Biometric Technology Today
ISSN (online): 1873-1880

Biometric Contracts: Legal Considerations for Using Biometrics in Consumer Services

Dr. Yogesh Gurav[1], Dr. Rahul Manjre[2], Mr. Aakash Yadav[3], Dr. Hrishikesh Bhagat[4], Dr. Abhijeet Rajan[5], Amar Buchade[6]

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

[2]Assistant Professor, Bharati Vidyapeeth (Deemed to be University) Abhijit Kadam Institute of Management and Social Sciences, Solapur, India. rahul.manjre@bharatividyapeeth.edu

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

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

[5]Assistant Professor,Symbiosis Law School, Nagpur Campus, Symbiosis International (Deemed University), Pune, India, Email Id-abhijeetrajan@slsnagpur.edu.in

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

Abstract: As the use of biometric technologies—such as fingerprint recognition, facial identification, and voice authentication—grows in consumer services, so does the need for clear legal frameworks governing their deployment. Biometric contracts are emerging as a critical tool to address the unique legal challenges associated with biometric data. This paper explores the intersection of biometric technologies and legal considerations, focusing on how biometric contracts can be designed to protect consumer rights and ensure compliance with privacy laws. Biometric data, by its nature, is highly sensitive and personal, leading to concerns about privacy and data security. Traditional contracts often fall short in addressing the complexities of biometric data usage, which includes collection, storage, and sharing practices. Biometric contracts, therefore, need to encompass detailed provisions that specifically address the collection methods, consent processes, data protection measures, and the rights of individuals regarding their biometric information. This study examines various legal frameworks and privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, highlighting how these laws influence the drafting of biometric contracts. It also explores the challenges of ensuring informed consent, as biometric data collection can occur without explicit consumer awareness. The paper discusses best practices for developing biometric contracts that not only meet legal requirements but also build consumer trust through transparency and accountability. In addition, the paper evaluates the implications of biometric contracts for different stakeholders, including consumers, service providers, and regulatory bodies. It offers insights into how these contracts can be structured to address potential risks such as data breaches and unauthorized access. The study further considers the evolving landscape of biometric technology and the need for adaptive legal strategies that can respond to technological advancements and emerging threats.

Keywords: Biometric Data, Privacy Regulations, Consumer Consent, Data Protection, Legal Framework

I. Introduction

In recent years, biometric technologies have transformed various sectors, including consumer services, by providing innovative ways to authenticate identities and secure transactions. From fingerprint scanning and facial recognition to voice authentication, these technologies offer enhanced security and convenience. However, the

increasing reliance on biometric data raises significant legal and ethical concerns that necessitate careful consideration. The use of biometric information introduces unique challenges that traditional contracts and privacy policies may not adequately address. This has led to the emergence of biometric contracts—agreements designed specifically to manage the complexities associated with biometric data. Understanding the legal considerations surrounding these contracts is crucial for ensuring that consumer rights are protected while leveraging the benefits of biometric technologies. Biometric data, by its very nature, is highly personal and sensitive. Unlike other types of data, such as passwords or credit card numbers, biometric attributes are immutable and inherently linked to an individual's identity [1]. This uniqueness underscores the need for robust legal frameworks to govern the collection, use, and storage of such data. Biometric technologies have found applications in various consumer services, including banking, healthcare, and retail, where they enhance security measures and streamline user experiences. For instance, biometric authentication can simplify login processes and prevent fraud, offering significant advantages over traditional methods. However, these benefits come with increased risks of privacy breaches and misuse. Therefore, the development of comprehensive biometric contracts becomes essential to address these risks and provide clear guidelines for data handling. Traditional privacy policies and terms of service often fall short in addressing the specific needs of biometric data management [2]. Conventional contracts typically outline general terms related to personal data but may lack the specificity required for biometric information. For example, while standard privacy policies might cover data collection and usage, they may not sufficiently address the nuances of biometric data, such as the need for explicit consent before capturing biometric attributes or the protocols for safeguarding this data against unauthorized access.

