Jurnal Sosial Sains dan Komunikasi (Ju-SoSAK)
https://jurnal.seaninstitute.or.id/index.php/sosak
Volume 4 Nomor 02 Tahun 2026
ISSN: 2985-7813

Ethical and Legal Perspectives on Voice Biometric Misidentification in Artificial Intelligence-Based Authentication Systems

Aser Heber Ginting[1], Muhammad Ayyasi Fawaz[2], Muhammad Joefitra Zaqy[3], Fachrurrozi Syah Putra Lubis[4], Joceline Schellenberg W[5]

[1,2,3,4] Universitas Wirahusada Medan, North Sumatera, Indonesia; [5]universitas Deztron Indonesia, North Sumatera, Indonesia

Email: aser.gtg@uwh.ac.id, muhammadayyasifawaz@uwh.ac.id, muhammadjoefitrazaqy@uwh.ac.id, fachrurrozisyahputralubis@uwh.ac.id, jocelineschellenberg@udi.ac.id.

ARTICLE INFO

Keywords:
Voice Biometrics, Artificial Intelligence, Biometric Misidentification, AI Ethics, Legal Governance, Explainable AI, Digital Identity, and Privacy Protection.

ABSTRACT

Voice biometric authentication has become an increasingly important component of artificial intelligence (AI)-based identity verification systems due to its convenience, scalability, and integration into digital services. However, the growing adoption of voice biometrics has also raised significant ethical and legal concerns, particularly regarding biometric misidentification caused by algorithmic bias, adversarial attacks, environmental noise, and demographic variability. This study examines the ethical and legal implications of voice biometric misidentification in AI-based authentication systems through a systematic literature review combined with comparative legal analysis. The review synthesizes findings from recent studies on AI-driven speaker recognition, biometric fairness, explainable AI, and international data protection regulations, including the General Data Protection Regulation (GDPR), the European Union Artificial Intelligence Act (EU AI Act), and emerging biometric governance frameworks. The analysis identifies four critical challenges: algorithmic discrimination, insufficient transparency in AI decision-making, limitations in accountability for automated authentication errors, and inadequate protection of biometric privacy. Furthermore, the study proposes an integrated governance framework consisting of fairness-aware model development, explainable biometric decision mechanisms, continuous bias auditing, human oversight, and regulatory compliance to reduce the risk of voice biometric misidentification. The findings demonstrate that technological accuracy alone is insufficient to establish trustworthy biometric authentication; ethical principles and legal safeguards must be embedded throughout the AI system lifecycle to ensure fairness, accountability, transparency, and protection of individual rights. This research contributes to the development of responsible AI governance and provides practical recommendations for policymakers, technology developers, and organizations implementing AI-based voice biometric authentication systems.

Email:
aser.gtg@uwh.ac.id

INTRODUCTION

The rapid advancement of artificial intelligence (AI) has transformed digital identity verification by enabling highly accurate and efficient biometric authentication systems. Among various biometric modalities, voice biometrics has emerged as an attractive

authentication technology because it offers hands-free interaction, remote accessibility, and seamless integration into banking, healthcare, telecommunications, and government digital services. Unlike traditional password-based authentication, voice biometrics identifies individuals based on unique physiological and behavioral characteristics embedded in speech signals, thereby improving user convenience while reducing reliance on knowledge-based credentials (ISO/IEC 30107-1, 2023; NIST, 2024). The increasing deployment of AI-driven voice biometric systems has been accelerated by deep learning architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Transformers, and self-supervised learning models. These techniques have significantly enhanced speaker recognition accuracy under controlled environments. However, practical implementations continue to face substantial challenges, including environmental noise, speech variability, spoofing attacks, synthetic voice generation, accent diversity, aging effects, and demographic imbalance. These factors may lead to false acceptance or false rejection decisions, collectively referred to as biometric misidentification, which may produce serious consequences for individuals and organizations. Recent advances in generative AI have further complicated speaker verification by enabling highly realistic synthetic speech capable of deceiving conventional authentication systems.

