 02:24pm)

at risk if these databases get hacked. Also, some worry about being constantly watched or tracked, raising questions about individual freedom. So, while biometrics offer advanced and secure features, we must be careful about how our personal information is used and protected.

Privacy concerns majorly include the hampering or how biometric data can be misused. The misuse of biometric data refers to the inappropriate or unauthorized use of unique physical or behavioral characteristics, such as fingerprints, facial features, or voice patterns, used for identity verification. If someone gains access to biometric databases through hacking or other means, they could exploit this sensitive information for various malicious purposes. For instance, unauthorized individuals might use stolen biometric data to impersonate someone else, gain access to secure areas, commit fraud, or engage in identity theft.[8]

Concerns have been raised over the usage of this data without the consent of the individuals to whom it belongs. Because biometric data is publicly available, there are concerns regarding its collection and usage. For instance, taking pictures of people's faces is simple without their knowledge. People who touch hard surfaces leave prints, which makes fingerprint collection easier. When an intentionally obtained biometric characteristic is utilized for another reason without the subject's knowledge or consent, it is a cause for concern. Certain traits, like fingerprints, are identifiable and relatively permanent, giving biometrics the potential for many applications. Biometric features that were first gathered for a different main reason may contain secondary information, which raises another privacy risk. For instance, iris scans used in identification systems may provide more details about an individual's health, whereas fingerprints may reveal information on a person's employment or socio-economic standing. The most common illustration is DNA, which uniquely identifies a person and provides a wealth of health-related data.[9]

INDIAN LEGAL FRAMEWORK GOVERNING BIOMETRIC TECHNOLOGIES

India has witnessed a rapid evolution in the use of biometric data, mainly through initiatives like Aadhaar, which has become the world's most extensive biometric identification system. With the increasing integration of biometrics into various aspects of daily life, there is a growing need for legal frameworks to safeguard individual privacy, ensure ethical use, and

[8] Kelsey Atherton, The enduring risks posed by biometric identification systems, Brookings, (https://www.brookings.edu/articles, last visited 25/01/24, 03:02pm)
[9] EBELOGU Christopher U, Privacy Concerns in Biometrics, 10 IEEE-SEM 45 (2019)

regulate the collection and storage of sensitive biometric information.[10]The Aadhaar Act primarily shapes the legal landscape for biometric data in India, as it is the Information Technology Act, Digital Personal Data Protection Act, etc.

The Digital Personal Data Protection Bill, 2023, which was introduced in Lok Sabha on August 3, 2023, by the Minister of Electronics & Information Technology,was passed on August 11, 2023,to support India's progress towards the adoption of artificial intelligence (AI) and other future technologies while protecting personal data.

- Article 21 of the Indian Constitution

"No person shall be deprived of his life or personal liberty except according to procedure established by law."[11]

Article 21 asserts that no one may be deprived of their life unless the legal process has been followed. It safeguards people's freedoms. The right to privacy under Article 21 of the Indian Constitution is a fundamental aspect that protects an individual's personal space and autonomy. While the Constitution does not explicitly mention the right to privacy, the Supreme Court of India has interpreted Article 21 to include the right to privacy as an integral part of the right to life and personal liberty. In simple terms, individuals can keep certain aspects of their lives private, free from unwarranted interference by the government or other entities.[12]

In a landmark judgment, the Supreme Court, in the case of *K.S. Puttaswamy v. Union of India*[13] (commonly referred to as the privacy judgment), affirmed the right to privacy as a fundamental right safeguarded under Article 21 of the Constitution. The court asserted that privacy is vital to personal liberty and dignity. This landmark decision underscored the intrinsic value of privacy, recognizing its significance in preserving individual autonomy, dignity, and overall constitutional principles.[14]

[10]Trishna Devi, Biometric Data, Identification and Authentication in India – Legal Framework, Challenges and Impact, 4 ISSN 1001 (2021)
[11]Article 21, Constitution of India, 1950
[12]Article 21 in Constitution of India, Indian Kanoon (https://indiankanoon.org, last visited, 26/01/24, 12:22am)
[13]K.S.Puttaswamy v. Union of India, A.I.R. 2017 S.C. 4161
[14] Supra note 11

In practical terms, the right to privacy means that individuals have the authority to control their personal information, decisions, and choices without undue intrusion. It serves as a crucial safeguard against potential abuses of power and protects individuals from unwarranted surveillance or intrusion into their private lives. The right to privacy is considered a cornerstone in upholding citizens' dignity and individuality within India's constitutional framework.[15]