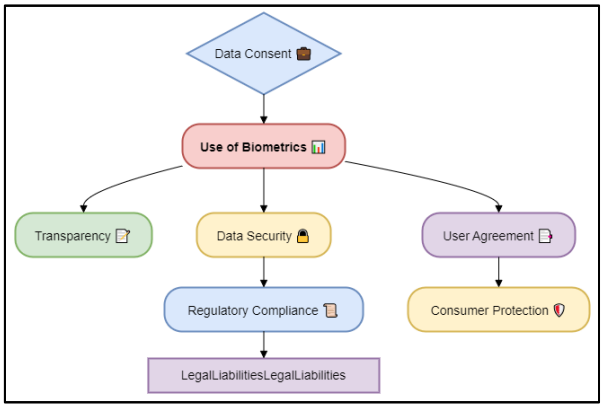

Figure 1: Illustrating legal considerations for biometric contracts

Biometric contracts must therefore be crafted with particular attention to the unique characteristics of biometric data, ensuring that they provide detailed provisions for consent, data protection, and individual rights. Legal frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have established important standards for data protection and privacy, influencing how biometric contracts should be designed [3]. The GDPR, for instance, includes specific provisions for the processing of sensitive data, which encompass biometric information used for uniquely identifying individuals. Similarly, the CCPA outlines rights related to data access and deletion, which are pertinent to biometric data handling. These regulations set a precedent for how biometric contracts should address consent requirements, data security measures, and individuals' rights to access and control their biometric information. Understanding and integrating these legal requirements into biometric contracts is crucial for ensuring compliance and protecting consumer rights. In addition to regulatory compliance, biometric contracts must address practical challenges related to informed consent [4]. Unlike traditional data collection methods, biometric data collection can occur passively or without the explicit knowledge of the individual. For instance, facial recognition systems might capture biometric data without a user's active engagement. This raises important questions about how to ensure that individuals are fully aware of and agree to the collection and use of their biometric data. Biometric contracts should include clear and transparent consent processes, informing consumers about what data is being collected, how it will be used, and their rights regarding this data.

The implications of biometric contracts extend beyond compliance and consent. They also encompass the responsibilities of service providers in safeguarding biometric data and mitigating risks associated with data

breaches. Biometric data breaches can have severe consequences, as compromised biometric attributes cannot be easily changed or replaced like passwords or credit cards [5]. Therefore, biometric contracts must outline stringent security measures and protocols for responding to data breaches, ensuring that service providers are held accountable for maintaining the integrity and confidentiality of biometric data. As biometric technologies continue to evolve, the legal landscape surrounding biometric contracts must also adapt. Emerging advancements in biometric technology may introduce new challenges and considerations that existing contracts may not fully address. For example, the use of advanced algorithms and machine learning techniques in biometric systems may raise new privacy concerns or affect the effectiveness of existing data protection measures. Consequently, biometric contracts must be designed with flexibility and foresight, allowing them to evolve in response to technological advancements and emerging risks.

II. Background Work

The integration of biometric technologies into consumer services has prompted significant academic and legal scrutiny, leading to the development of various frameworks and studies aimed at addressing the associated privacy and security concerns. Background work in this field primarily revolves around understanding the implications of biometric data use, the existing legal landscape, and the emerging need for specialized biometric contracts. Biometric technologies, which include fingerprint recognition, facial recognition, and iris scanning, have been widely adopted due to their potential to enhance security and user convenience. Research has shown that these technologies offer substantial benefits over traditional methods of authentication by providing more accurate and difficult-to-forge credentials. However, the inherent sensitivity of biometric data—being unique and immutable to individuals—raises critical privacy issues [6]. Academic studies have examined the risks associated with biometric data breaches, highlighting how the exposure of such data can lead to severe identity theft and misuse. Legal scholarship has increasingly focused on the inadequacies of traditional privacy laws in addressing biometric data concerns. Existing regulations such as the GDPR and the CCPA provide broad privacy protections but often lack specific provisions tailored to biometric data. For instance, GDPR categorizes biometric data as a special category of personal data, requiring explicit consent for its processing. However, the practical application of these regulations to biometric data remains complex due to the nuances involved in consent and data management. Similarly, the CCPA addresses biometric data but does not offer comprehensive guidelines on its use and protection, indicating a gap that biometric contracts aim to fill. In response to these challenges, researchers and legal experts have proposed various frameworks and best practices for developing biometric contracts [7]. These contracts are designed to address the specific needs of biometric data by incorporating detailed provisions for data collection, consent, security, and individual rights. Studies have suggested that effective biometric contracts should include clear terms regarding how biometric data is collected, stored, and used, as well as measures to ensure transparency and accountability. Additionally, there is a growing emphasis on the need for ongoing updates to these contracts to adapt to technological advancements and evolving privacy standards.

