Biometric Technology Today
ISSN (online): 1873-1880

Ethical and Legal Issues of Biometric Databases in Law Enforcement

Dr. Pranoti Prashant Mane[1], Sunil M Sangve[2], Dr Vivek Deshpande[3], Dr. Nitin Dhawas[4], Aishath Khaleela Abdul Sattar[5], Dr. Ganesh Vishnu Gosavi[6]

[1]Associate Professor and HOD, Department of Electronics & Telecommunications, MES's Wadia College of Engineering, Pune ppranotimane@gmail.com

[2]Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology, Pune, Maharashtra, India. sunil.sangve@vit.edu

[3]Vishwakarma Institute of Technology, Pune, Maharashtra, India. vivek.deshpande@viit.ac.in

[4]Professor & Dean Academics, Department of Electronics and Telecommunication Engineering, Nutan Maharashtra Institute of Engineering and Technology, Pune. nitin.dhawas@nmiet.edu.in

[5]Senior Lecturer, Faculty of Shariah and Law, Villa College, Maldives Email aishath.khaleela@villacollege.edu.mv

[6]M.Sc. PhD in Mathematics, Assistant Professor D Y Patil College of Engineering, Akurdi Email Id : gvg.math@gmail.com

Abstract: Biometric databases in law enforcement have become a pivotal tool for enhancing security and investigative efficiency. These databases, which store biometric identifiers such as fingerprints, facial recognition data, and iris scans, offer significant advantages in terms of identification accuracy and speed. However, their use raises a range of ethical and legal issues that merit careful consideration. Ethically, the deployment of biometric databases introduces concerns about privacy and consent. The collection and storage of biometric data involve sensitive personal information that is inherently unique to individuals. There is a risk that such data could be misused or accessed without proper authorization, leading to potential violations of privacy. The principle of informed consent becomes complex in law enforcement contexts, where individuals may not have a choice in providing their biometric data. Moreover, there is a potential for misuse of biometric data beyond its intended purpose, such as for unwarranted surveillance or profiling. Legally, the use of biometric databases intersects with various laws and regulations designed to protect individual rights. Data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, impose strict requirements on the collection, storage, and processing of personal data, including biometric information. In the United States, the Fourth Amendment protects against unreasonable searches and seizures, raising questions about the legal boundaries of biometric data collection and its use in law enforcement. Ongoing dialogue between stakeholders, including the public, legal experts, and technology developers, is essential to address these challenges and foster an environment where biometric technologies can be used responsibly and ethically in law enforcement.

Keywords: Privacy, Consent, Data Protection, Surveillance, Legal Compliance

I. Introduction

The advent of biometric technology has revolutionized the field of law enforcement, offering tools for rapid and accurate identification that were previously unattainable. Biometric databases, which store unique physiological or behavioral characteristics such as fingerprints, facial features, and iris patterns, have become integral to modern investigative practices. They enable law enforcement agencies to match suspects to crime scenes, verify identities quickly, and streamline various aspects of criminal justice. Despite these significant advantages, the use of biometric databases in law enforcement is fraught with ethical and legal challenges that necessitate a critical examination. One of the primary ethical concerns associated with biometric databases is the issue of privacy. Biometric data is intrinsically linked to an individual's identity and cannot be changed, unlike other personal

information such as passwords or social security numbers. This permanence makes the protection of biometric data particularly crucial. Unauthorized access or misuse of such data could lead to severe privacy violations, potentially exposing individuals to identity theft, wrongful accusations, or even unjust surveillance [1]. The ethical principle of privacy is fundamentally challenged when personal data is collected and stored without explicit consent or clear understanding of its potential uses. This raises important questions about how law enforcement agencies obtain and handle biometric information and whether individuals are adequately informed about the scope of its use. Consent, or the lack thereof, is another significant ethical issue in the realm of biometric databases. Unlike traditional forms of evidence collection, such as witness statements or physical evidence, biometric data is often collected in situations where individuals have limited choice or awareness. For instance, biometric data might be collected during routine interactions with law enforcement, such as traffic stops or arrests, without a thorough explanation of how this data will be used or protected [2]. This raises concerns about whether individuals are truly providing informed consent and if their rights are being adequately protected in these situations.

