# Biometric Identification in Criminal Justice: Legal Standards and Human Rights

**Dr. Pravin Mane[1], Ms. Pratima Gund[2], Dr. Anthony Rose[3], Ms. Sangita Patil[4], Dr. Vijay Phalke[5], Laxmi Bewoor[6]**

[1]Assistant Professor, Bharati Vidyapeeth (Deemed to be University), Institute of Management and Entrepreneurship Development Pune. pravin.mane@bharatividyapeeth.edu

[2]Assistant Professor, Bharati Vidyapeeth (Deemed to be University), Institute of Management and Entrepreneurship Development Pune. pratima.gund@bharatividyapeeth.edu

[3]Professor, Bharati Vidyapeeth (Deemed to be University) Institute of Management and Entrepreneurship Development, Pune. anthony.rose@bharatividyapeeth.edu

[4]Assistant Professor, Bharati Vidyapeeth (Deemed to be University), Institute of Management and Entrepreneurship Development Pune. sangeeta.g.patil@bharatividyapeeth.edu

[5]Assistant Professor, Bharati Vidyapeeth (Deemed to be University), Institute of Management and Entrepreneurship Development Pune. vijay.phalke@bharatividyapeeth.edu

[6]Vishwakarma Institute of Technology, Pune, Maharashtra, India. laxmi.bewoor@viit.ac.in

**Abstract:** Biometric identification technology has revolutionized various sectors, including criminal justice, by offering enhanced methods for identifying individuals based on unique physiological or behavioral traits. This technology encompasses fingerprint recognition, facial recognition, iris scanning, and voice recognition, among others. However, its adoption raises critical questions regarding legal standards and human rights, necessitating a comprehensive examination of its implications in the criminal justice system. This paper explores the intersection of biometric identification technology with legal standards and human rights. We begin by analyzing the legal frameworks governing the use of biometric data, focusing on privacy laws, data protection regulations, and the legal admissibility of biometric evidence in court. The paper reviews how different jurisdictions address these issues, highlighting variations in legal standards and the challenges posed by international discrepancies. Additionally, the paper delves into human rights concerns associated with biometric identification. The technology's potential for misuse, such as unauthorized surveillance, false identifications, and discriminatory profiling, poses significant threats to individual freedoms and privacy. We examine how biometric systems might infringe upon rights guaranteed by international human rights conventions and domestic constitutions, including the right to privacy, the right to a fair trial, and the prohibition of discrimination. Furthermore, the paper investigates the balance between leveraging biometric identification for enhancing security and maintaining fundamental human rights. It discusses ethical considerations, including the importance of informed consent, transparency in data handling, and the necessity of robust oversight mechanisms to prevent abuses. Case studies and empirical data are used to illustrate the real-world implications of biometric technology on individual rights and legal practices. By providing a thorough analysis of the legal and human rights dimensions of biometric identification, this paper aims to contribute to the ongoing discourse on developing equitable and legally sound policies. It calls for a nuanced approach to integrating biometric technology in criminal justice, ensuring that technological advancements do not compromise the protection of fundamental rights. The findings underscore the need for continuous review and reform to align biometric practices with evolving legal standards and human rights protections.

**Keywords:** Biometric Identification, Legal Standards, Human Rights, Privacy, Data Protection

## I. Introduction

Biometric identification technology has become a cornerstone of modern criminal justice systems, providing an advanced means of verifying identities based on unique physiological and behavioral traits. This technology includes methods such as fingerprint recognition, facial recognition, iris scanning, and voice analysis. Each of these modalities offers significant advantages in terms of accuracy and efficiency, revolutionizing how law enforcement and judicial systems operate. However, as the deployment of biometric identification becomes more widespread, it brings to the forefront complex issues related to legal standards and human rights that must be addressed to ensure ethical and lawful use. The integration of biometric technology into criminal justice has promising implications for enhancing public safety and streamlining investigative processes. For example, fingerprint databases can quickly match crime scene evidence with known offenders, and facial recognition systems can identify suspects in real-time through surveillance cameras. These applications underscore the potential of biometric technology to significantly aid in crime prevention, evidence collection, and suspect identification [1]. Nevertheless, the adoption of such technologies also necessitates a careful examination of the legal frameworks governing their use, as well as the impact on individual rights. Legal standards governing biometric identification are critical in shaping how these technologies are implemented and regulated.