III. Legal Framework for Biometric Data

A. Existing Legislation (GDPR, BIPA, etc.)

The legal framework for biometric data is shaped by a variety of regulations designed to protect personal information, with notable examples including the General Data Protection Regulation (GDPR) and the Biometric Information Privacy Act (BIPA). The GDPR, implemented by the European Union, provides a comprehensive approach to data protection, including strict guidelines on biometric data, which is classified as a special category of personal data. Under the GDPR, processing biometric data requires explicit consent from the data subject, and such data must be handled with enhanced protection measures to prevent unauthorized access and misuse. The GDPR mandates that organizations must inform individuals about the purpose of data collection, the length of time data will be retained, and the rights individuals have regarding their data [12]. In the United States, BIPA is a state-level regulation enacted in Illinois that specifically addresses biometric data. Unlike federal regulations, BIPA provides a more detailed framework for biometric data, requiring entities to obtain informed consent before collecting or using biometric identifiers such as fingerprints and facial recognition. BIPA also stipulates that organizations must establish a written policy outlining how biometric data is stored, used, and destroyed. Furthermore, BIPA grants individuals the right to seek damages if their biometric data is mishandled, emphasizing the importance of compliance and transparency [13]. These legislations illustrate the evolving approach to

biometric data regulation, highlighting the need for organizations to adhere to specific consent requirements and data protection measures. However, the differences between GDPR and BIPA also underscore the challenges faced by multinational companies in harmonizing their data protection practices across different jurisdictions.

B. Data Privacy Laws and Biometrics

Data privacy laws play a crucial role in shaping how biometric data is managed and protected. While general privacy laws provide a broad framework for personal data protection, the unique nature of biometric data necessitates additional considerations. Privacy laws such as the GDPR and BIPA focus on ensuring that biometric data is collected and processed with the highest level of security and transparency. These regulations address key aspects such as data subject consent, data retention policies, and the implementation of robust security measures to prevent unauthorized access. One significant challenge in applying data privacy laws to biometric data is ensuring informed consent. Unlike other personal data, biometric data is often collected passively, making it difficult to obtain explicit consent [14]. Privacy laws require that individuals are aware of and agree to the collection and use of their data, which can be complex when dealing with biometric attributes. Additionally, the requirement to implement stringent security measures and provide clear policies on data handling reflects the heightened sensitivity of biometric data and the potential risks associated with its misuse. The interplay between data privacy laws and biometric data highlights the need for specialized regulations and practices to address the unique challenges posed by biometric information. As biometric technologies continue to evolve, data privacy laws must adapt to ensure that they effectively protect individuals' rights and maintain the integrity of their personal data.

C. International Legal Considerations

International legal considerations are increasingly relevant as biometric technologies gain global traction. Different countries have varying approaches to regulating biometric data, resulting in a complex landscape for multinational organizations. The GDPR serves as a prominent example of an international regulation that sets a high standard for biometric data protection. Its extraterritorial reach requires organizations outside the EU to comply if they process data of EU citizens, influencing global data protection practices. Other countries have also introduced their own regulations, which may differ significantly from the GDPR. For instance, countries like Brazil and Japan have enacted data protection laws that include provisions for biometric data, but the specifics of these laws can vary [15]. This diversity in regulations creates challenges for organizations operating across borders, as they must navigate and comply with multiple legal frameworks. International cooperation and alignment of data protection standards are essential to address these challenges.

