THE LAWWAY WITH LAWYERS JOURNAL
VOLUME:-29 ISSUE NO:- 29 , NOVEMBER 23, 2025
ISSN (ONLINE):- 2584-1106
Website: www.the lawway with lawyers.com
Email: thelawwaywithelawyers@gmail.com
Digital Number : 2025-23534643

Authored By :- Shivansh singh

THE APPLICATION OF BIOMETRICS INFORMATION IN BANKING LAW

ABSTRACT

The application of biometric information in the banking industry has moved at a lightning pace over the last ten years. Banks globally have adopted biometrics for improved security, customer experience, and cost savings. But this is not without challenges. Biometric systems also pose serious risks when it comes to data privacy, regulatory compliance, ethical issues, and vulnerability to possible legal risks. The paper compares and contrasts the benefits and pitfalls of biometric data use in banking, aligns them with the regulatory structures employed within data protection, and summarises results of some of the largest research studies. The discussion ends by proposing best practices for balancing innovation and risk in biometric banking

INTRODUCTION

It all began in spy films: fingerprint scanning, retina scanning, and face recognition. It was like a dream that could only be realized in the movies. Today, all this is referred to as the simple term biometrics and is used in the security field actively.

This type of access control and authentication is particularly commonly applied in the banking and finance sectors. As of 2023, the market for digital identification solutions, the primary building block of biometric technology, was valued at $34.5 billion[1]. Experts forecast active development in the next few years, and the global market for biometric systems itself can hit $83 billion by 2027[2].

---

[1]Biometrics Market Size, Share, Trends and Forecast by Technology, Functionality, Component, Authentication, and End-User, and Region, 2025-2033< https://www.imarcgroup.com/biometrics-market> accessed on 29-04-25

[2] Ibid

There are growing concerns about how financial institutions in Ghana handle and protect biometric data[3]. Biometric information like fingerprints or facial recognition is extremely sensitive, and banks must take serious steps to guard it against cyber threats. However, Ghana's cybersecurity systems are still developing, raising doubts about whether local banks are fully equipped to fend off advanced cyberattacks. If such sensitive data were to be compromised, it wouldn't just lead to financial losses for individuals it could also damage public confidence in the entire banking system. This concern is especially urgent given the rise in high-profile data breaches around the world, proving that even major institutions with strong security measures can still fall victim to cybercrime.

On top of the security risks, there are also ethical questions around how biometric data might be used. While this technology is meant to improve security, it can also open the door to surveillance. For instance, facial recognition systems can track where people go and how they behave. In Ghana, where people are already becoming more aware and concerned about digital surveillance by both government and private entities, the use of biometric data by banks adds to those fears[4]. There's a real risk that this data could be used for purposes beyond what customers agreed to like monitoring movements or targeting individuals with marketing without their full knowledge or consent.

Ultimately, banks have a serious ethical obligation to protect biometric data and use it responsibly. It's not just about improving security; it's also about respecting people's privacy and ensuring their personal information isn't misused.

UNDERSTANDING BIOMETRIC DATA

According to the Merriam-Webster Dictionary, Biometrics is defined as "the measurement and analysis of unique physical or behavioural characteristics (such as fingerprint or voice patterns), especially as a means of verifying personal identity"[5] In the legal realm, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, [6]defines biometrics under ***Rule 2(b)*** as "Biometrics means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises, 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes." With the fast movements in biometric technologies, strong legal steps taken towards greater care to protect the privacy rights and data of the citizens were found quite inevitable. In the case of Aadhaar, India's biometric verification system, stirred many legal debates that quite intricately reflected the need for strong legal frameworks on the use of this sort of data..