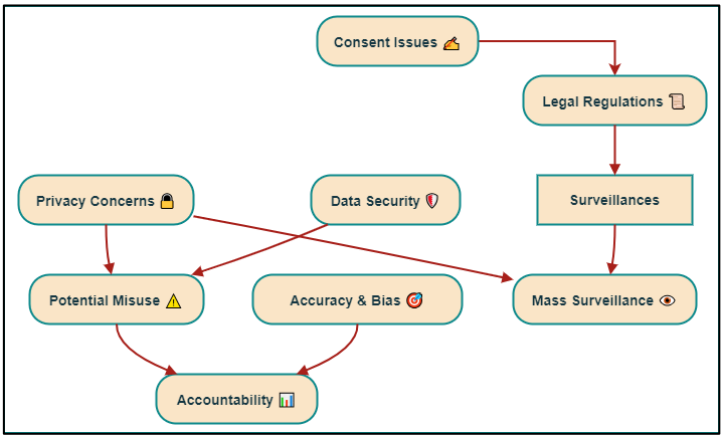

Figure 1: Ethical and Legal Issues of Biometric Databases in Law Enforcement

The ethical dilemma lies in balancing the benefits of enhanced security and investigative efficiency with the need to respect individual autonomy and privacy. From a legal perspective, the use of biometric databases intersects with a complex web of regulations and standards designed to protect personal data and civil liberties. Data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union, set stringent requirements for the collection, storage, and processing of personal information, including biometric data. These regulations emphasize the need for transparency, data minimization, and the secure handling of personal information [3]. In the United States, legal frameworks like the Fourth Amendment provide protection against unreasonable searches and seizures, which complicates the use of biometric data in law enforcement. Courts and lawmakers must navigate these legal boundaries to ensure that biometric databases are used in compliance with constitutional rights and data protection laws. Moreover, the issue of data security presents a significant legal challenge. Biometric databases are attractive targets for cyberattacks, given the sensitive nature of the information they hold. A breach of such a database could have far-reaching consequences, including the exposure of individuals' personal information and the potential for misuse. Ensuring robust security measures and protocols is crucial for maintaining public trust and protecting individuals' rights [4]. Law enforcement agencies must implement stringent safeguards to prevent unauthorized access, data breaches, and other security threats that could undermine the integrity of biometric systems.

II. Related Work

Research and discussions surrounding the ethical and legal issues of biometric databases in law enforcement have grown significantly as the technology has advanced. Scholars, legal experts, and policymakers have explored various aspects of this complex issue, shedding light on both the benefits and potential pitfalls of biometric systems. One notable area of research focuses on privacy concerns associated with biometric databases. Studies emphasize the challenges posed by the inherent permanence and sensitivity of biometric data. Unlike traditional data, biometric identifiers cannot be easily changed or revoked if compromised. This permanence makes the data particularly valuable and vulnerable, necessitating robust safeguards to prevent misuse. Research has explored the effectiveness of current data protection measures and advocated for stronger regulations to address the unique

risks posed by biometric data. Consent and autonomy are also critical issues explored in the literature [5]. Privacy advocates highlight the importance of informed consent in the collection and use of biometric data. It is often argued that current practices fall short of ensuring that individuals fully understand how their data will be used, raising ethical concerns about the legitimacy of consent obtained under these conditions. Additionally, revelations about government surveillance practices illustrate the potential for abuse in biometric data collection, highlighting the need for transparent policies and rigorous oversight [6]. Legal perspectives on biometric databases are informed by case law and statutory regulations. The implementation of comprehensive data protection laws has been a significant development in addressing the unique challenges of biometric data. These regulations specifically address biometric data and the complexities of applying them in law enforcement contexts. In the United States, the Fourth Amendment's interpretation in relation to biometric data collection has been scrutinized, with legal analyses exploring how courts protect privacy in the digital age.

III. The Role of Biometric Databases in Law Enforcement

A. Types of Biometric Data

Biometric data encompasses a range of physiological and behavioral characteristics used to uniquely identify individuals. The primary types of biometric data include fingerprints, facial recognition, DNA, iris scans, and voice patterns. Each type offers distinct advantages and applications in law enforcement. Fingerprints are one of the oldest and most widely used forms of biometric data. They involve the analysis of the unique patterns of ridges and valleys on the skin of the fingers. Modern systems use sophisticated algorithms and machine learning techniques to compare facial features against a database of known images [7]. This technology is increasingly used in public surveillance and security applications, enabling law enforcement to identify suspects or locate missing persons more effectively. DNA profiling involves analyzing specific regions of an individual's DNA to generate a unique genetic fingerprint. This method is highly accurate and can be used to link suspects to crime scenes, identify victims, and establish familial relationships. DNA databases have become essential in solving cold cases and providing conclusive evidence in criminal investigations. Iris scans capture the intricate patterns in the colored part of the eye. Each iris is unique, and the patterns remain stable throughout an individual’s life, making iris recognition a highly reliable method of identification [8]. Iris recognition is less common in everyday law enforcement but is used in high-security environments and critical applications where high accuracy is required.