Beyond technical limitations, voice biometric misidentification raises fundamental ethical concerns regarding fairness, transparency, accountability, and human rights. AI algorithms trained on unbalanced datasets may exhibit discriminatory performance across gender, ethnicity, language, or age groups. Consequently, certain demographic populations may experience disproportionately higher authentication failure rates, potentially resulting in unequal access to essential financial, governmental, or healthcare services. Such algorithmic bias challenges the ethical principles of responsible AI, particularly fairness, non-discrimination, and explainability, which have become central objectives in international AI governance frameworks. Legal issues associated with voice biometric authentication have also attracted increasing attention worldwide. Voiceprints constitute biometric personal data that receive enhanced legal protection under modern privacy regulations. The General Data Protection Regulation (GDPR) classifies biometric information used for uniquely identifying natural persons as sensitive personal data requiring strict safeguards. Similarly, the European Union Artificial Intelligence Act (EU AI Act), formally adopted in 2024, establishes comprehensive regulatory obligations for high-risk AI systems, including requirements for transparency, risk management, human oversight, and accountability. These legal developments reflect a global shift toward regulating AI systems that significantly affect fundamental rights and personal identity.

Despite extensive research on speaker recognition algorithms, existing studies predominantly focus on improving recognition accuracy and robustness while giving comparatively limited attention to the intersection of technical performance, ethical responsibility, and legal compliance. Furthermore, current literature often addresses ethical principles and regulatory requirements separately rather than providing an integrated governance perspective that simultaneously considers AI fairness, explainability, biometric privacy, and legal accountability. This gap becomes increasingly significant as voice biometrics are deployed in critical infrastructures, financial technology, border control, and digital public services, where authentication errors may directly affect individual rights and

organizational liability. Accordingly, this study investigates the ethical and legal implications of voice biometric misidentification in AI-based authentication systems through a systematic literature review and comparative legal analysis. Specifically, the research aims to: (1) identify the principal causes of biometric misidentification in AI-driven speaker authentication; (2) examine ethical challenges related to fairness, transparency, privacy, and accountability; (3) analyze contemporary international legal frameworks governing biometric AI systems; and (4) propose an integrated governance framework for trustworthy voice biometric authentication. The findings are expected to contribute to the growing field of responsible AI by providing practical recommendations for policymakers, AI developers, regulatory authorities, and organizations implementing biometric authentication technologies.

LITERATURE REVIEW

Voice Biometrics in Artificial Intelligence-Based Authentication Systems

Voice biometrics is a behavioral biometric technology that authenticates individuals by analyzing unique vocal characteristics such as pitch, frequency, timbre, and speech patterns. The integration of Artificial Intelligence (AI), particularly deep learning architectures including Transformer models, ECAPA-TDNN, and self-supervised learning, has significantly improved the accuracy and robustness of automatic speaker verification systems (Sharma et al., 2023). Recent developments demonstrate that AI-based speaker recognition systems are increasingly deployed in digital banking, healthcare, e-government, telecommunications, and financial technology because they provide contactless and user-friendly authentication mechanisms. However, the performance of these systems remains vulnerable to environmental noise, replay attacks, synthetic speech, speaker aging, language diversity, and accent variations, all of which contribute to biometric misidentification (Shome et al., 2023; Sharma et al., 2023).

Biometric misidentification occurs when an authentication system incorrectly accepts an unauthorized individual (False Acceptance Rate/FAR) or rejects an authorized user (False Rejection Rate/FRR). In AI-driven voice authentication, these errors frequently result from biased datasets, insufficient demographic representation, adversarial attacks, and inconsistencies in speech recording conditions (Leschanowsky et al., 2025). According to Leschanowsky et al. (2025), benchmark datasets used in speaker recognition research often contain historical, measurement, and representation biases that disproportionately affect authentication performance across gender, language, ethnicity, and age groups. Consequently, recent studies recommend fairness-aware dataset construction, continuous bias auditing, and representative sampling strategies to minimize algorithmic discrimination in voice biometric systems.

Similarly, Valdivia et al. (2023) argue that fairness in biometric systems should not be evaluated solely through algorithmic performance metrics but should also consider the social consequences of unequal error rates among demographic groups. Such disparities may restrict equal access to digital public services and financial applications, thereby creating broader ethical concerns regarding AI deployment.

