Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Legal and Ethical Implications of Biometric Data Collection in VR/AR Environments

Afreen Mujawar (Assistant Professor)
Department of Computer Science and Engineering,
SECAB Institute of Engineering and Technology (Affiliated to VTU Belagavi),
Vijayapur, Karnataka, India.

Rajeshwari Peeraji Khandekar
Department of Computer Science and Engineering,
SECAB Institute of Engineering and Technology (Affiliated to VTU Belagavi),
Vijayapur, Karnataka, India.

Dr. Noorullah Shariff
Department of AIML,
Ballari Institute of Technology and Management (Affiliated to VTU Belagavi),
Ballari, Karnataka, India.

***Abstract* - Utilising highly immersive environments that rely more and more on biometric inputs—such as gaze behaviour, facial expressions, speech patterns, and physiological indicators—to improve personalization and interactivity is now feasible due to the rapid development of VR and AR. These capabilities open up new possibilities in industries like healthcare, education, and entertainment, but they also present significant moral and legal dilemmas. This study investigates the complicated consequences of biometric data usage in VR/AR situations, with emphasis on privacy, informed consent, security, surveillance issues, and potential misuse. It assesses how well-suited existing legal frameworks—like GDPR, HIPAA, and new data protection laws—are to meeting the unique requirements of immersive systems while also pointing out where they fall short. The report also discusses the ethical obligations of developers and organizations, promoting openness, user autonomy, and fair data management. The paper offers doable suggestions for preserving rights while promoting innovation in immersive technology, drawing on legal research, moral reasoning, and real-world case studies.**

Keywords* - *Biometric, Collection, Data Virtual Reality, Augmented Reality

I. INTRODUCTION

Virtual Reality (VR) and Augmented Reality (AR) have revolutionised digital interaction, facilitating immersive participation across various sectors, including gaming, education, healthcare, defence, and collaborative environments. These systems progressively integrate biometric inputs—such as facial expressions, gaze tracking, vocal intonation, body position, and emotional signals—to provide more responsive and immersive user experiences. The amalgamation of biometric sensors and AI-driven analytics presents novel opportunities for personalisation and usefulness, yet simultaneously engenders significant legal and ethical dilemmas.

Biometric data fundamentally varies from traditional personal information due to its uniqueness, relative permanence, and frequent real-time collection. In immersive environments, users may lack awareness of the magnitude of data collecting, which raises significant concerns about consent, data governance, privacy, and the potential for profiling or exploitation. The demarcation between digital and physical realms further complicates the implementation of conventional laws and enforcement strategies.

While global data protection standards—such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other regional statutes—establish a framework for the protection of personal information, they are insufficient for tackling the enduring and contextually complex characteristics of biometric streams in virtual and augmented reality. Concurrently, there is a significant lack of comprehensive ethical frameworks specifically designed for these contexts.

This research seeks to examine the legal and ethical aspects of biometric data collecting in immersive technologies, assess the sufficiency of current rules, uncover regulatory deficiencies, and develop frameworks that enhance accountability while prioritising individual rights.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

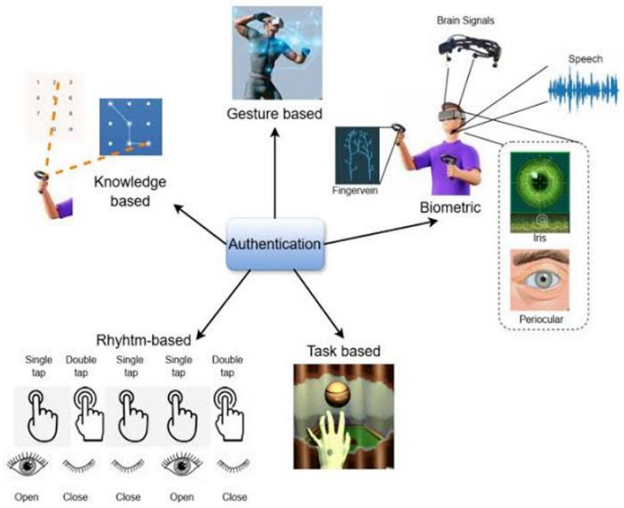

Figure: 1(a) Authentication Sources

Figure 1(a) categorises and visualises the primary authentication approaches relevant to immersive VR/AR systems, illustrating the integration of many modalities—from cognitive understanding to physical biometrics—for user identity verification.

Figure: 1(b)Data Collection Environments

Figure 1(b) illustrates a conceptual description of the fundamental ethical and legal difficulties associated with VR/AR biometric data collecting, highlighting the significance of user rights, transparency, and secure data management.