B. Applications of Biometric Databases in Criminal Investigations

Biometric databases play a crucial role in modern criminal investigations, providing law enforcement with advanced tools for identification, verification, and evidence collection. The applications of these databases span a wide range of investigative tasks, from solving current cases to addressing historical crimes. One primary application is the identification of suspects. When law enforcement agencies collect biometric data from crime scenes, such as fingerprints or DNA, this information can be compared against existing databases to identify potential suspects. For instance, if a fingerprint or DNA sample collected from a crime scene matches a record in the database, it can lead to the identification of a suspect or person of interest. Biometric databases also aid in locating missing persons [9].

C. Benefits of Biometric Databases in Enhancing Law Enforcement Efficiency

Biometric databases offer numerous benefits that significantly enhance the efficiency of law enforcement agencies. These benefits include improved accuracy, faster identification, and enhanced investigative capabilities. Accuracy is one of the foremost advantages of biometric databases. Biometric identifiers, such as fingerprints and DNA, are unique to each individual, reducing the likelihood of false positives or mistaken identity [10]. The high accuracy of biometric data enables law enforcement to make more reliable identifications and connections, leading to more accurate and effective investigations.

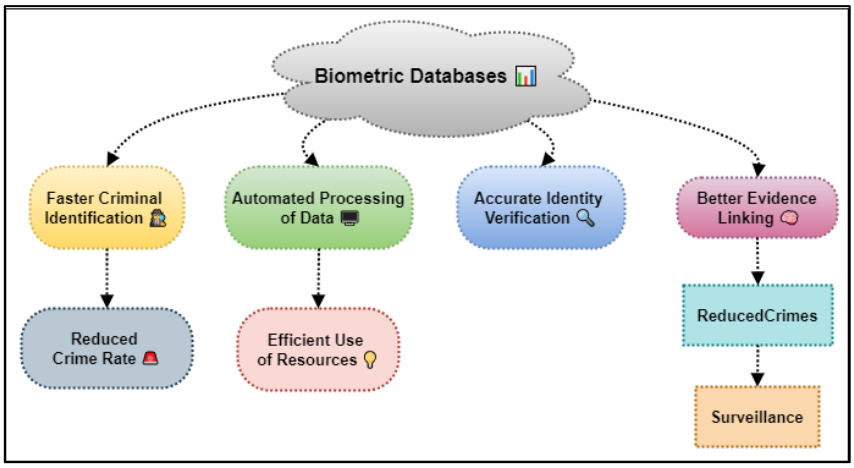

Figure 2: Benefits of Biometric Databases in Enhancing Law Enforcement Efficiency

This allows law enforcement personnel to focus on other critical aspects of their work, such as gathering evidence and interviewing witnesses. Integration with other systems is a significant advantage of modern biometric databases. Many databases can be integrated with existing law enforcement systems, such as criminal records management and surveillance systems. This integration provides a comprehensive view of investigative data, streamlining workflows and improving coordination among various departments and agencies. Deterrence is an indirect benefit of biometric databases.

IV. Ethical Issues Related to Biometric Databases

A. Data Security and Breaches

Data security is a critical concern in the realm of biometric databases. Given the sensitivity and uniqueness of biometric data, safeguarding it against unauthorized access, theft, and breaches is paramount. Biometric data, such as fingerprints, facial features, and DNA profiles, are inherently personal and immutable, meaning that once compromised, this data cannot be easily changed or revoked. This permanence increases the potential harm in the event of a security breach, making robust security measures essential [11]. Despite the implementation of advanced security protocols, biometric databases are not immune to cyberattacks and data breaches. Instances of hacking or insider threats can lead to the exposure of sensitive information, which could be exploited for identity theft, fraudulent activities, or wrongful accusations. The 2015 breach of the U.S. Office of Personnel Management, which compromised fingerprint data of millions of individuals, underscores the severe consequences of inadequate data protection. To address these concerns, it is crucial for organizations managing biometric databases to adopt comprehensive security strategies. These strategies should include encryption of biometric data, secure access controls, regular security audits, and prompt incident response mechanisms [12]. Additionally, there should be stringent protocols for data storage and transmission to mitigate risks associated with potential breaches. The ethical obligation to protect biometric data extends to ensuring that appropriate measures are in place to detect and respond to security threats, thereby safeguarding individuals' privacy and trust.