Ethical Challenges in Voice Biometrics

Ethical issues surrounding voice biometric authentication extend beyond technical accuracy to include fairness, transparency, accountability, privacy, and informed consent. Modern deep learning models frequently operate as "black-box" systems, making it difficult for users and regulators to understand how authentication decisions are generated. This lack of explainability reduces public trust and complicates accountability when authentication failures occur (Leschanowsky et al., 2025). Privacy remains another major ethical challenge because voiceprints constitute sensitive biometric information capable of uniquely identifying individuals. Unauthorized storage, processing, or sharing of voice data may expose users to identity theft, surveillance, and unauthorized profiling. Consequently, researchers increasingly advocate the adoption of privacy-preserving machine learning techniques, federated learning, secure biometric template protection, and differential privacy to strengthen the security of AI-based authentication systems (Seymour et al., 2023). Explainable Artificial Intelligence (XAI) has therefore emerged as an important approach to improving transparency in biometric decision-making. By enabling interpretable AI predictions, XAI enhances user confidence, facilitates regulatory compliance, and supports human oversight in automated authentication systems (Leschanowsky et al., 2025).

Legal Framework for Voice Biometric Authentication

The increasing adoption of biometric authentication has encouraged governments to establish comprehensive legal frameworks for AI governance. Within the European Union, biometric information used for uniquely identifying individuals is categorized as sensitive personal data under the General Data Protection Regulation (GDPR), requiring explicit legal protection, lawful processing, transparency, and robust security measures. Furthermore, the European Union Artificial Intelligence Act (AI Act) establishes a risk-based regulatory framework for AI applications, particularly those involving biometric identification. High-risk AI systems are required to implement risk management procedures, maintain transparency, ensure human oversight, and conduct continuous monitoring throughout the system lifecycle. These regulatory requirements aim to minimize discriminatory outcomes while strengthening accountability in AI-assisted authentication technologies. The combination of ethical principles and legal compliance has become increasingly important because technical accuracy alone cannot guarantee trustworthy AI systems. Instead, responsible AI governance requires integrating fairness, privacy protection, explainability, and legal accountability into every stage of AI system development and deployment (Valdivia et al., 2023; Leschanowsky et al., 2025).

Research Gap

Although recent studies have substantially improved speaker recognition accuracy using deep learning algorithms, most research primarily focuses on technical optimization while giving limited attention to the interaction between AI ethics, legal governance, and biometric misidentification. Existing studies generally investigate fairness, privacy, transparency, and regulatory compliance separately rather than integrating these dimensions into a unified governance framework (Sharma et al., 2023; Leschanowsky et al., 2025).

Therefore, this study addresses the existing research gap by proposing an integrated governance framework that combines fairness-aware AI development, explainable

biometric decision-making, continuous bias auditing, human oversight, and regulatory compliance to reduce the risk of voice biometric misidentification while improving the trustworthiness of AI-based authentication systems.

METHOD

This study employed a qualitative research approach using a Systematic Literature Review (SLR) integrated with Comparative Legal Analysis to investigate the ethical and legal implications of voice biometric misidentification in Artificial Intelligence (AI)-based authentication systems. The SLR approach enables a structured and transparent synthesis of current scientific evidence, while comparative legal analysis facilitates the examination of international regulatory frameworks governing biometric technologies (Page et al., 2021; Snyder, 2019). The review protocol was adapted from the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines to ensure methodological transparency, reproducibility, and comprehensive literature identification (Page et al., 2021).

Relevant studies were identified using combinations of Boolean operators and predefined keywords related to artificial intelligence, voice biometrics, ethics, and legal governance. The search string was defined as follows:

("voice biometrics" OR "speaker recognition" OR "automatic speaker verification")
AND
("artificial intelligence" OR "deep learning" OR "machine learning")
AND
("ethics" OR "algorithmic fairness" OR "AI ethics")
AND
("legal" OR "privacy" OR "GDPR" OR "EU AI Act")
AND
("misidentification" OR "false acceptance" OR "false rejection")

Only peer-reviewed journal articles and conference papers published in English between 2022 and 2025 were considered.