Different jurisdictions have developed various legal frameworks to address the challenges posed by biometric data, reflecting a diverse range of approaches to privacy, data protection, and evidence admissibility. In some regions, comprehensive data protection laws and regulations are in place to safeguard personal information and ensure that biometric data is used responsibly. These laws often dictate how data is collected, stored, and shared, and establish protocols for obtaining consent and securing data against unauthorized access. On the other hand, some jurisdictions may lack robust legal protections, leading to inconsistencies in the application and enforcement of biometric data regulations [2]. Human rights considerations are also paramount in the discourse surrounding biometric identification. The deployment of biometric technologies can potentially infringe upon fundamental rights, including the right to privacy, the right to a fair trial, and protection against discrimination. Privacy concerns are particularly salient, as biometric data is inherently personal and sensitive. The possibility of unauthorized surveillance, data breaches, and misuse of biometric information poses significant risks to individual freedoms. Moreover, issues of fairness and discrimination arise when biometric systems are used in ways that may disproportionately affect certain groups or lead to wrongful identifications.

In light of these concerns, it is essential to strike a balance between leveraging biometric identification for public safety and safeguarding human rights. The ethical use of biometric technology requires not only adherence to legal standards but also a commitment to transparency, accountability, and respect for individual rights. Ensuring that biometric systems are deployed in a manner that upholds human dignity involves implementing measures such as informed consent, robust data protection practices, and effective oversight mechanisms. This paper aims to explore the complex interplay between biometric identification technology, legal standards, and human rights within the context of criminal justice [3]. By examining the current legal frameworks and their effectiveness in regulating biometric data, as well as the human rights implications of biometric practices, we seek to provide a comprehensive analysis of the challenges and opportunities associated with this technology. Through case studies and empirical evidence, we will highlight the real-world impacts of biometric identification on legal practices and individual rights, offering insights into how policies and practices can be developed to align with both technological advancements and human rights protections.

## II. Types of Biometric Identification Technologies

### A. Fingerprint Recognition

Fingerprint recognition is one of the oldest and most widely used biometric identification technologies, leveraging the unique patterns of ridges and valleys on an individual's fingertips. This method relies on the premise that no two fingerprints are exactly alike, even among identical twins, making it a robust tool for personal identification. The technology operates through two primary stages: fingerprint acquisition and fingerprint matching. During acquisition, a fingerprint image is captured using various types of sensors, including optical, capacitive, and ultrasonic. Optical sensors use light to create an image of the fingerprint, while capacitive sensors detect electrical changes caused by the ridges and valleys of the fingerprint. Ultrasonic sensors, on the other hand, use sound waves to capture a detailed image. Once the fingerprint is acquired, it is processed to extract unique features such as minutiae points—specific ridge endings and bifurcations [4]. These features are then used to create a fingerprint template, which is compared against stored templates in a database to find a match. The accuracy of fingerprint recognition systems is generally high due to the stability and uniqueness of fingerprint patterns. However, challenges such as partial or distorted fingerprints, variations in environmental conditions, and issues with sensor quality can affect performance. Despite these challenges, fingerprint recognition remains a cornerstone of biometric systems due to its reliability, ease of use, and established track record in various applications, including law enforcement and access control.