B. Consent and the Collection of Biometric Data

Consent is a fundamental ethical issue related to the collection of biometric data. The process of obtaining informed consent from individuals before collecting their biometric information is essential to respect personal autonomy and privacy. In many cases, especially in law enforcement contexts, individuals may not have a genuine opportunity to consent freely. For example, biometric data may be collected during routine interactions, such as traffic stops or arrests, where individuals may not fully understand or be able to negotiate the terms of data collection.

C. Ethical Implications of Data Retention Policies

Data retention policies for biometric databases raise significant ethical issues regarding how long biometric information should be kept and under what conditions it should be stored. The retention of biometric data must balance the benefits of maintaining records for law enforcement purposes with the potential risks of prolonged

storage. Extended data retention increases the risk of data misuse, unauthorized access, or accidental exposure, while also raising concerns about privacy and individual rights. By addressing these ethical concerns, organizations can promote transparency and trust in the handling of biometric data.

V. Legal Issues Surrounding Biometric Databases

A. Existing Laws and Regulations

The legal framework governing biometric databases varies by jurisdiction but generally includes a mix of data protection laws, privacy regulations, and specific statutes addressing biometric data. In many countries, biometric data is classified as sensitive personal information, and its collection, storage, and use are subject to stringent legal controls. In the European Union, the General Data Protection Regulation (GDPR) is a key regulation that addresses the processing of biometric data. Under GDPR, biometric data is classified as a special category of personal data, requiring explicit consent for its collection and processing. Organizations must demonstrate a lawful basis for processing such data, implement appropriate security measures, and adhere to principles of data minimization and purpose limitation. GDPR also mandates the right for individuals to access their data, rectify inaccuracies, and request erasure, offering a comprehensive approach to protecting biometric information. In the United States, there is no single federal law that comprehensively regulates biometric data. However, several states have enacted specific legislation. For instance, Illinois' Biometric Information Privacy Act (BIPA) imposes strict requirements on the collection, use, and storage of biometric data, including obtaining informed consent and providing clear data retention policies. Similarly, the California Consumer Privacy Act (CCPA) includes provisions related to biometric data within the broader framework of consumer privacy rights. The lack of a unified federal approach creates a patchwork of regulations that can be challenging for organizations operating across state lines. Internationally, various other countries have implemented or are considering regulations to address the unique challenges of biometric data.

B. Consent and Legal Standards for Biometric Data Collection

The legal standards for biometric data collection are closely tied to the concept of consent. In many jurisdictions, biometric data is classified as sensitive or special category data, requiring a higher standard of consent compared to other personal information. This typically involves obtaining explicit and informed consent from individuals before collecting their biometric data. Under GDPR, consent must be clear, informed, and freely given. Organizations are required to provide individuals with detailed information about the purposes of data collection, how the data will be used, and any potential risks. Consent must be specific and unambiguous, and individuals must have the option to withdraw their consent at any time. This high standard ensures that individuals are fully aware of and agree to the collection and processing of their biometric data. In the U.S., legal standards for consent can vary significantly by state. For instance, BIPA mandates that organizations must obtain written consent before collecting biometric data and provide a written policy on data retention and destruction. In contrast, other states may have less stringent requirements or no specific regulations on biometric data. This variability in consent standards can lead to inconsistencies in how biometric data is handled and protected across different jurisdictions. Ensuring that consent practices align with legal requirements is crucial for organizations to maintain compliance and protect individuals' rights. Implementing transparent and robust consent processes helps mitigate legal risks and fosters trust between organizations and the public.