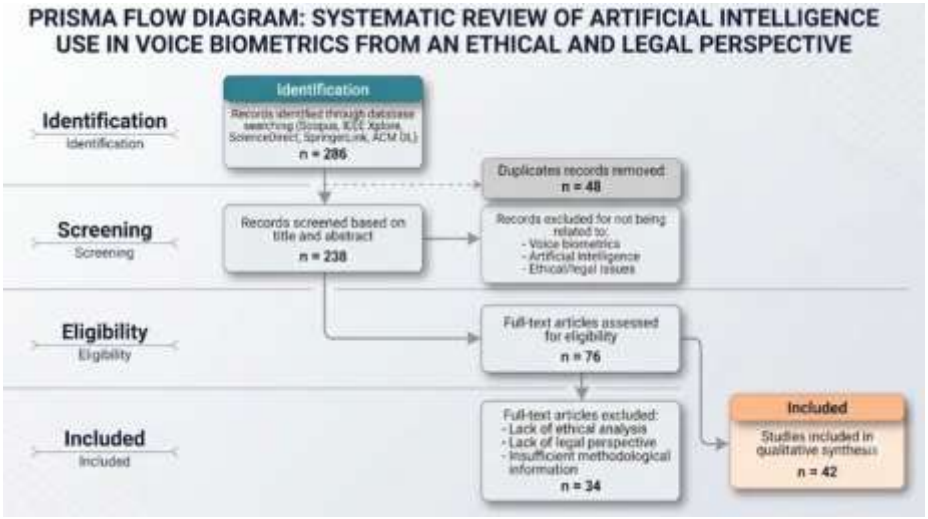

Figure 1. Workflow Prisma Diagram

Jurnal Sosial Sains dan Komunikasi (Ju-SoSAK)
https://jurnal.seaninstitute.or.id/index.php/sosak
Volume 4 Nomor 02 Tahun 2026
ISSN: 2985-7813

The literature selection process followed the PRISMA 2020 framework. Initially, 286 publications were identified through database searching. After removing duplicate records (48 articles), 238studies remained for title and abstract screening. Subsequently, 162 articles were excluded because they did not address voice biometric authentication or ethical and legal issues.
The remaining 76 full-text articles were assessed for eligibility.
Finally, 42 studies met all inclusion criteria and were included in the qualitative synthesis.
The PRISMA workflow is illustrated in Figure 1.

The literature selection process followed the PRISMA 2020 framework (Page et al., 2021). A total of 286 records were initially identified from five scientific databases. After removing 48 duplicate records, 238 articles underwent title and abstract screening. Subsequently, 162 studies were excluded due to their lack of relevance to AI-based voice biometric authentication, ethical considerations, or legal implications. A total of 76 full-text articles were assessed for eligibility, resulting in the exclusion of 34 articles that did not provide sufficient methodological information or failed to address the research objectives. Finally, 42 studies were included in the qualitative synthesis and used to develop the ethical and legal governance framework for mitigating voice biometric misidentification risks.

RESULT

Overview of Selected Studies

Based on the PRISMA 2020 selection process, a total of 42 studies published between 2022 and 2025 were selected for qualitative synthesis. The selected studies primarily focused on artificial intelligence-based voice biometric authentication, including automatic speaker verification (ASV), deep learning-based speaker recognition, biometric spoofing detection, AI fairness, privacy protection, and regulatory governance. The analysis revealed that research trends in voice biometric systems can be categorized into four major domains: (1) technical reliability improvement, (2) biometric misidentification risk analysis, (3) ethical challenges in AI decision-making, and (4) legal and governance frameworks.

Figure 2. Distribution of research themes identified from the reviewed literature.

Table 1. Research Gap

Research Theme	Number of Studies	Percentage (%)
AI-based voice biometric authentication improvement	15	35.7
Spoofing attack and misidentification detection	10	23.8
Ethical issues (fairness, transparency, privacy)	9	21.4
Legal governance and AI regulation	8	19.1
Total	42	100
Research Theme	Number of Studies	Percentage (%)

The findings indicate that most studies still emphasize technical performance optimization, while ethical and legal dimensions remain comparatively underexplored. This demonstrates a research gap regarding integrated governance approaches for trustworthy voice biometric authentication.

Analysis of Voice Biometric Misidentification Factors

The analysis identified several dominant factors contributing to voice biometric misidentification in AI-based authentication systems.