SURGE & OPERATION OF BIOMETRIC DATA

---

[3] Kwakye Agyapong, The Ethical Implications of Using Biometric Data for Bank Authentication: Balancing Security and Privacy in the Ghanaian Banking Sector, International Journal of Research Publication and Reviews, Vol 5, no 12, pp 2859-2865 December 2024

[4] ibid

[5] Merriam-Webster's Collegiate Dictionary (11th edn, Merriam-Webster 2003)

[6] IT Act , 2011

In several industries, including banking, where security and fraud prevention are crucial, biometric authentication has become a game-changing technology. A move toward safer means of confirming people's identities may be seen in Ghana[7], where banks are increasingly using biometric information including fingerprints, facial recognition, and iris scans. Biometric systems offer an apparently infallible method of preventing unwanted access to financial accounts by taking advantage of each person's distinct physical characteristics. This change occurs at a time when fraudsters are posing a growing threat to the financial sector by taking advantage of readily compromised traditional authentication methods like passwords and PINs. However, since biometric information is unique to each person, it provides a better level of security, lowering the hazards

The **surge in biometric data** has been driven by the growing demand for secure, convenient, and efficient identity verification methods across various sectors. Biometric technologies such as fingerprint recognition, facial recognition, iris scanning, and voice authentication have seen widespread adoption in areas ranging from law enforcement and national security to consumer electronics, banking, and healthcare. Governments have implemented large-scale biometric ID systems, such as India's Aadhaar program[8], while private companies use biometrics to enhance user experience and protect sensitive data. The COVID-19 pandemic further accelerated the use of contactless biometric systems, especially facial and voice recognition, as alternatives to touch-based systems.

This rapid growth is underpinned by advances in artificial intelligence and machine learning[9], which have significantly improved the accuracy, speed, and scalability of biometric recognition. Mobile devices now commonly include biometric sensors, enabling users to unlock phones, authorize payments, and access apps securely. In finance, banks use biometric authentication to prevent fraud and streamline services, while healthcare providers employ it to ensure accurate patient identification and data access.

The **operation of biometric data** begins with the collection of unique biological or behavioural traits through specialized devices cameras for facial recognition, sensors for fingerprints, or microphones for voice patterns[10]. These inputs are converted into a digital format known as a biometric template. Once captured, this data is stored either locally on the user's device or in a centralized or cloud-based database, depending on the system's architecture. Storage is typically secured using encryption and other cybersecurity measures to protect against unauthorized access.

When a user attempts to verify their identity, the system performs a matching process. This can be a one-to-one (1:1) verification, where the user claims an identity and the system checks if the biometric data matches the stored template, or a one-to-many (1:N)

---

[7] ibid

[8] Unique Identification Authority of India, Aadhaar: Myths and Facts (Government of India 2022)

[9] Woodward JD Jr, Orlans NM and Higgins PT, *Biometrics: Identity Assurance in the Information Age* (McGraw-Hill 2003)

[10] Anil K Jain, Arun Ross and Karthik Nandakumar, *Introduction to Biometrics* (Springer 2011)

identification, where the system searches a database to find a potential match[11]. These operations rely on algorithms that evaluate the similarity between biometric templates, factoring in variations due to lighting, angle, or device differences.

Despite its advantages, the use of biometric data raises significant privacy and ethical concerns. Biometric identifiers are permanent and cannot be changed if compromised, making breaches particularly dangerous. There are also growing concerns over surveillance, especially when biometric data is collected or used without informed consent. Additionally, algorithmic bias has been observed in some biometric systems, leading to disparities in performance across different racial or demographic groups. As the use of biometric data continues to grow, it is vital to implement strong legal frameworks, transparent policies, and ethical guidelines to ensure responsible and equitable use.

BANKING BIOMETRIC & BENEFITS

The protection of users' financial and personal information as well as the execution of financial transactions are often the main concerns of biometrics in financial digital services. In this instance, the system verifies specific physical characteristics, like fingerprints, to process payments.

Biometrics is widely used. Because each user's information is unique and impossible to copy, it lowers the likelihood of financial data being stolen or misused. Nowadays, biometrics are used by all trustworthy banking service providers.