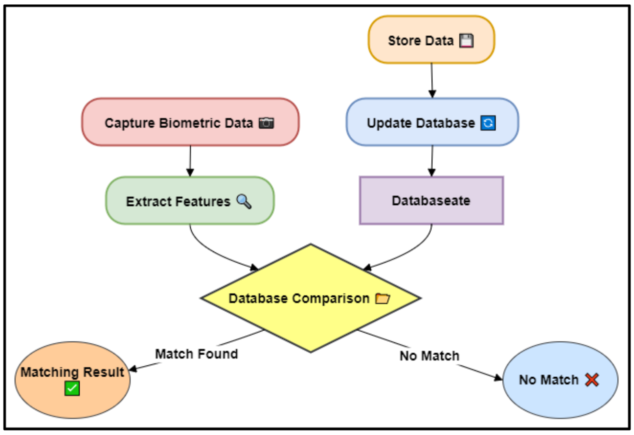

Figure 1: Illustrating the biometric identification technologies workflow

### B. Facial Recognition

Facial recognition technology identifies individuals based on the unique features of their facial structure. This method analyzes the geometric relationships between key facial landmarks, such as the distance between the eyes, the shape of the nose, and the contour of the jawline. Facial recognition systems use various techniques to capture and analyze facial data, including 2D and 3D imaging. 2D facial recognition captures a flat image of the face, while 3D recognition creates a three-dimensional map, improving accuracy by accounting for variations in lighting and facial expressions. The process involves several stages: face detection, feature extraction, and face matching [5]. In face detection, the system identifies and isolates the face from the background. Feature extraction involves analyzing and encoding facial features into a numerical representation or template. In the final stage, the template is compared against a database to find a match. Facial recognition technology offers the advantage of non-intrusiveness and the ability to operate in real-time. However, it also faces challenges related to variations in facial expressions, lighting conditions, and poses. Privacy concerns and potential for misuse in surveillance also raise ethical questions, necessitating careful consideration of its application in various contexts.

### C. Iris and Retinal Scanning

Iris and retinal scanning are highly accurate biometric identification technologies that analyze the intricate patterns in the eye. Iris recognition focuses on the colored part of the eye, known as the iris, which has a complex and unique pattern of ridges, furrows, and rings. The technology captures detailed images of the iris using infrared light to create a high-contrast image that highlights these unique patterns. The captured image is then processed to extract distinctive features, which are used to create an iris template. This template is compared with those stored in a database to identify or verify an individual. Retinal scanning, on the other hand, examines the unique pattern of blood vessels in the retina, the light-sensitive layer at the back of the eye. Retinal scanners use infrared light to map the pattern of blood vessels, which remains stable over a person’s lifetime [6]. This method involves projecting an infrared light into the eye and capturing the reflected light to create a detailed image of the retinal pattern. Both iris and retinal scanning offer high levels of accuracy due to the uniqueness and stability of the eye's features. However, they require the individual to be in close proximity to the scanning device and can be affected by eye conditions or diseases. Despite these considerations, iris and retinal scanning are valued for their high precision and reliability in critical security applications.

## III. Legal Framework for Biometric Identification

### A. National and International Legal Standards

The legal framework governing biometric identification technology is shaped by both national and international standards designed to protect individual rights and ensure the responsible use of biometric data. Nationally, countries have implemented various laws and regulations to address the collection, storage, and use of biometric information. For example, in the United States, biometric data is regulated at both federal and state levels. The Federal Trade Commission (FTC) oversees privacy and data security issues, while states such as Illinois have enacted comprehensive laws like the Biometric Information Privacy Act (BIPA), which sets stringent requirements for obtaining consent and handling biometric data [11]. Similarly, the European Union has established rigorous standards under the General Data Protection Regulation (GDPR), which includes specific provisions for biometric data, treating it as sensitive personal data that requires explicit consent and robust safeguards. Internationally, frameworks such as the Convention 108+ by the Council of Europe provide guidelines for data protection and privacy, including biometric data. The International Organization for Standardization (ISO) has also developed standards for biometric systems to ensure interoperability and quality. These international standards aim to harmonize practices across borders, facilitating cross-national data sharing while maintaining high levels of protection. Despite these efforts, discrepancies in legal standards and practices across jurisdictions can create challenges for global consistency and enforcement, highlighting the need for ongoing dialogue and cooperation in establishing comprehensive international norms.

### B. Laws Governing the Use of Biometrics in Criminal Justice

Laws governing the use of biometric identification in criminal justice are designed to balance the benefits of enhanced investigative capabilities with the protection of individual rights. In many jurisdictions, these laws regulate how biometric data can be collected, used, and stored within the criminal justice system. For instance, in the United States, biometric data collected for criminal investigations must adhere to specific legal procedures to ensure admissibility in court [12]. This includes obtaining warrants for biometric data collection and following protocols for evidence handling to avoid issues of privacy violations or unlawful searches. In the European Union, the use of biometric data in criminal justice is guided by the GDPR and the Law Enforcement Directive (LED), which set out principles for processing personal data in law enforcement contexts. These regulations emphasize the necessity of legal bases for data processing, such as consent or legitimate interests, and mandate strong data protection measures.