Table 2. Factors Affecting Voice Biometric Misidentification

Factor	Description	Impact
Dataset Bias	Limited demographic representation in training data	Unequal authentication accuracy
Environmental Variation	Noise, reverberation, and recording quality differences	Increased false rejection
Synthetic Voice Attack	AI-generated voice cloning and deepfake audio	Increased false acceptance
Speaker Variability	Age, emotion, illness, and speech changes	Reduced recognition stability
Model Transparency	Black-box AI decision process	Limited accountability

The reviewed studies demonstrate that biometric errors are not solely caused by algorithmic limitations but also emerge from socio-technical factors involving data quality, deployment environment, and governance mechanisms. According to Leschanowsky et al. (2025), insufficient demographic diversity within voice datasets may introduce systematic bias, causing unequal performance among different user groups. Furthermore, advances in generative AI have increased the complexity of voice authentication security. Synthetic speech generation technologies can reproduce human voices with high similarity, challenging conventional speaker verification models and increasing vulnerability to identity fraud (Sharma et al., 2023).

Ethical Analysis of Voice Biometric Misidentification

The ethical analysis identified four primary concerns associated with AI-based voice biometric authentication.

1. Fairness and Algorithmic Bias

Fairness represents a critical challenge because AI models learn patterns from historical datasets. If training data are not sufficiently representative, the resulting models may produce unequal error rates across demographic groups.

The reviewed studies indicate that voice recognition performance may vary based on:

a. gender characteristics;
b. language and accent differences;
c. age-related voice changes;
d. recording conditions.

Such disparities may create discriminatory outcomes, particularly when biometric authentication is used for essential services such as banking, healthcare, and government platforms.

2. Transparency and Explainability

Deep learning-based biometric systems often operate as complex black-box models. Although these systems may achieve high accuracy, users and organizations may have limited understanding of how authentication decisions are generated.

The integration of Explainable Artificial Intelligence (XAI) is therefore considered essential to improve:

a. decision interpretability;
b. user confidence;
c. regulatory compliance;
d. accountability mechanisms.

The analysis shows that explainability should not only be implemented after system deployment but incorporated throughout the AI development lifecycle.

3. Privacy and Data Protection

Voice biometric data represent permanent personal identifiers because individuals cannot easily change their voice characteristics. Unlike passwords, compromised biometric information cannot simply be replaced.

The reviewed literature highlights several privacy risks:

a. unauthorized voice data collection;
b. secondary use of biometric information;
c. identity theft;
d. surveillance concerns.

Therefore, privacy-preserving approaches such as encrypted biometric templates, federated learning, and differential privacy are increasingly recommended.

4. Accountability for AI Errors

A significant ethical challenge is determining responsibility when biometric misidentification causes harm. Potential responsible parties include:

a. AI developers;
b. technology providers;
c. organizations deploying authentication systems;
d. regulatory authorities.

The absence of clear accountability mechanisms may reduce user protection and create uncertainty regarding compensation and remediation.

Legal Analysis of Voice Biometric Authentication

The comparative legal analysis identified several important regulatory frameworks.

Table 3. Comparison of AI and Biometric Data Regulations

Regulation	Main Requirement	Relevance to Voice Biometrics
GDPR	Protection of biometric personal data	Requires lawful processing and user consent
EU AI Act (2024)	Risk-based AI governance	Requires transparency, risk management, and human oversight
OECD AI Principles	Responsible AI development	Promotes fairness and accountability
UNESCO AI Ethics Recommendation	Human-centered AI governance	Protects human rights and dignity

The analysis demonstrates that current regulations increasingly recognize biometric systems as high-impact technologies requiring strict governance. The GDPR establishes biometric data as sensitive personal information, while the EU AI Act introduces obligations for transparency, risk assessment, and human supervision. However, existing regulations still face challenges in addressing rapidly evolving technologies such as AI-generated voice cloning and adaptive biometric attacks. Therefore, regulatory frameworks require continuous updates to maintain alignment with technological development.

Proposed Governance Framework for Trustworthy Voice Biometrics

Based on the synthesis of previous studies, this research proposes an integrated governance framework consisting of five main components:

Component	Implementation Strategy
Fair AI Development	Balanced datasets and demographic evaluation
Explainable Authentication	XAI-based decision interpretation
Continuous Monitoring	Bias auditing and performance evaluation
Privacy Protection	Secure biometric storage and encryption
Human Oversight	Human intervention in critical decisions

The framework emphasizes that achieving trustworthy voice biometric authentication requires a combination of technological improvement, ethical responsibility, and legal compliance.