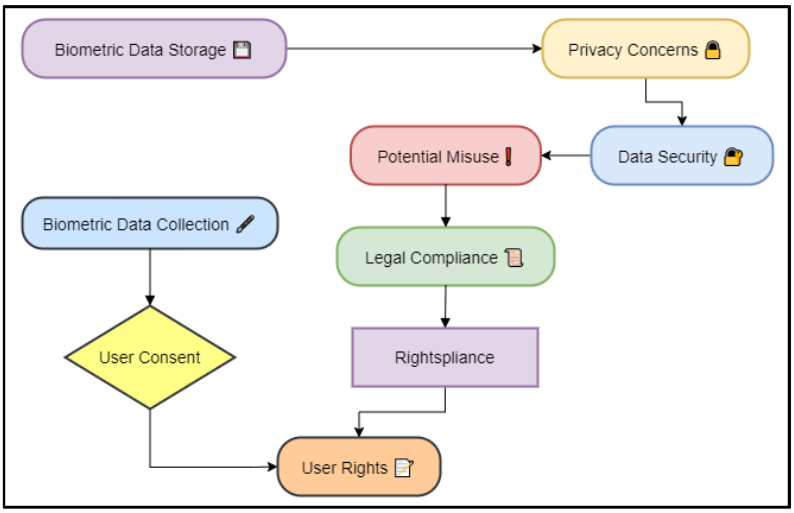

Figure 3: Illustrating Legal Issues Surrounding Biometric Databases

C. Accountability and Oversight Mechanisms

Accountability and oversight mechanisms are essential to ensure that biometric databases are managed in compliance with legal and ethical standards. Effective oversight helps prevent misuse, addresses potential breaches, and ensures that biometric data is handled with the utmost care. In jurisdictions with comprehensive data protection laws, such as the European Union under GDPR, oversight mechanisms are integral to regulatory compliance. Data protection authorities (DPAs) are responsible for monitoring and enforcing compliance with data protection regulations. These authorities have the power to conduct investigations, issue fines, and mandate corrective actions for organizations that fail to adhere to legal requirements. GDPR also requires organizations to appoint a Data Protection Officer (DPO) to oversee data handling practices and ensure adherence to legal standards. In the United States, oversight mechanisms vary depending on state regulations. For example, BIPA grants the Illinois Attorney General the authority to enforce compliance and pursue legal action against violators. However, the lack of a federal regulatory body dedicated to biometric data creates gaps in oversight and enforcement, leading to varying levels of accountability across different states. To enhance accountability, organizations managing biometric databases should implement internal controls and conduct regular audits to assess compliance with legal and ethical standards. Establishing clear policies for data handling, security, and breach response, along with providing training for staff, helps ensure that biometric data is managed responsibly.

VI. Impact of Biometric Databases on Civil Liberties

A. Impact on Public Spaces and Protests

The use of biometric databases in public spaces, such as through surveillance cameras equipped with facial recognition technology, can significantly impact civil liberties, particularly the freedom to gather and protest. Biometric surveillance in public areas can be used to monitor and identify individuals participating in demonstrations, rallies, or other public gatherings. This capability raises concerns about the potential for increased state control and repression of dissent. When biometric technology is deployed in public spaces, it can create an environment where individuals feel constantly watched, which may deter participation in public protests and social movements. The ability to track and identify individuals in real-time can lead to a chilling effect on free expression, where people self-censor or avoid public demonstrations due to fears of being monitored or targeted. This can undermine democratic freedoms and restrict the ability to protest and express dissenting views without fear of reprisal. Moreover, the extensive use of biometric surveillance in public areas can lead to a normalization of surveillance culture, where individuals become accustomed to being monitored as part of everyday life. This normalization can further erode the boundary between public and private spheres, impacting how people perceive their right to privacy and freedom of assembly.

B. Chilling Effect on Personal Freedoms

The chilling effect of biometric databases on personal freedoms arises from the fear of being constantly monitored and potentially misidentified. When individuals know that their biometric data, such as facial images or voice patterns, could be collected and analyzed without their knowledge or consent, they may alter their behavior to avoid drawing attention or being identified. This effect can manifest in various ways, including reduced participation in social or political activities, reluctance to engage in certain online or offline interactions, and self-censorship. The pervasive nature of biometric surveillance can lead to an environment where individuals feel compelled to conform to societal norms and avoid activities that might draw scrutiny. Such behavior undermines the fundamental principles of personal freedom and autonomy, as individuals should be able to express themselves and engage in activities without fear of surveillance or reprisal.