A. Background

Virtual Reality (VR) and Augmented Reality (AR) have advanced swiftly, evolving from specialised entertainment applications to essential instruments in education, healthcare, industrial training, social engagement, and defence. These systems operate efficiently owing to their ability to gather and analyse biometric data. This data encompasses physiological indications (e.g., heart rate, pupil dilation, skin temperature), behavioural indicators (e.g., gaze movement, gestures, vocal attributes), and, in certain instances, mental activity recorded via brain-computer interfaces. This ongoing acquisition allows systems to provide authentic, flexible, and exceptionally tailored experiences.

The dependence on biometrics has enhanced VR/AR functionalities while also exacerbating privacy issues, as these data streams are uniquely identifiable, enduring, and intrinsically sensitive. This necessitates a critical equilibrium between technology progress and accountable governance.

B. Risks to Privacy and Security

Biometric data gathered in VR/AR settings amalgamates unchangeable personal characteristics with behavioural and physiological indicators, rendering it both significant and susceptible. In contrast to conventional identifiers like passwords, biometric characteristics cannot be modified if they are hacked.

The immersive characteristics of these technologies provide continuous data collection at high resolution within context-rich environments, enabling profound conclusions regarding users' identification, health, preferences, and emotions. This depth and endurance exacerbate dangers such as unauthorised access or breaches.

• Vulnerability of sensitive biometric profiles to attackers.

• Characterization and Monitoring

Continuous monitoring may facilitate intrusive behavioural analytics.

• Regulatory Deficiencies

Current frameworks are inadequate for the intricacies of real-time, multi-modal biometric gathering.

Mitigating these dangers necessitates privacy-by-design, strong encryption, transparent policies, and international collaboration in regulatory enforcement.

C. Significance

The incorporation of biometric data into virtual reality and augmented reality systems has enhanced their functionality while simultaneously increasing legal and ethical concerns. Principal reasons for the importance of this research encompass:

1. Protecting Privacy and Autonomy—Guaranteeing that users maintain authority over sensitive personal information.
2. Addressing Legal Deficiencies—Revising frameworks to accommodate developing biometric technologies.
3. Ethical Governance - Formulating protocols for equitable and transparent use of biometric data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

4. Risk Mitigation - Averting misuse that may undermine public trust.
5. Global Significance — Transnational data transfers necessitate global standards.

II. LITERATURE REVIEW

A. Scope and Contemporary Trends

Research on biometrics in Extended Reality (XR)—including VR, AR, and MR—has considerably increased, with investigations into many modalities such as eye tracking, gait analysis, facial and iris identification, voice patterns, physiological responses, and neurological signals. A discernible trend has developed towards multimodal and continuous biometric acquisition in immersive environments, facilitating enhanced personalisation while simultaneously heightening privacy issues.

B. Technical Studies

Technical literature addresses biometric authentication inside immersive systems, encompassing both continuous verification and task-specific assessments. Numerous datasets have been created for headset-based biometrics, accompanied by assessments of vulnerabilities such as presentation assaults. Findings demonstrate that modalities like iris or periocular recognition and gesture-based identification can be exceptionally effective; yet, efficacy frequently hinges on device quality and context, with persistent vulnerabilities in cross-device and cross-session applications.

C. Analysis on Privacy and protection of data

Comprehensive research on eye tracking in virtual reality indicates that gaze patterns, when analysed with session content, can unveil intimate information such as emotional state, cognitive load, or personal preferences. Anonymisation solutions frequently exhibit fragility in immersive environments because to the uniqueness of high-frequency, multimodal biometric data streams.

D. Legal and Regulatory Considerations

Legal study categorises VR/AR biometric collecting within the framework of existing privacy regulations, including the GDPR in Europe and biometric-specific statutes such as Illinois' BIPA in the United States. Nonetheless, these frameworks were not designed for the continuous, inferential data streams characteristic of immersive environments. Prevalent legal concerns encompass:

- The sufficiency of one-time consent in contrast to continuous informed consent.
- Risks associated with "function creep" when data is utilised beyond its initial intent.
- The intricacy of enforcing privacy legislation in transnational operations.

E. Synthesis

From a technical perspective, VR/AR biometric systems provide robust identification and personalisation functionalities, although they also provide distinct security, privacy, and identifiability vulnerabilities. Current legal and ethical frameworks provide guiding principles but necessitate XR-specific explanations, especially for inferred sensitive data and continuous biometric processing.