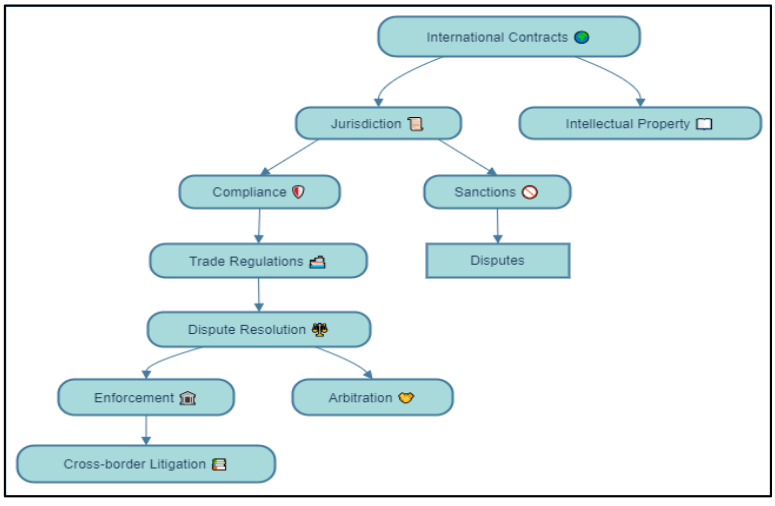

Figure 2: Illustrating International Legal Considerations

Efforts to harmonize regulations, such as through international agreements or frameworks, could simplify compliance and enhance the protection of biometric data globally. Additionally, organizations must stay informed about evolving legal standards and adapt their practices to meet the requirements of different jurisdictions.

IV. Contractual Considerations

A. Consent Requirements

Consent is a foundational element in the legal and ethical management of biometric data, and it plays a crucial role in biometric contracts. Given the sensitive nature of biometric information, obtaining explicit and informed consent from individuals is not only a legal requirement but also a critical aspect of protecting their privacy. Consent requirements are often outlined in various privacy regulations, such as the GDPR and BIPA, which mandate that organizations secure clear and affirmative consent before collecting, processing, or sharing biometric data. In biometric contracts, consent provisions must be detailed and transparent. Individuals should be fully informed about the purpose of biometric data collection, the scope of its use, and how long it will be retained [16]. Contracts should specify whether the consent is for a one-time use or an ongoing basis and outline the process for withdrawing consent. It is essential that consent is obtained through a clear and unambiguous action, such as signing a contract or clicking an opt-in button, rather than through pre-ticked boxes or passive acceptance. Additionally, biometric contracts should address scenarios where biometric data might be shared with third parties, ensuring that consent is obtained for such disclosures as well. To comply with legal standards and foster trust, biometric contracts must also provide mechanisms for individuals to access their data, review how it is used, and request its deletion if they choose to withdraw consent. Effective consent management not only meets regulatory requirements but also enhances transparency and strengthens the relationship between organizations and their customers.

B. Data Ownership and Control

Data ownership and control are central to biometric contracts, reflecting the rights of individuals over their personal information. Biometric data is unique because it is intrinsically linked to an individual's identity, making clear delineation of ownership and control crucial. Typically, biometric contracts should specify that individuals retain ownership of their biometric data, while the organization collecting the data is granted specific usage rights under clearly defined conditions. Contracts should address how data ownership impacts data management, including storage, processing, and access rights. It is important to establish protocols for data security, ensuring that biometric data is protected against unauthorized access or breaches. Organizations must also clarify their responsibilities in maintaining data integrity and providing individuals with control over their data, including rights to access, correction, and deletion. Data ownership clauses should be structured to comply with applicable laws and regulations, and clearly state how data will be used, shared, and ultimately disposed of. Furthermore, biometric contracts should address scenarios involving data transfers or sharing with third parties, ensuring that individuals are informed and that their data remains protected. By clearly defining data ownership and control, biometric contracts help to mitigate potential disputes and enhance compliance with privacy laws.

C. Terms of Use and Limitations

The terms of use and limitations outlined in biometric contracts are vital for defining the scope and boundaries of biometric data utilization. These terms should provide a comprehensive overview of how biometric data can be used, including any restrictions or limitations on its use. Contracts should specify the permissible purposes for which biometric data can be collected and processed, such as authentication, security, or user identification, and outline any conditions under which data may be shared with third parties. Effective biometric contracts also include limitations on data retention, ensuring that biometric data is not stored longer than necessary for its intended purpose. Terms should specify the duration for which biometric data will be retained and the procedures for securely deleting or anonymizing it once it is no longer needed. Additionally, contracts should address limitations related to the use of biometric data for secondary purposes, such as research or marketing, ensuring that any such uses are explicitly authorized and subject to additional consent. Another important aspect of terms of use is the inclusion of provisions related to data security and breach notification. Contracts should outline the security measures in place to protect biometric data and specify the steps that will be taken in the event of a data breach. By clearly defining the terms of use and limitations, biometric contracts help to establish clear expectations, ensure compliance with legal requirements, and protect the rights of individuals.