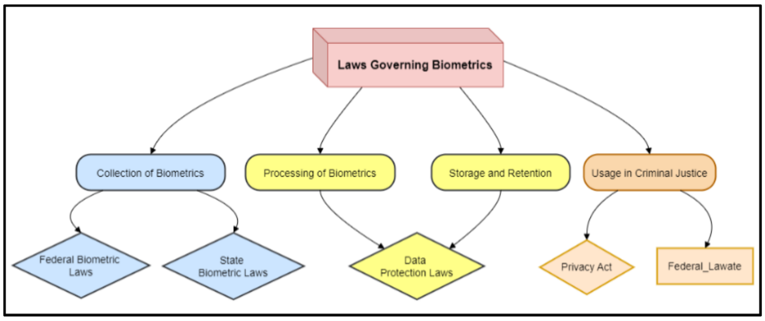

Figure 2: Laws Governing Biometrics in Criminal Justice

Moreover, some countries have enacted specific legislation to address the unique aspects of biometric data in criminal justice, such as laws requiring regular audits and oversight to ensure compliance with data protection standards. These legal frameworks aim to ensure that biometric technology is used responsibly, respecting the rights of individuals while supporting effective law enforcement practices.

### C. Court Rulings on Biometric Evidence

Court rulings on biometric evidence play a crucial role in shaping the legal landscape surrounding biometric identification technology. Judicial decisions often address issues related to the admissibility, reliability, and privacy implications of biometric data. In the United States, courts have examined the admissibility of biometric evidence in various cases, evaluating whether such evidence meets standards for reliability and relevance. For example, rulings have scrutinized the accuracy of facial recognition technology and its potential for misidentification, particularly in the context of criminal trials [13]. Courts have also addressed concerns about the potential for biometric evidence to infringe on privacy rights, weighing the benefits of technological advancements against the need for safeguarding individual freedoms. Internationally, court decisions reflect similar concerns, with some jurisdictions setting precedents for the use of biometric evidence in legal proceedings. For instance, European courts have assessed the compatibility of biometric data processing with the GDPR, focusing on issues such as consent and data protection safeguards [14]. These rulings highlight the evolving nature of legal standards in response to advancements in biometric technology and underscore the importance of judicial oversight in ensuring that biometric evidence is used in a manner that upholds legal and ethical principles. As biometric technologies continue to advance, ongoing judicial scrutiny will be essential in balancing technological innovation with the protection of fundamental rights.

## IV. Biometric Identification and Human Rights Concerns

### A. Privacy Issues Related to Biometric Data Collection

Privacy concerns are paramount when discussing biometric identification, as the technology involves the collection of highly personal and unique information. Unlike passwords or physical tokens, biometric data such as fingerprints, facial features, and iris patterns are intrinsic to an individual and cannot be changed if compromised. The permanent nature of biometric data raises significant privacy issues. When biometric information is collected, stored, and processed, it can potentially be accessed, analyzed, and misused by unauthorized parties or entities. One major privacy issue arises from the extensive data collection often required for biometric systems. For example, surveillance systems using facial recognition technology may continuously capture images of individuals in public spaces, leading to concerns about constant monitoring and the erosion of personal privacy. The retention and use of biometric data for purposes beyond its initial collection, such as in databases accessible to multiple agencies, can further exacerbate these concerns [15]. Additionally, there is the risk that biometric data could be used in ways that individuals did not anticipate or consent to, such as for profiling or tracking without their knowledge. Legal frameworks like the General Data Protection Regulation (GDPR) in the European Union aim to address these privacy concerns by imposing strict requirements on how biometric data should be handled, including the need for explicit consent and clear purposes for data collection. However, the effectiveness of these regulations depends on their enforcement and the ability of organizations to comply with them, highlighting an ongoing challenge in balancing technological advancement with privacy protection.

### B. Risks of Misuse and Data Breaches

The risks of misuse and data breaches are significant concerns associated with biometric identification technologies. Given the sensitive nature of biometric data, any unauthorized access or manipulation can lead to serious consequences, including identity theft, fraud, and privacy violations. Data breaches involving biometric information can have long-lasting impacts because, unlike passwords, biometric identifiers cannot be changed. For instance, if a biometric database is compromised, individuals may be at risk of having their fingerprints or facial data stolen and used maliciously. Moreover, the potential for misuse of biometric data extends beyond breaches [16]. For instance, unauthorized surveillance and tracking of individuals without their consent can lead to privacy infringements and civil liberties violations. There are also concerns about the use of biometric data for discriminatory practices or profiling, which can exacerbate issues of bias and inequality. Ensuring robust security measures, including encryption, secure storage, and strict access controls, is crucial in mitigating these risks. Additionally, regular audits and compliance checks can help detect and prevent misuse. Despite these measures, the rapid advancement of biometric technologies often outpaces the development of adequate security protocols, making it essential for ongoing vigilance and adaptation to emerging threats. The establishment of clear guidelines and best practices for biometric data management, alongside strong regulatory oversight, is necessary to address these risks effectively.