C. Expansion of Surveillance Networks

The expansion of biometric databases has contributed to the growth of surveillance networks, both in scope and sophistication. With advancements in biometric technology, law enforcement and security agencies have increasingly integrated biometric data into broader surveillance systems. These networks often combine multiple data sources, such as CCTV footage, social media profiles, and biometric identifiers, to create comprehensive profiles of individuals. The growth of these surveillance networks raises concerns about the potential for mass surveillance and the erosion of privacy rights. The ability to monitor and track individuals on a large scale can lead to the accumulation of vast amounts of personal data, which may be used to profile and target individuals based on their behavior or affiliations. This expansion can also increase the risk of data misuse, as large-scale surveillance systems are vulnerable to breaches and unauthorized access. Additionally, the integration of biometric data into surveillance networks can lead to a lack of transparency and accountability, as individuals may not be aware of how their data is being used or monitored. This lack of oversight can further exacerbate concerns about privacy violations and the potential for abuse of surveillance technologies.

VII. Result and Discussion

The integration of biometric databases in law enforcement offers substantial benefits in terms of identification accuracy and efficiency. However, it also presents significant ethical and legal challenges. Ethically, issues such as data security, consent, and the retention of biometric data raise concerns about privacy and autonomy. Legally, the framework for handling biometric data varies widely, with varying standards for consent and data protection across jurisdictions. The expansion of biometric databases can lead to increased surveillance, potentially infringing on civil liberties and public freedoms. Balancing the advantages of biometric technology with stringent ethical and legal safeguards is essential to ensure that its use respects individual rights and complies with established regulations.

Biometric Data Storage shows a moderate level of data privacy protection at 65%, indicating that while some safeguards are in place, there is room for improvement. Consent and transparency are relatively lower at 50%, highlighting concerns about how well individuals are informed about the use of their data. The risk of data misuse is notably high at 75%, reflecting significant apprehensions about potential breaches or improper use of stored biometric data.

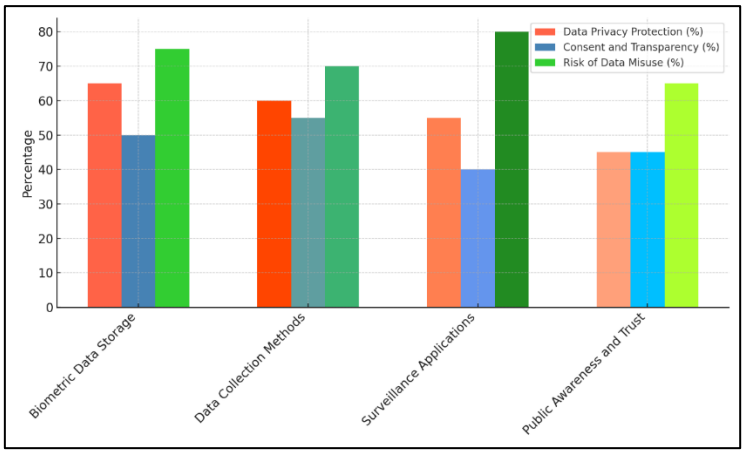

Figure 4: Comparison of Data Privacy, Consent, and Risk in Technology Practices

Data Collection Methods demonstrate a slightly better performance in data privacy protection at 60%, but still face challenges in ensuring comprehensive consent and transparency, which stands at 55%. The risk of data misuse in this category is 70%, suggesting that while collection methods may be somewhat controlled, the potential for misuse remains a serious concern.