V. Consumer Rights and Protections

A. Right to Privacy

The right to privacy is a fundamental aspect of consumer rights, particularly when dealing with sensitive biometric data. This right underscores the importance of safeguarding individuals' personal information from unauthorized access, misuse, and exposure. Biometric data, being intrinsically tied to a person's identity, is particularly vulnerable to privacy breaches, making stringent privacy protections essential. Biometric contracts must clearly outline how an individual's privacy will be protected throughout the data lifecycle. This includes specifying measures for data encryption, secure storage, and controlled access to ensure that biometric information is not exposed to unauthorized parties. Contracts should also detail how data is anonymized or pseudonymized to reduce privacy risks, particularly in scenarios where data is used for analytics or research purposes. Additionally, the right to privacy involves informing individuals about the types of biometric data collected, the purposes for which it is used, and any potential risks associated with its collection. Transparency in data practices helps build trust and ensures that consumers are fully aware of how their information is handled. Biometric contracts should include explicit clauses that address privacy concerns, such as limiting data sharing and ensuring that any third parties involved adhere to the same privacy standards.

B. Right to Access and Correct Data

The right to access and correct data is a crucial consumer protection that enables individuals to review and amend their biometric information. This right ensures that consumers can verify the accuracy of their data and request corrections if discrepancies are found. Given the sensitivity of biometric data, it is vital that consumers have control over their information and can ensure it remains accurate and up-to-date. Biometric contracts should include provisions for data access, allowing individuals to request and obtain copies of their biometric data. The process for accessing data should be straightforward and accessible, with clear instructions provided within the contract. Additionally, individuals should be able to request corrections or updates to their biometric information, and organizations must have procedures in place to accommodate these requests efficiently. Ensuring that consumers can exercise their right to access and correct their data also involves clear communication about how these rights can be exercised. Contracts should specify the process for submitting access or correction requests, the time frame for responses, and any potential costs involved. By facilitating easy access and correction, organizations not only comply with legal requirements but also demonstrate a commitment to consumer rights and data integrity.

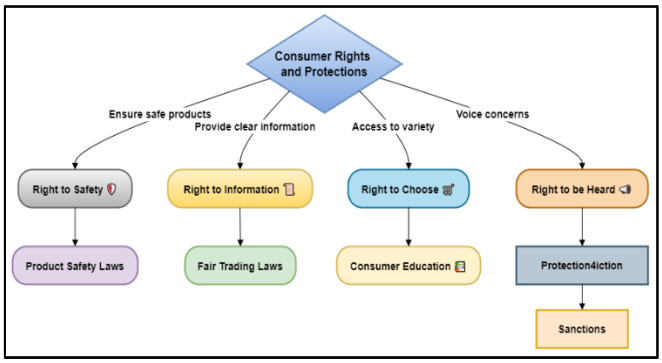

Figure 3: Illustrating Consumer Rights and Protections

C. Opt-Out Mechanisms and Informed Consent

Opt-out mechanisms and informed consent are pivotal in biometric contracts, providing individuals with control over their participation in biometric data collection and use. Informed consent requires that individuals are fully aware of and agree to the collection, processing, and potential sharing of their biometric data before it occurs. This consent must be obtained through clear, unambiguous actions and should be given voluntarily. Biometric contracts should incorporate robust opt-out mechanisms that allow individuals to withdraw consent or refuse to participate in biometric data collection without facing negative consequences. These mechanisms should be easy to use and should not penalize individuals for exercising their right to opt-out. Additionally, contracts must inform consumers of their right to withdraw consent at any time and describe the implications of doing so, including the

potential impact on their ability to use certain services or features. Informed consent goes beyond merely obtaining approval; it involves ensuring that individuals understand the scope, purpose, and risks associated with biometric data collection. Contracts should provide comprehensive information about how biometric data will be used, stored, and shared, including any third parties involved. By ensuring that consent is genuinely informed and offering clear opt-out options, organizations can uphold consumer autonomy and trust while adhering to legal and ethical standards.