The palm-reading technology Amazon One, which enables users to safely link their fingerprints to their bank accounts for quicker online transactions, is one of the well-known instances of the application of biometrics[12].

Nearly 60% of US IT and cybersecurity professionals surveyed in 2023 stated they plan to use voice authentication, fingerprint, iris, or facial recognition technology in place of workplace passwords[13].
According to 46% of respondents, multi-factor authentication has been implemented by their organization or plans to be implemented in place of current passwords[14].

Biometric technology has significantly reshaped the banking sector by providing more secure, efficient, and user-friendly ways to manage financial transactions. A key benefit is the **enhanced security** that biometric systems offer compared to traditional methods like

---

[11] National Institute of Standards and Technology (NIST), 'Biometric Standards and Testing' (NIST) https://www.nist.gov/programs-projects/biometrics accessed 29 April 2025.

[12] Ajay Kumar and David Zhang, 'Integrating Palmprint with Face for User Authentication' (2006) 39 Pattern Recognition 2045

[13] NIST, 'Face Recognition Vendor Test (FRVT)' (NIST) https://pages.nist.gov/frvt/ accessed 29 April 2025

[14] ibid

passwords or PINs. Because biometric features such as fingerprints, facial patterns, and voice recognition are unique to each individual, they are difficult to forge or steal, which helps reduce fraud and unauthorized access in banking services.

Another advantage of biometric banking is its ability to **simplify the user experience**. Customers can access their accounts or authorize transactions quickly without the need to remember passwords or carry physical cards. This is especially helpful for users with limited literacy, the elderly, or those with physical challenges, making banking more accessible. In developing regions, biometric verification also plays a crucial role in onboarding new customers who may not have conventional identification documents, thereby helping to expand financial inclusion.

However, there are important concerns that must be addressed. The **protection of biometric data** is a major issue, as unlike passwords, biometric traits cannot be changed if they are stolen or leaked. A breach of such sensitive data could have lasting consequences, raising concerns about how securely banks handle and store biometric information. This is particularly worrying in countries that lack strong privacy regulations or data protection policies.

Another challenge is the **possibility of system bias and exclusion**. Some biometric technologies may be less effective for certain groups due to variations in skin tone, facial features, or even physical conditions like worn fingerprints. These limitations can result in failed authentication attempts and inconvenience for users, potentially locking them out of their own accounts. Technical issues, such as poor sensor performance, can further disrupt access.

There are also **ethical and regulatory questions** surrounding the widespread use of biometric data in banking. Without proper transparency and oversight, there is a risk of misuse or overreach, especially if biometric data is shared across platforms or used for surveillance purposes. To ensure fair and ethical use, strict policies and clear consent procedures are essential.

In summary, while biometric banking offers notable improvements in security and user accessibility, it also presents serious risks regarding privacy, data protection, and system fairness. To fully benefit from this technology, financial institutions must adopt strong safeguards and inclusive practices.

COMPROMISES PRIVACY & HOW TO DEAL WITH IT

Resolving privacy concerns and guaranteeing regulatory compliance are two of the biggest obstacles in the use of biometric banking systems.

This mostly relates to biometrics like fingerprints and facial recognition scans. As a result, you will be subject to stringent regulations as a financial institution concerning the gathering, storing, and application of biometric data.

There are also a number of other significant obstacles in this field. Even with the advancements in biometric technology, hackers exploit flaws to obtain user data without authorization.

The use of deepfake technology presents biometric systems with additional difficulties. Biometric authentication techniques may become confused by deepfakes, making it challenging for systems to tell the difference between a real and a fake person[15].

LEGAL BACKUP OF PRIVACY LAWS AND BIOMETRIC DATA

India has established a legal framework to protect biometric data through a combination of data protection laws and regulatory bodies. At the center of this framework is the Personal Data Protection Bill, which lays out a structured approach to managing personal data, including biometric details. The bill sets clear guidelines for the collection, storage, and usage of such data, promoting lawful, fair, and transparent handling to ensure individuals' privacy is upheld.