- Information Technology Act, 2000

Section 43A[16] primarily focuses on the responsibilities of companies or entities handling sensitive personal data. It mandates that if a corporate body (organization) possessing, dealing with,or handling any sensitive personal data or information in a computer resource is negligent in implementing and maintaining reasonable security practices and procedures and, as a result, causes wrongful loss or wrongful gain to any person, such a body corporate shall be liable to pay compensation to the affected party. The section empowers the affected individual to seek compensation for any harm caused by the organization's negligence in safeguarding sensitive personal data. Additionally, the Indian government can prescribe reasonable security practices and procedures for such organizations.[17]

- IT Rules, 2011

As per Rule 2(b)[18] of IT Rules, 2011, biometrics refers to the technologies used for authentication that measure and analyze physical traits of the human body, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements, and DNA.

The term “sensitive personal data” is primarily addressed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued under Section 43A of the Information Technology Act, 2000. These rules

[15]Different aspects of Right to Privacy under Article 21, iPleaders (https://blog.ipleaders.in, last visited, 26/01/24, 11:16pm)
[16] Section 43A, Information Technology Act, 2000, No. 21 of 2000
[17] Trisha Agarwala, Laws in India governing Facial Recognition Technology, Legal Service India (https://www.legalserviceindia.com, last visited 27/0124, 09:50 am)
[18]Rule 2, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

list the requirements for protecting sensitive personal data and information by entities handling such data.

The term "sensitive personal data or information" is defined in Rule 3[19] of these rules. As per Rule 3 of IT Rules, 2011, any information about a person's password, bank account, credit card, debit card, or other payment instrument details, physical, physiological, and mental health conditions, sexual orientation, medical records, and history, biometric information, any details provided to the body corporate for service, and any information received under the clauses as mentioned earlier by the body corporate for processing, storing, or processing under a lawful contract or otherwise is considered sensitive personal data or information.

- Aadhaar Act, 2016

As per Section 2(g)[20]of the Aadhaar Act, 2016, biometric information refers to a person's picture, fingerprint, iris scan, or any other biological characteristic that may be required by law. Section 2(j)[21]of this Act defines core biometric information as the fingerprint, iris scan, or any other biological characteristic of an individual as outlined by regulations. According to Section 2(n)[22]of the Act, identity information concerning an individual encompasses their Aadhaar number, biometric data, and demographic details.

The term "Aadhaar biometrics" refers to an individual's distinct behavioral and physical traits that are recorded and kept in the Aadhaar database under the Unique Identification Authority of India (UIDAI) management. Biometric data is gathered and stored in Aadhaar to build a reliable and secure identifying system. Regarding verification, biometrics is a more dependable tool than traditional identifying techniques like documents and PINs. They offer better protection since they are particular to each person and challenging to counterfeit.[23]

- Digital Personal Data Protection Act, 2023

[19]Rule 3, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
[20]Section 2, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No.18 of 2016
[21]ibid
[22] ibid
[23]Bajaj Finserv, (https://www.bajajfinserv.in, last visited 27/01/24 05:36pm)

As per Section 2(i)[24] of the Digital Personal Data Protection Act, 2023, a Data Fiduciary is an individual or a collective entity that, independently or in collaboration with others, decides the purpose and methods for processing personal data. Section 2(j)[25] of the Act defines a Data Principal as a person to whom the personal data pertains. As per Section 2(n)[26], Digital Personal Data is a digitalized form of personal data. According to Section 2(t)[27] of the DPDP Act, any information that can be used to identify an individual is considered personal data. Section 2(u)[28], a personal data breach happens when someone wrongly handles personal information or accidentally reveals, gets, shares, uses, changes, destroys, or loses access to it. This could jeopardize how private, correct, or accessible the personal data is. Lastly, as per Section 4(1)[29], someone can only use a Data Principal's data as per the rules in this Act and for a legal reason, whether the person agrees to it or for specific valid purposes.