III. METHODOLOGY

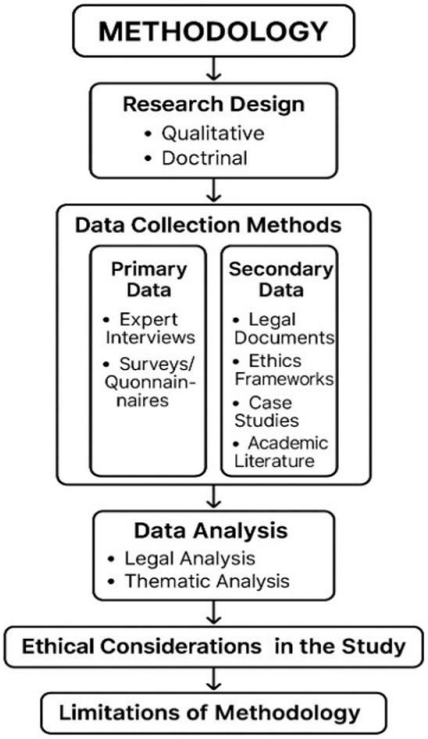

Figure 2: Methodology adopted in the research design

A. Research Approach

This research employs a qualitative and doctrinal methodology, integrating comparative legal analysis with ethical assessment to evaluate biometric data governance in immersive settings.

B. Data Sources

- Primary Data: Interviews with legal experts, VR/AR developers, and cybersecurity specialists; user surveys focussing on perceptions about biometric privacy in VR/AR.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

- Secondary Data: Examination of international privacy rules (GDPR, CCPA, DPDP Act), scholarly articles, industry analyses, and case studies.

C. Analysis Methods

- Legal Analysis: A comparative examination of regional and international legislation to discern regulatory deficiencies.
- Thematic Analysis: Classifying persistent ethical and privacy issues derived from interviews and literature.
- Ethical Considerations: Securing participant agreement, anonymising sensitive responses, and reducing bias in qualitative analysis.

D. Limitations

The principal constraint resides in the dearth of legal precedents unique to VR/AR and the swift evolution of technology, which can rapidly render regulatory interpretations obsolete.

IV. CONCLUSIONS

The integration of biometric data in virtual and augmented reality possesses transformative potential, facilitating increased personalisation, improved security, and immersive experiences. Nevertheless, it also presents a multifaceted set of legal and ethical dilemmas that must not be overlooked. Primary considerations encompass the protection of privacy, the assurance of informed consent, the establishment of stringent security protocols, and the formulation of appropriate policies for the management of ongoing and contextually rich biometric data streams.

A meticulous equilibrium between technological advancement and the safeguarding of fundamental rights is important. Resolving these difficulties necessitates collaborative efforts among legislators, developers, and industry stakeholders, in conjunction with the formulation of XR-specific guidelines. Implementing this approach will enhance user trust, mitigate risks of misuse, and foster the ethical and sustainable integration of immersive technology.

ACKNOWLEDGMENT

Author would like to extend her sincere thanks to her guide, HOD, Principal and Management of SECAB Institute of Engineering and Technology, Vijayapura, Karnataka, India for their kind support and encouragement to pursue this work.

REFERENCES

[1] G. Kumarapeli, D., Jung, S., & Lindeman, R. W. (2024). Privacy threats of behavior identity detection in VR, Frontiers in Virtual Reality.

[2] Bozkir, E., Özdel, S., Wang, M., et al. (2023). Eye-tracked Virtual Reality: A Comprehensive Survey on Methods and Privacy Challenges, arXiv preprint.

[3] Bisztray, T., Gruschka, N., Bourlai, T., & Fritsch, L. (2022). Emerging Biometric Modalities and Their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks, arXiv preprint.

[4] Survey of VR privacy and biometrics in Springer (2024).

[5] TrustArc (2024). Privacy in Augmented and Virtual Reality Platforms: Challenges and Solutions (Charlotte Tilbury BIPA case)

[6] IBA (2024?). AR and VR devices in the healthcare business: legal and ethical challenges

[7] Springer (2025). Augmented reality and ethics: key issues

[8] Springer (2024). Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations

[9] Frontiers in Virtual Reality—Privacy threats of behavior identity detection in VR https://www.frontiersin.org/articles/10.3389/frvir.2024.1197547/full

[10] ArXiv – Eye-tracked Virtual Reality: Privacy Challenges https://arxiv.org/abs/2305.14080

[11] Dentons – Virtual reality: Top data protection issues to consider https://www.dentons.com/en/insights/articles/2019/october/18/virtual-reality-top-data-protection-issues-to-consider