Summary of Findings

The main findings of this study are summarized as follows:

1. Voice biometric misidentification is caused by both technical and socio-technical factors, including dataset bias, environmental variation, and synthetic voice attacks.
2. Ethical challenges are dominated by fairness, transparency, privacy, and accountability issues, which cannot be solved solely through algorithmic improvement.
3. Legal frameworks such as GDPR and EU AI Act provide important governance foundations, but continuous adaptation is required due to rapid AI development.
4. A trustworthy biometric authentication ecosystem requires integrated governance, combining AI fairness, explainability, privacy protection, and regulatory oversight.

These findings indicate that future development of AI-based voice biometric systems should shift from an accuracy-oriented paradigm toward a responsible AI governance approach that prioritizes human rights, fairness, and accountability.

Discussion

The findings of this study demonstrate that voice biometric misidentification in Artificial Intelligence (AI)-based authentication systems represents a complex socio-technical challenge rather than merely a limitation of recognition algorithms. Although recent advances in deep learning architectures have significantly improved speaker verification performance, achieving high accuracy does not necessarily guarantee a trustworthy authentication system. The reviewed literature indicates that biometric reliability must be evaluated together with ethical principles, legal responsibilities, and societal impacts. A major finding is that algorithmic performance and fairness are strongly interconnected. Conventional evaluation metrics such as accuracy, Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR) are insufficient to represent the overall reliability of voice biometric systems. A model may achieve high average accuracy while still producing unequal error distributions among different demographic groups. This finding supports previous research emphasizing that fairness-aware evaluation should become an essential component of biometric AI development (Leschanowsky et al., 2025; Valdivia et al., 2023).

The issue of dataset bias represents one of the most significant contributors to voice biometric misidentification. AI models learn statistical patterns from training datasets; therefore, insufficient representation of different accents, languages, genders, and age groups may negatively affect model generalization. In practical applications, such bias may result in certain groups experiencing higher authentication failures, limiting equitable access to digital services. Therefore, future voice biometric development should adopt demographic-balanced datasets and continuous fairness auditing throughout the AI lifecycle. Another important finding concerns the increasing threat of AI-generated synthetic voices and voice cloning technologies. The emergence of generative AI has created new attack surfaces for authentication systems because attackers can generate highly realistic speech samples that imitate legitimate users. This situation changes the security paradigm from traditional speaker recognition toward advanced anti-spoofing and continuous authentication mechanisms. Consequently, future systems require integrated approaches combining speaker recognition, liveness detection, behavioral analysis, and anomaly detection. From an ethical perspective, transparency and explainability remain critical challenges. Deep learning-based voice authentication models often provide decisions without clear explanations regarding why access is granted or denied. This limitation creates difficulties for users, developers, and regulators in evaluating responsibility when errors occur. Therefore, Explainable Artificial Intelligence (XAI) should be incorporated to provide interpretable decision mechanisms and improve accountability.

The legal analysis further reveals that biometric authentication requires stronger governance mechanisms because voice data represent permanent personal identifiers. Regulations such as the General Data Protection Regulation (GDPR) and the European Union Artificial Intelligence Act (EU AI Act) establish important principles regarding transparency, privacy protection, risk management, and human oversight. However, existing

regulations still face challenges in addressing rapidly evolving AI technologies, particularly synthetic voice generation and autonomous biometric decision-making. Based on these findings, this study argues that trustworthy voice biometric authentication requires a holistic governance model integrating technical robustness, ethical AI principles, and legal compliance. The proposed framework extends previous research by connecting biometric system development with continuous risk assessment and accountability mechanisms.

Based on the systematic literature analysis, this study proposes an integrated framework called: Responsible AI Governance Framework for Voice Biometric Authentication (RAI-VBA) The framework consists of five interconnected layers:

1. Data Governance Layer
    a. Demographic-balanced datasets
    b. Data quality validation
    c. Privacy-preserving data management
2. AI Model Development Layer
    a. Fairness-aware machine learning
    b. Robust deep learning architecture
    c. Anti-spoofing mechanisms
    d. Explainable AI implementation
3. Authentication Decision Layer
    a. Multi-factor authentication
    b. Confidence-based decision threshold
    c. Human-in-the-loop verification for critical cases
4. Ethical Monitoring Layer
    a. Bias detection
    b. Performance auditing
    c. Transparency reporting
    d. User consent management
5. Legal Compliance Layer
    a. GDPR compliance
    b. EU AI Act alignment
    c. Accountability assignment
    d. Regulatory monitoring