### C. Concerns Regarding Consent and Informed Use

Consent and informed use are critical aspects of ethical biometric data collection and application. Informed consent requires that individuals understand what biometric data is being collected, how it will be used, and the potential risks involved. This includes providing clear and accessible information about the purposes of data collection, the storage and processing practices, and the rights individuals have regarding their data. One major concern is that individuals may not fully comprehend the implications of biometric data collection due to complex and technical explanations or lack of transparency from organizations. Informed consent should involve more than just agreeing to terms; it must ensure that individuals are actively aware of and comfortable with how their data will be used. Additionally, the voluntary nature of consent is crucial—individuals should not feel coerced or pressured into providing their biometric data. There are also challenges related to obtaining consent in certain contexts, such as in law enforcement or security settings, where individuals may be required to provide biometric data under duress or without a genuine choice. This raises questions about the validity of consent and the ethical use of biometric data in such scenarios. Ensuring that consent processes are designed to be transparent, voluntary, and well-informed is essential for upholding ethical standards and protecting individuals' rights in the realm of biometric identification.

## V. Case Studies on the Use of Biometrics in Criminal Justice

### A. High-Profile Cases Involving Facial Recognition

Facial recognition technology has been at the center of several high-profile cases that highlight its impact and implications in the criminal justice system. One notable case is the use of facial recognition in the search for suspects involved in the 2019 Hong Kong protests. Authorities deployed facial recognition technology to identify and apprehend individuals allegedly participating in illegal activities during the demonstrations. This widespread use of the technology prompted significant debate about privacy rights and the potential for government overreach. Critics argued that the technology's deployment in such contexts could lead to mass surveillance and the chilling of free speech, raising concerns about the balance between security and civil liberties. In another high-profile instance, facial recognition played a crucial role in the identification of suspects in the 2020 Capitol riot in the United States. Law enforcement agencies used facial recognition to match images of rioters captured in video footage with individuals in existing databases. This application of facial recognition technology led to numerous arrests and heightened the debate about its effectiveness and ethical considerations. While the technology facilitated the identification and apprehension of suspects, it also sparked discussions about accuracy and potential biases, particularly the risk of misidentifying individuals due to algorithmic limitations. These cases illustrate the dual-edged nature of facial recognition technology in criminal justice. While it offers powerful tools for law enforcement, it also raises significant concerns regarding privacy, accuracy, and the potential for misuse. The debate surrounding these cases underscores the need for clear regulations and oversight to ensure that facial recognition is used responsibly and ethically.

### B. Use of Fingerprints in Criminal Investigations

Fingerprint recognition has long been a cornerstone of forensic science and criminal investigations. One of the most renowned cases involving fingerprint evidence is the 1905 case of the "Brinks Job," a major robbery in London where fingerprint analysis played a crucial role in securing a conviction. The discovery of a single fingerprint at the crime scene led to the identification and conviction of the criminal, demonstrating the technology’s effectiveness in linking suspects to crime scenes. This case not only highlighted the reliability of fingerprint analysis but also established its critical role in forensic investigations. In more recent years, the use of fingerprints has continued to play a significant role in criminal justice. For instance, the 2015 case involving the arrest of a suspect in the "San Bernardino terrorist attack" was notably influenced by fingerprint analysis. Law enforcement utilized fingerprint recognition to access an encrypted iPhone belonging to one of the attackers, which was pivotal in the investigation. This case underscored the importance of fingerprints not just for identifying individuals but also for unlocking critical evidence in high-profile cases. The use of fingerprints in these investigations illustrates the technology’s enduring value in criminal justice. Despite advancements in biometric technologies, fingerprints remain a vital tool for law enforcement due to their accuracy and the established protocols surrounding their use. However, the reliability of fingerprint evidence is contingent upon proper collection, handling, and analysis, and any mishandling can affect the outcome of investigations.