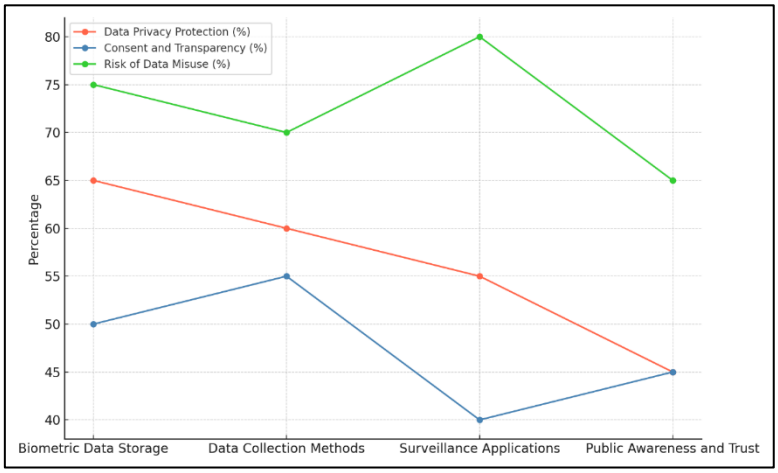

Figure 5: Trend Analysis of Privacy Protection, Transparency, and Risk Over Time

Surveillance Applications are the most problematic, with data privacy protection at 55% and consent and transparency at a low 40%. The risk of data misuse is the highest at 80%, indicating that surveillance practices pose the greatest threat to ethical standards. Public Awareness and Trust score the lowest in data privacy protection at 45% and consent and transparency at 45%, which may contribute to diminished public confidence and increased concerns about privacy and misuse, with a risk of data misuse at 65%.

GDPR (EU) demonstrates a strong compliance with data laws at 70% and robust data security enforcement at 75%, reflecting its comprehensive approach to data protection. However, accountability mechanisms at 60% and consistency of legal frameworks at 65% indicate that while GDPR provides a solid regulatory foundation, there is room for improvement in ensuring thorough accountability and uniformity across member states.

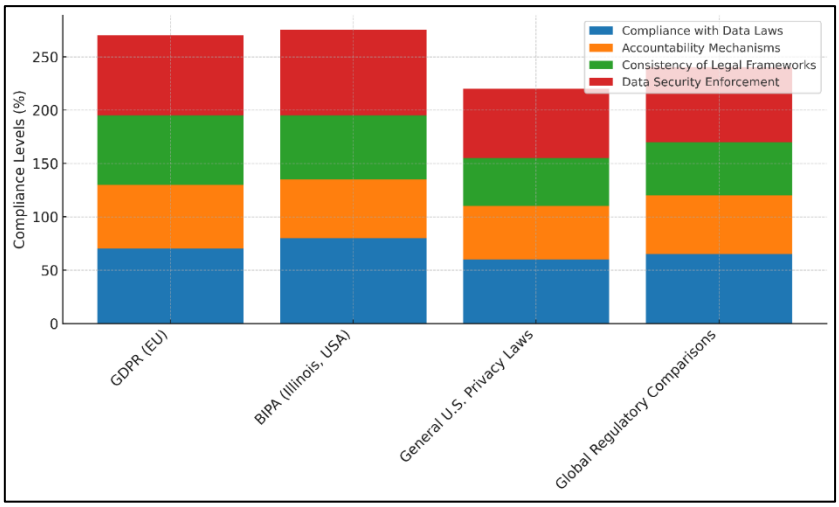

Figure 6: Comparative Compliance with Privacy Laws and Regulations

BIPA (Illinois, USA) stands out with high compliance with data laws at 80% and excellent data security enforcement at 80%. This suggests that Illinois has strong protections in place for biometric data. However, accountability mechanisms are weaker at 55%, and consistency of legal frameworks is only 60%, highlighting gaps in oversight and standardization compared to GDPR. General U.S. Privacy Laws exhibit lower performance, with compliance at 60%, accountability mechanisms at 50%, and consistency of legal frameworks at 45%. This indicates a less cohesive approach to biometric data protection across the U.S., with significant challenges in maintaining uniformity and robust oversight.

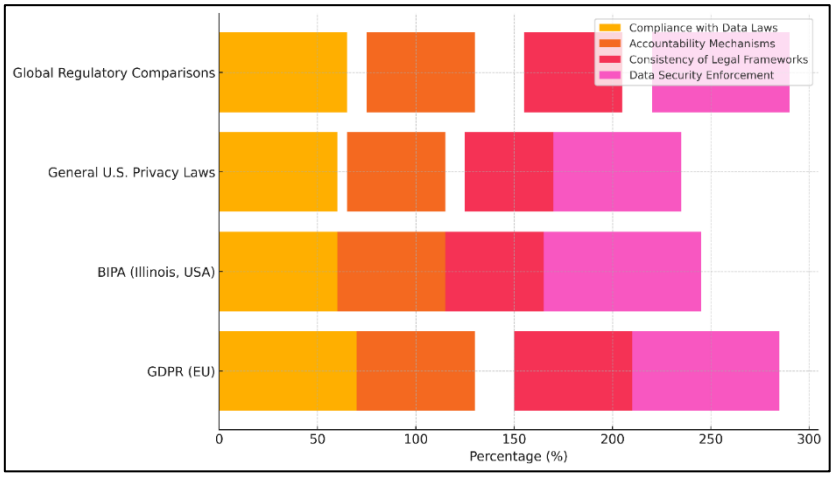

Figure 7: Distribution of Compliance Factors in Global Privacy Regulations

Data security enforcement is moderately better at 65%, but still falls short compared to more comprehensive frameworks like GDPR and BIPA. Global Regulatory Comparisons show a mixed performance with compliance at 65%, accountability at 55%, consistency at 50%, and data security enforcement at 70%. This reflects a varied global landscape where different regions have different strengths and weaknesses in regulating biometric data.