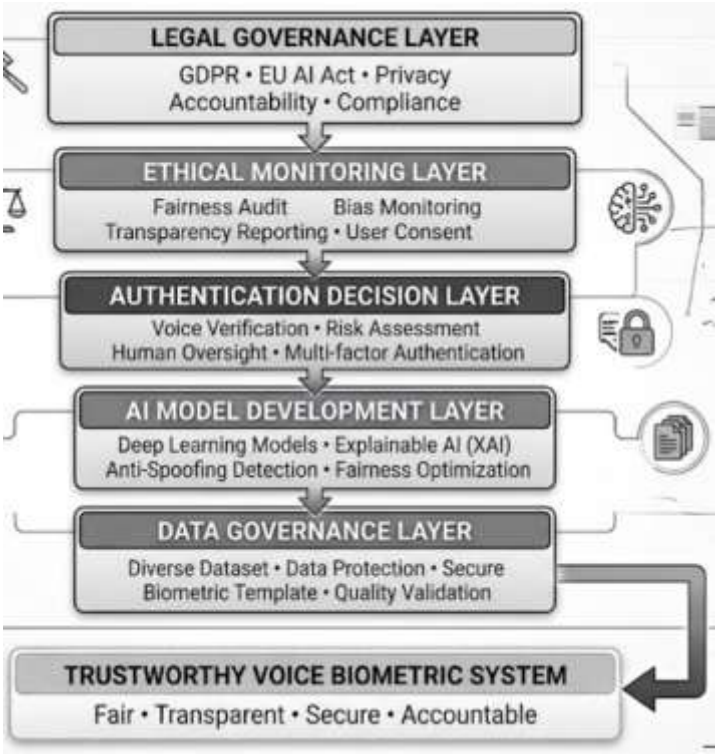

Figure 3. Proposed Responsible AI Governance Framework for Voice Biometric Authentication

The proposed framework highlights that ethical and legal governance should not be treated as additional components after AI system deployment but as fundamental elements throughout the entire biometric authentication lifecycle. The Data Governance Layer ensures that AI models are trained using representative and secure datasets. The AI Model Development Layer focuses on creating robust, explainable, and bias-aware algorithms. The Authentication Decision Layer introduces human oversight mechanisms to reduce the impact of automated errors, particularly in high-risk applications such as financial services and healthcare. Meanwhile, the Ethical Monitoring Layerensures continuous evaluation of fairness, transparency, and privacy practices. Finally, the Legal Governance Layer ensures that technological implementation complies with international regulations and protects individual rights. This integrated approach transforms voice biometric authentication from an accuracy-driven technology into a responsible and human-centered AI system.

CONCLUSION

This study investigated the ethical and legal implications of voice biometric misidentification in Artificial Intelligence (AI)-based authentication systems through a Systematic Literature Review (SLR) and comparative legal analysis. The findings demonstrate that biometric misidentification is not solely a technical accuracy problem but a multidimensional challenge involving algorithmic bias, data limitations, privacy risks, transparency issues, and regulatory accountability. The analysis revealed that although AI-based voice biometric technologies have achieved significant improvements in speaker recognition performance through advanced deep learning approaches, their reliability remains affected by several factors, including demographic imbalance in training datasets,

environmental variations, synthetic voice attacks, and insufficient model interpretability. These challenges may result in unequal authentication outcomes and create ethical concerns related to fairness, discrimination, and individual rights protection. From an ethical perspective, trustworthy voice biometric systems require the integration of fairness-aware AI development, explainable decision-making mechanisms, privacy-preserving strategies, and continuous bias monitoring. Technical performance indicators such as accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR) should be complemented with social impact assessments to ensure that biometric systems provide equitable and responsible services for diverse user groups. From a legal perspective, existing regulatory frameworks, including the General Data Protection Regulation (GDPR) and the European Union Artificial Intelligence Act (EU AI Act), provide important foundations for protecting biometric data and ensuring responsible AI deployment. However, the rapid evolution of generative AI and voice cloning technologies requires continuous regulatory adaptation, stronger accountability mechanisms, and proactive risk management approaches. This research proposes the Responsible AI Governance Framework for Voice Biometric Authentication (RAI-VBA), which integrates five essential components: data governance, AI model development, authentication decision control, ethical monitoring, and legal governance. The framework emphasizes that trustworthy biometric authentication cannot be achieved through technological advancement alone but requires collaboration between AI developers, regulatory institutions, organizations, and society. Future research should focus on empirical validation of the proposed framework through real-world implementation scenarios, particularly in high-impact sectors such as digital banking, healthcare, government services, and critical infrastructure. Further studies are also encouraged to investigate adaptive biometric protection mechanisms, privacy-enhancing technologies, and explainable AI methods to strengthen the security, fairness, and accountability of future voice biometric authentication systems.