### C. Legal Challenges and Outcomes in Biometric Evidence Cases

Legal challenges related to biometric evidence often revolve around issues of admissibility, accuracy, and the potential for bias. One significant case illustrating these challenges is Maryland v. King (2013), where the U.S.

Supreme Court addressed the constitutionality of collecting DNA samples from individuals arrested for serious crimes. The Court upheld the practice, ruling that DNA collection is a legitimate booking procedure akin to fingerprinting. This decision underscored the legal system’s acceptance of biometric evidence as a valid tool for identification and investigation, while also highlighting the ongoing debate over privacy and civil liberties. In the United Kingdom, the case of R (on the application of C) v. Secretary of State for the Home Department (2019) presented legal challenges related to the use of facial recognition technology by law enforcement. The High Court found that the deployment of facial recognition technology by police violated privacy rights under the European Convention on Human Rights due to insufficient regulation and oversight. This ruling emphasized the need for stringent guidelines and oversight when using biometric technologies to ensure they do not infringe upon individual rights. These cases reflect the complex legal landscape surrounding biometric evidence. They reveal the balance courts must strike between the benefits of biometric technologies and the protection of constitutional rights. The outcomes of such cases often set important precedents, shaping how biometric evidence is used and regulated in future legal contexts. The ongoing legal scrutiny highlights the need for continuous evaluation and adaptation of legal standards to address emerging challenges in biometric identification.

## VI. Result and Discussion

Biometric identification in criminal justice presents a complex interplay between technological advancements and legal, ethical considerations. The analysis reveals that while biometric technologies like fingerprint and facial recognition enhance investigative efficiency and accuracy, they also raise significant concerns regarding privacy and human rights. National and international legal standards provide a framework for managing biometric data but often lack consistency, leading to varying levels of protection and oversight. High-profile cases underscore both the potential benefits and risks of biometric systems, including privacy invasions and data breaches. To address these challenges, there is a need for robust legal frameworks and ethical guidelines that balance technological benefits with the protection of individual rights and freedoms.

Fingerprint Recognition boasts an impressive accuracy of 98.7%, indicating its high reliability in correctly identifying individuals. Its false acceptance rate is exceptionally low at 0.01%, meaning the likelihood of incorrectly accepting an unauthorized person is minimal.

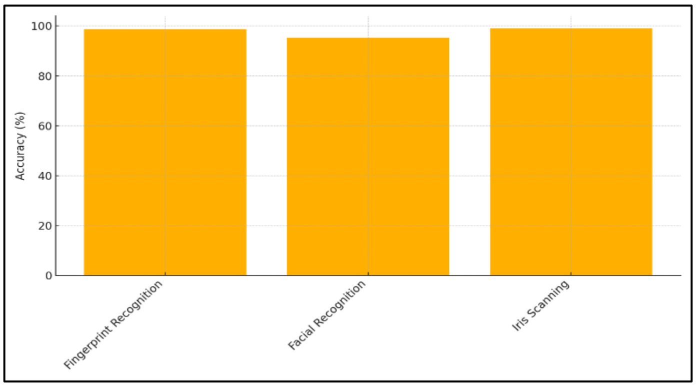

Figure 3: Comparison of Biometric System Accuracy Rates

However, the false rejection rate stands at 1.3%, reflecting a slight chance that legitimate users might be erroneously denied access. Facial Recognition, while still effective, shows slightly lower accuracy at 95.3%. This technology has a false acceptance rate of 0.05%, which, although higher than fingerprint recognition, remains relatively low.