The Data Protection Authority (DPA)[16] is entrusted with ensuring regulatory compliance and enforcing provisions related to the protection of biometric data. Judicial precedents have been instrumental in interpreting and refining the legal contours of biometric data governance, thereby enhancing safeguards against misuse. In particular, litigation concerning the Aadhaar system has illuminated the nuanced challenges of regulating biometric identifiers and has substantially contributed to the evolving discourse on privacy rights and data protection frameworks in India.[17]

Ensuring Privacy Rights in Biometric Data Usage

The sensitive nature of biometric data necessitates stringent measures to protect individuals' privacy and security. Key considerations include:

1. **Informed Consent:** Obtaining informed consent whenever biometric data is processed, though achieving genuine consent can be challenging due to the complexity of biometric systems.
2. **Balancing Benefits and Privacy:** Weighing the advantages of biometric authentication against the preservation of individuals' privacy rights, ensuring proportionality and respect for personal integrity.

---

[15] Equa Law, 'Regulatory Challenges of Biometric Payment Systems in Indian Banking: Safeguarding Security and Ensuring Compliance' (Equa Law, 2024) https://blog.equa.law/2024/02/regulatory-challenges-of-biometric.html accessed 30 April 2025.

[16] *Digital Personal Data Protection Act 2023* (India).

[17] *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors* (2017) 10 SCC 1.

3. **Security Measures:** Implementing robust security measures, such as encryption and access controls, to mitigate the risks associated with storing biometric identifiers.

A multifaceted approach is essential to ensure privacy rights, incorporating informed consent, respect for individual rights, and comprehensive security measures.

Security Measures for Handling Biometric Data

Robust security measures are vital for protecting biometric data from unauthorized access and misuse. Key considerations include:

1. **Data Security:** Ensuring secure transmission and storage of biometric data to prevent unauthorized access.
2. **Incident Response:** Establishing protocols to respond promptly to potential breaches or incidents involving personal data.
3. **Facial Recognition Technology:** Employing advanced facial recognition algorithms for authentication and incorporating privacy features, such as liveness detection and anti-spoofing measures.

Organizations handling biometric data must adhere to international cybersecurity standards to ensure responsible data management and protection.

1. The case of **Patel v. Facebook** [18]from 2019 alleged that the social media giant's application of facial recognition technology to tag users in photos violated an Illinois privacy law protecting biometric data. The 9th Circuit Court ruled that the collection of facial geometry constituted sensitive personal information requiring explicit opt-in, even absent direct commercial motives. This established biometric identifiers like facial scans as deserving of heightened legal safeguards.

SURVEYS AND STATISTICS

Biometrics is the basis of passwordless authentication, which is actively spreading worldwide. Experts estimated this market at more than $15 billion in 2022. According to forecasts, it will exceed $53 billion by 2030.

Year	Market Size (in billion U.S. dollars)

[18] Patel vs Facebook,932 F. 3d 1264 (9th Cir. 2019),

Year	Market Size (in billion U.S. dollars)
2021	12.8
2022	15.6
2023	18.5
2024	21.6
2025	25.2
2026	29.3
2027	34.1
2028	39.7
2029	46.2
2030	53.6[19]

WAY FORWARD WITH FUTURE TRENDS

India faces a range of emerging challenges in regulating the use of biometric data, particularly as biometric technologies continue to evolve. Among the most pressing concerns is the rise of **deepfake technology**[20], which threatens the reliability of biometric authentication. Deepfakes sophisticated manipulated images or videos can be exploited to deceive biometric systems, potentially enabling identity fraud. This significantly undermines the accuracy and trustworthiness of biometric verification. To counter such risks, it is imperative for regulators and policymakers to remain vigilant and develop advanced

[19] **Acumen Research and Consulting**, 'Big Data Market Size - Acumen Research and Consulting' (Acumen Research and Consulting, 2022) https://www.acumenresearchandconsulting.com/big-data-market accessed 30 April 2025.