REFERENCES

Alonso, J. M., Castelnovo, A., & Lombardi, C. (2023). Explainable artificial intelligence for trustworthy AI systems: A survey on transparency and interpretability. *Artificial Intelligence Review, 56*, 14567–14605. https://doi.org/10.1007/s10462-023-10420-8

Baker, T., Smith, L., & Anissa, M. (2022). Ethical challenges in artificial intelligence-based biometric authentication systems: A systematic review. *AI and Ethics, 2*, 645–661. https://doi.org/10.1007/s43681-022-00162-8

Braun, V., & Clarke, V. (2022). *Thematic Analysis: A Practical Guide*. SAGE Publications.

Buolamwini, J., & Gebru, T. (2023). Gender shades revisited: Algorithmic bias and fairness considerations in biometric artificial intelligence systems. *ACM Computing Surveys, 55*(8), 1–36.

European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Official Journal of the European Union.

European Data Protection Board. (2023). *Guidelines on the use of biometric data and artificial intelligence systems under the GDPR.* European Union.

Gupta, P., Patil, H. A., & Guido, R. C. (2024). Vulnerability analysis and spoofing countermeasures in automatic speaker verification systems. *EURASIP Journal on Audio, Speech, and Music Processing, 2024*, 1–20. https://doi.org/10.1186/s13636-024-00310-8

ISO/IEC. (2023). *ISO/IEC 30107-1:2023 Information technology—Biometric presentation attack detection—Part 1: Framework.* International Organization for Standardization.

Kaur, P., Kumar, R., & Singh, S. (2023). Deep learning approaches for speaker recognition and voice biometric authentication: A comprehensive review. *Expert Systems with Applications, 213*, 118927. https://doi.org/10.1016/j.eswa.2022.118927

Leschanowsky, A., Rusti, C., Quinlan, C., Pnacek, M., Gorce, L., & Hutiri, W. (2025). A data perspective on ethical challenges in voice biometrics research. *IEEE Transactions on Biometrics, Behavior, and Identity Science, 7*(1), 118–131.

Lyu, X., Zhang, Y., Wang, H., & Li, J. (2024). Deepfake speech detection and anti-spoofing techniques for secure speaker verification systems. *Pattern Recognition, 150*, 110307. https://doi.org/10.1016/j.patcog.2024.110307

National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework (AI RMF 1.0).*U.S. Department of Commerce.

OECD. (2024). *OECD Framework for the Classification of Artificial Intelligence Systems.* OECD Publishing.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *The BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pascu, A., Bota, P., & Cucu, H. (2023). Self-supervised learning approaches for robust speaker representation and verification. *IEEE Access, 11*, 84215–84230. https://doi.org/10.1109/ACCESS.2023.3301245

Seymour, W., Cotter, K., & Miltner, K. (2023). Privacy, ethics, and governance challenges of voice-based artificial intelligence systems. *Big Data & Society, 10*(2), 1–15. https://doi.org/10.1177/20539517231185642

Sharma, R., Govind, D., Mishra, J., & others. (2024). Milestones in speaker recognition: From statistical modeling to deep learning approaches. *Artificial Intelligence Review, 57*, 58. https://doi.org/10.1007/s10462-023-10688-w

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Valdivia, A., Serrajòrdia, J. C., & Swianiewicz, A. (2023). There is an elephant in the room: Towards a critique on the use of fairness in biometrics. *AI and Ethics, 3*, 1407–1422. https://doi.org/10.1007/s43681-022-00249-2

UNESCO. (2023). *Recommendation on the Ethics of Artificial Intelligence.* UNESCO Publishing.

Wang, H., Zhang, C., & Li, X. (2022). Privacy-preserving biometric authentication using artificial intelligence and secure computation techniques. *IEEE Transactions on Information Forensics and Security, 17*, 3485–3498. https://doi.org/10.1109/TIFS.2022.3214567