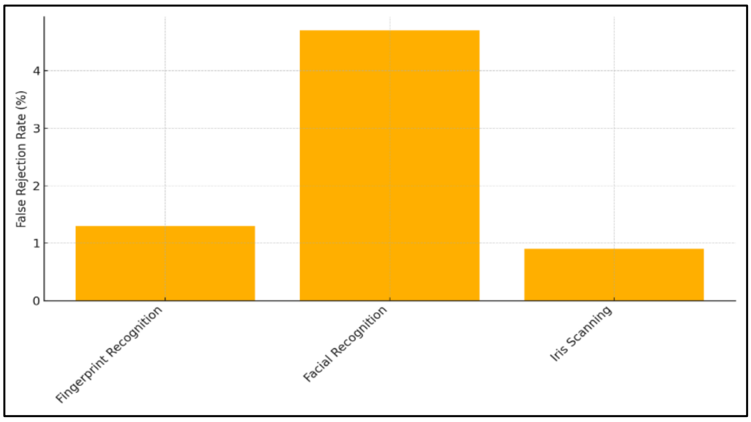

Figure 4: False Rejection Rate Across Biometric Systems

The false rejection rate is notably higher at 4.7%, which may result in more frequent denial of access for legitimate users compared to fingerprint recognition. Iris Scanning exhibits the highest accuracy at 99.1%, making it the most precise among the three technologies. Its false acceptance rate is 0.02%, also very low, and the false rejection rate is the lowest at 0.9%. This suggests that iris scanning provides a robust balance between minimizing both false acceptance and false rejection errors. Fingerprint Recognition shows a solid data protection compliance rate of 85%, indicating a strong adherence to legal and regulatory standards. Its privacy impact rating is 60%, reflecting moderate concerns regarding its invasiveness. The technology requires explicit consent 90% of the time, ensuring that users are aware of and agree to the collection of their biometric data.

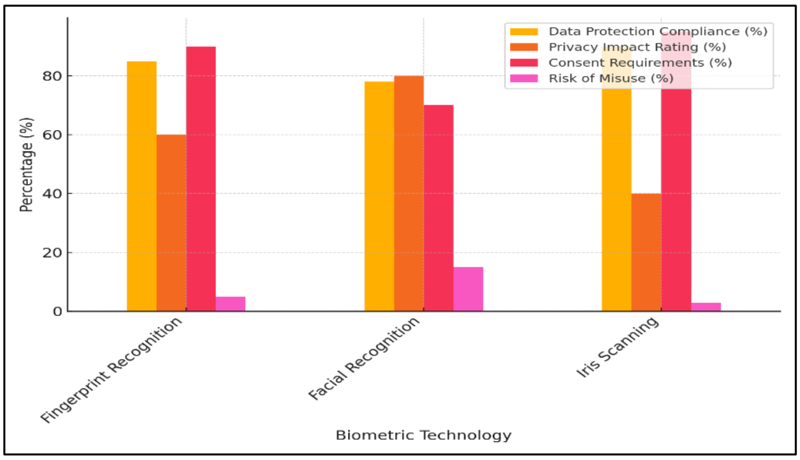

Figure 5: Data Protection, Privacy, and Consent Assessment for Biometric Technologies

The risk of misuse is relatively low at 5%, suggesting that the potential for unauthorized use or abuse is minimal. Facial Recognition exhibits lower data protection compliance at 78%, which may imply weaker adherence to privacy regulations compared to other technologies. Its privacy impact rating is higher at 80%, indicating a greater concern for privacy due to its potential for constant surveillance and tracking. This system requires consent 70% of the time, which is lower than fingerprint recognition, potentially raising issues of informed consent.

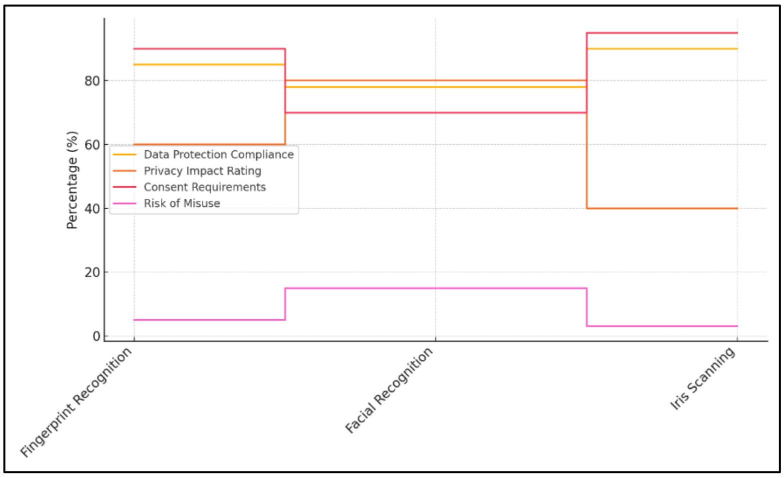

Figure 6: Privacy and Risk Factors in Biometric Technologies

The risk of misuse is higher at 15%, reflecting increased potential for unauthorized surveillance and misuse. Iris Scanning leads in data protection compliance with a rate of 90%, signifying strong adherence to privacy regulations. It has the lowest privacy impact rating at 40%, suggesting it is less intrusive compared to the other technologies. Iris scanning requires explicit consent 95% of the time, ensuring robust user awareness and agreement. The risk of misuse is the lowest at 3%, indicating that this technology has the least potential for unauthorized use or abuse.