VIII. Conclusion

Biometric databases have become integral tools in modern law enforcement, enhancing the ability to identify individuals and solve crimes with unprecedented accuracy and speed. However, their use raises complex ethical and legal issues that require careful consideration. The permanence and sensitivity of biometric data necessitate robust security measures to protect against breaches and misuse. Ensuring that data is handled with the highest standards of security is crucial to maintaining public trust and protecting individual privacy. Ethically, the collection and use of biometric data must be accompanied by informed consent. Individuals should be fully aware of how their biometric information will be used, stored, and shared. The current practices in many jurisdictions

often fall short of these standards, raising concerns about whether consent is genuinely informed and voluntary. Additionally, the retention and potential misuse of biometric data pose significant ethical dilemmas, as individuals' personal information can be leveraged beyond its original purpose, leading to potential privacy violations and abuse. Legally, the regulatory landscape for biometric data is fragmented, with varying standards across different regions. While some jurisdictions have comprehensive data protection laws, such as the GDPR in the EU, others lack cohesive frameworks, leading to inconsistent protections and enforcement. The absence of a unified approach can create challenges for organizations and law enforcement agencies operating across borders. Furthermore, the expansion of biometric surveillance networks can impact civil liberties by increasing the potential for unwarranted surveillance and monitoring. This can have a chilling effect on public freedoms, such as the right to protest and express dissenting views. The balance between leveraging biometric technology for security purposes and safeguarding individual rights is delicate and requires ongoing scrutiny.

References

[1] Formosa, P. A principlist-based study of the ethical design and acceptability of artificial social agents. Int. J. Hum. Comput. Stud. 2023, 172, 102980.

[2] Pawlicka, A.; Choraś, M.; Kozik, R.; Pawlicki, M. First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions. Pers. Ubiquitous Comput. 2021.

[3] Pawlicki, M.; Choraś, M.; Kozik, R. Defending network intrusion detection systems against adversarial evasion attacks. Future Gener. Comput. Syst. 2020, 110, 148–154.

[4] Timmers, P. Ethics of AI and Cybersecurity When Sovereignty is at Stake. Minds Mach. 2019, 29, 635–645.

[5] Dhirani, L.L.; Armstrong, E.; Newe, T. Industrial IoT, Cyber Threats, and Standards Landscape: Evaluation and Roadmap. Sensors 2021, 21, 3901.

[6] Furey, H.; Hill, S.; Bhatia, S.K. Beyond the Code: A Philosophical Guide to Engineering Ethics; Taylor & Francis: Abingdon, UK, 2021.

[7] Martinho, A.; Herber, N.; Kroesen, M.; Chorus, C. Ethical issues in focus by the autonomous vehicles industry. Transp. Rev. 2021, 41, 556–577.

[8] Hansson, S.O.; Belin, M.Å.; Lundgren, B. Self-Driving Vehicles—An Ethical Overview. Philos. Technol. 2021, 34, 1383–1408.

[9] Siau, K.; Wang, W. Artificial intelligence (AI) Ethics: Ethics of AI and ethical AI. J. Database Manag. 2020, 31, 74–87.

[10] Campero-Jurado, I.; Márquez-Sánchez, S.; Quintanar-Gómez, J.; Rodríguez, S.; Corchado, J.M. Smart Helmet 5.0 for Industrial Internet of Things Using Artificial Intelligence. Sensors 2020, 20, 6241.

[11] Zhan, X.; Wu, W.; Shen, L.; Liao, W.; Zhao, Z.; Xia, J. Industrial internet of things and unsupervised deep learning enabled real-time occupational safety monitoring in cold storage warehouse. Saf. Sci. 2022, 152, 105766

[12] Kendal, E. Ethical, Legal and Social Implications of Emerging Technology (ELSIET) Symposium. J. Bioeth. Inq. 2022, 19, 363–370.