The act permits the processing of personal data for any legitimate reason. The party handling the data may do so with the consent of the person being processed or for legitimate uses, as defined by law. For a particular aim, consent needs to be free, specific, informed, unconditional, and unambiguous with clear affirmative action. The information gathered must be restricted to what is required for the intended use. Customers must get a clear notice outlining all of these elements, along with information about the grievance redress procedure and the rights of the affected parties. If consent is the legal basis for processing data, people have the right to revoke it.[30]

The act also mentions that biometric information can only be shared with third parties inside and outside India through an agreement and a valid contract between the Data Principal and Data Fiduciary. The government could also whitelist and ban such cross-border data exchanges.[31]

[24]Section 2, The Digital Personal Data Protection Act, 2023, No. 22 of 2023
[25]ibid
[26]ibid
[27]ibid
[28]ibid
[29]Section 4, The Digital Personal Data Protection Act, 2023, No. 22 of 2023
[30]Anirudh Burman, Understanding India's New Data Protection Law, Carnegie (https://carnegieindia.org last visited 28/01/24, 01:35pm)
[31]Regulation of Biometric Data under the Digital Personal Data Protection Act, 2023, KSK Advocates & Attorneys (https://ksandk.com, last visited 28/01/24 03:29 pm)

ETHICAL CONSIDERATION OF BIOMETRIC DATA COLLECTION IN INDIA

Informed permission, protection from potential misuse, and respect for individual privacy are the main ethical concerns with biometric data gathering in India. People must be made entirely aware of the reason for and consequences associated with collecting biometric data, and their consent must be acquired in a clear, understandable manner. It is crucial to balance privacy rights and technology improvements to avoid identity theft, illegal access, and other discriminatory effects.[32]

The accuracy and reliability of biometric systems must be maintained to avoid wrongful identification, and measures should be in place to address biases that may disproportionately affect certain groups. Data security is crucial in preventing breaches that may jeopardize citizens' personal information. More ethical considerations include allowing people to control their biometric data, maintaining responsibility and legal compliance, and carrying out social impact analyses to comprehend the broader ramifications on society. Education and public awareness are crucial for empowering people and building confidence in the moral application of biometrics. [33]

It can be seen that biometrics are used in every corner today. For instance, we know that Aadhaar is India's primary proof of identification and is used in almost every sector for verification and recognition. Our biometrics are linked to our Aadhar cards and other identity proofs or personal documents such as PAN cards, driving licenses, etc. Educational institutions, hospitals, banks, and hotels all require Aadhar Cards as proof of identification. However, we never know how the abovementioned places use these documents. Additionally, one can't be sure whether their personal information and data are safe in these hands or not. Such cases can lead to a significant misuse of one's data. For instance, we provide the hotel staff with our Aadhar cards for verification when checking into hotels. Still, if not taken with appropriate caution, these cards or ID proofs can easily be hampered, causing a threat to our personal information, including biometrics. Moreover, because these IDs are also linked to our bank accounts, one can easily access our accounts, which can lead to financial fraud. All personal and professional information can be extracted, and biometrics can be misused for

[32]Jordan Deliversky, Ethical and Legal Considerations in Biometric Data Usage—Bulgarian Perspective, National Library of Medicine (https://www.ncbi.nlm.nih.gov)
[33]Jan Lunter, The Ethical Implications and Legal Responsibilities of Biometric Data Security, Solutions Review (https://solutionsreview.com, last visited 28/01/24 04:48pm)

impersonating someone. Thus, consent for accessing data should be essential. On the contrary, one can be aware or cautious to avoid misusing personal information. For instance, instead of giving the original ID proofs or Aadhaar at certain places, one can provide a Masked Aadhaar card, where the first eight digits are masked or hidden and only the last four digits are shown. This ensures the safety and protection of one's data. DigiLocker is also one of the safe ways to protect digital documents, which are also considered legally valid under the Information Technology Act of 2000. People can also lock their biometrics by visiting the UIDAI website, which adds a layer of protection tosecure their identity.

CONCLUSION

In conclusion, "Biometrics Unveiled: Charting the Legal Aspects of Privacy Invasion" shows how biometric technology and our privacy rights are closely connected. Biometric advancements help with identity verification and security but also raise important ethical and legal questions. Looking at the laws and court decisions, it can be said that finding the right balance between the perks of technology and privacy is essential. From landmark judgments recognizing the right to privacy to creating data protection laws, the legal system is trying to handle the issues raised by collecting biometric data. However, because invading privacy in the digital age is a significant concern, we must keep updating and adjusting our laws to protect people's rights as technology evolves. As biometrics become more important in different areas, it's crucial to have a flexible legal approach that encourages innovation while respecting privacy and personal autonomy.