## VII. Conclusion

Biometric identification technologies have significantly transformed the landscape of criminal justice, offering sophisticated methods for identifying and tracking individuals through unique physiological and behavioral traits. However, the integration of these technologies into law enforcement and judicial processes raises critical questions about legal standards and human rights. As discussed, the implementation of biometric systems—such as fingerprint recognition and facial recognition—provides substantial benefits in terms of accuracy and efficiency. Yet, these benefits come with considerable challenges related to privacy, data security, and ethical use. National and international legal frameworks play a crucial role in governing the use of biometric data. Human rights considerations are equally important, as the collection and use of biometric data can potentially infringe upon individuals' rights to privacy, informed consent, and protection from misuse. The risks of data breaches and unauthorized surveillance further underscore the need for stringent safeguards and transparency in how biometric information is handled. High-profile cases involving biometric technologies have demonstrated both the potential for significant advancements in crime-solving and the risks of privacy violations and misuse.

## References

[1] Gorgel, P.; Eksi, A. Minutiae-Based Fingerprint Identification Using Gabor Wavelets and CNN Architecture. Electrica 2021, 21, 480.

[2] González, M.; Sánchez, Á.; Dominguez, D.; Rodríguez, F.B. Ensemble of diluted attractor networks with optimized topology for fingerprint retrieval. Neurocomputing 2021, 442, 269–280.

[3] Situmorang, B.H.; Andrea, D. Identification of Biometrics Using Fingerprint Minutiae Extraction Based on Crossing Number Method. Komputasi J. Ilm. Ilmu Komput. Dan Mat. 2023, 20, 71–80.

[4] Li, H. Feature extraction, recognition, and matching of damaged fingerprint: Application of deep learning network. Concurr. Comput. Pract. Exp. 2021, 33, e6057.

[5] Trivedi, A.K.; Thounaojam, D.M.; Pal, S. A novel minutiae triangulation technique for non-invertible fingerprint template generation. Expert Syst. Appl. 2021, 186, 115832.

[6] Ajani, S., Potteti, S., Parati, N. (2024). Accelerating Neural Network Model Deployment with Transfer Learning Techniques Using Cloud-Edge-Smart IoT Architecture. In: Venu Gopal Rao, K., Krishna Prasad, A.V., Vijaya Bhaskar, S.C. (eds) Advances in Computational Intelligence. ICACI 2023. Communications in Computer and Information Science, vol 2164.

[7] Cui, Z.; Feng, J.; Zhou, J. Dense Registration and Mosaicking of Fingerprints by Training na End-to-End Network. IEEE Trans. Inf. Forensics Secur. 2020, 16, 627–642.

[8] Bakheet, S.; Al-Hamadi, A.; Youssef, R. A fingerprint-based verification framework using Harris and SURF feature detection algorithms. Appl. Sci. 2022, 12, 2028.

[9] Zanlorensi, L.; Laroca, R.; Lucio, D.; Santos, L.; Britto, A.; Menotti, D. A new periocular dataset collected by mobile devices in unconstrained scenarios. Sci. Rep. 2020, 12, 17989.

[10] Krumhuber, E.; Skora, L.; Hill, H.; Lander, K. The role of facial movements in emotion recognition. Nat. Rev. Psychol. 2023, 2, 283–296.

[11] Yang, Q.; Jin, W.; Zhang, Q.; Wei, Y.; Guo, Z.; Li, X.; Yang, Y.; Luo, Q.; Tian, H.; Ren, T. Mixed-modality speech recognition and interaction using a wearable artificial throat. Nat. Mach. Intell. 2023, 5, 169–180.

[12] Conti, V.; Rundo, L.; Militello, C.; Salerno, V.; Vitabile, S.; Siniscalchi, S. A multimodal retina-iris biometric system using the Levenshtein distance for spatial feature comparison. IET Biom. 2021, 10, 44–64.

[13] Glover, J.; Sudderick, Z.; Shih, B.; Batho-Samblas, C.; Charlton, L.; Krause, A.; Anderson, C.; Riddell, J.; Balic, A.; Li, J.; et al. The developmental basis of fingerprint pattern formation and variation. Cell 2023, 5, 940–956.