[20] Waingankar, P., 'Deepfake and Digitally Altered Image Abuse and Its Legal Regimes in India' (2024) 6(3) Indian Journal of Law and Legal Research

detection and prevention strategies capable of keeping pace with these technological manipulations.

Ethical considerations also warrant serious attention as biometric technologies become increasingly pervasive. One key concern is **algorithmic bias**[21], which can result in systemic discrimination, particularly in facial recognition and predictive analytics. To ensure fairness and prevent marginalization, it is essential to embed inclusivity and equity into the design and deployment of biometric systems. This includes accounting for cultural differences, varying levels of accessibility, and ensuring that biometric tools are designed to function accurately across diverse populations.

Looking forward, a proactive regulatory and policy-oriented approach is crucial. Three key areas demand particular focus:

1. **Success factors in protecting user data with biometric in UAE**[22]

   Banks do not rely on biometrics alone; they implement **multi-layer security** (biometrics + OTP + device fingerprinting) to prevent unauthorized access .Data transmitted between the customer and the bank is **end-to-end encrypted**. Most banks **do not store the actual biometric data**. Instead, they verify it against government-controlled databases (like the Emirates ID system), reducing the risk of breaches.

2. **Analysis of Supreme court cases**

   HDFC Bank Ltd v Union of India (2022) [23]This case addressed the conflict between the Right to Information (RTI) Act and the right to privacy concerning banking information. The Supreme Court allowed banks to challenge the Reserve Bank of India's (RBI) directives mandating disclosure of confidential information under the RTI Act. The Court emphasized the need to balance transparency with individual privacy rights, especially in light of the precedent set in **K.S. Puttaswamy v. Union of India**[24], which recognized privacy as a fundamental right**.**

3. **Public Awareness**: Educating the public on the benefits, limitations, and risks associated with biometric data usage is critical. An informed populace is better equipped to exercise privacy rights and provide meaningful consent when their biometric information is requested.

4. **Stakeholder Collaboration**: Developing effective legal frameworks that balance innovation with privacy protections requires the active participation of all stakeholders including government entities, private sector actors, civil society, and

---

[21] Jayalakshmi, V., 'Deepfake Technology and Human Rights: Unmasking the Ethical Challenges and Impacts' (2024) 4(3) International Journal of Advanced Legal Research.

[22] 'Mashreq Bank Rolls Out AI-Based Biometric Verification' (The National, 14 July 2023) https://www.thenationalnews.com accessed 30 April 2025

[23] 6 SCC 497 (SC)

[24] (2017) 10 SCC 1

privacy advocates. Such multi-stakeholder collaboration is essential for addressing the multifaceted challenges posed by biometric technologies.

By anticipating future challenges and embedding ethical principles into the development and implementation of biometric systems, India can promote responsible innovation while safeguarding individual privacy and reinforcing public trust in biometric infrastructure.

CONCLUSION

The legal complexities surrounding the use of biometric data in India underscore the urgent need for a carefully structured legal framework to protect individuals' right to privacy. As biometric technologies rapidly evolve and become embedded across diverse sectors, the central challenge lies in crafting legal responses that are both forward-looking and capable of addressing emerging risks. India’s ability to navigate this intricate legal terrain will determine whether it can fully leverage the benefits of biometric innovation while upholding high standards of privacy and data protection. Striking this balance is crucial not only for fostering technological advancement but also for building public confidence in the digital ecosystem.

Achieving such equilibrium requires the implementation of comprehensive regulatory mechanisms grounded in principles of data protection, informed consent, and transparency. These mechanisms must provide precise guidance on the lawful collection, secure storage, and appropriate sharing of biometric data. Moreover, establishing a dedicated regulatory authority with the mandate to oversee compliance and respond effectively to violations is essential. Through these measures, India can lay the groundwork for the ethical and responsible use of biometric data safeguarding individual rights while supporting innovation and ensuring sustainable digital progress.