VI. Future Legal Challenges

A. Emerging Technologies and Their Legal Implications

As biometric technologies advance, new legal challenges are likely to emerge, driven by innovations such as advanced facial recognition, gait analysis, and biometric authentication through behavioral patterns. These technologies expand the scope of data collection and introduce new complexities into the legal landscape. For example, advancements in facial recognition technology can now identify individuals even in low-resolution images or from non-frontal angles, raising concerns about privacy and consent, especially in public spaces where individuals might not expect their biometric data to be captured or analyzed. One significant legal implication of these emerging technologies is the need to address the accuracy and potential biases inherent in biometric systems. As these technologies become more sophisticated, they may inadvertently perpetuate or even exacerbate existing biases, such as racial or gender biases, leading to discriminatory practices. This raises questions about fairness and accountability, necessitating stringent regulations to ensure that biometric systems are both accurate and equitable. Additionally, the increasing integration of biometric technologies into various aspects of daily life—from personal devices to public surveillance—highlights the need for comprehensive legal frameworks that address both privacy and security concerns. Regulations will need to keep pace with technological advancements to prevent misuse and ensure that individuals' rights are protected. This includes revisiting and updating existing laws to encompass new forms of biometric data and ensuring that legal standards remain relevant and effective in addressing the unique challenges posed by emerging technologies.

B. The Evolution of Biometric Contracts

The evolution of biometric contracts reflects the growing recognition of the need to address the specific challenges associated with biometric data. Initially, standard privacy policies and terms of service were insufficient to address the complexities of biometric data, leading to the development of specialized biometric contracts. These contracts are designed to provide more detailed and precise terms regarding data collection, processing, and protection. As biometric technologies continue to advance, biometric contracts will need to evolve to address new challenges and incorporate emerging best practices. For example, contracts may need to include provisions for novel data types, such as behavioral biometrics, and adapt to new privacy and security standards. Additionally, the evolution of biometric contracts will likely involve increased emphasis on transparency and consumer rights, with contracts providing clear and comprehensive information about how biometric data is used, stored, and shared. Moreover, the development of biometric contracts will need to address cross-border data transfers and compliance with international regulations. As organizations operate globally, they must navigate varying legal requirements across jurisdictions, making it essential for biometric contracts to include clauses that ensure compliance with diverse legal standards.

C. Recommendations for Policy and Legal Reform

To address the future legal challenges posed by biometric technologies, several policy and legal reforms are recommended. First, policymakers should prioritize the development of comprehensive and adaptive legal frameworks that specifically address the unique aspects of biometric data. This includes updating existing privacy laws to incorporate provisions tailored to biometric technologies and ensuring that regulations cover emerging data types and uses. Second, there is a need for international cooperation to harmonize biometric data regulations across borders. Given the global nature of technology and data flows, aligning legal standards can help address issues related to cross-border data transfers and ensure consistent protection for individuals worldwide. Third, it is crucial to enhance oversight and accountability mechanisms for biometric data usage. Establishing independent regulatory bodies or enhancing existing ones can provide robust oversight and enforcement of biometric data regulations. These bodies can also play a role in monitoring technological advancements and ensuring that legal

standards evolve in response to new developments. Lastly, public awareness and education about biometric data rights and protections should be increased. Consumers must be informed about their rights regarding biometric data and the implications of its use. This can empower individuals to make informed decisions and advocate for their privacy and security in the evolving digital landscape.

VII. Result and Discussion

The analysis of biometric contracts reveals that while existing regulations like GDPR and BIPA set foundational standards for biometric data protection, there are significant gaps in addressing emerging technologies and complex data usage scenarios. Effective biometric contracts must incorporate specific consent requirements, clear data ownership, and comprehensive privacy protections to address these gaps. The evolving nature of biometric technologies necessitates continuous updates to contractual terms to remain compliant with new legal standards and technological advancements. Future legal frameworks should focus on harmonizing international regulations, enhancing transparency, and implementing robust security measures to safeguard biometric data, ensuring both consumer protection and the effective use of biometric innovations in consumer services. The evaluation of biometric contracts based on privacy and consent parameters provides a comprehensive assessment of how effectively these contracts protect consumer rights and ensure transparency. The parameter of Informed Consent Clarity scores 85%, reflecting the importance of consumers being fully aware of and agreeing to how their biometric data is collected and used.

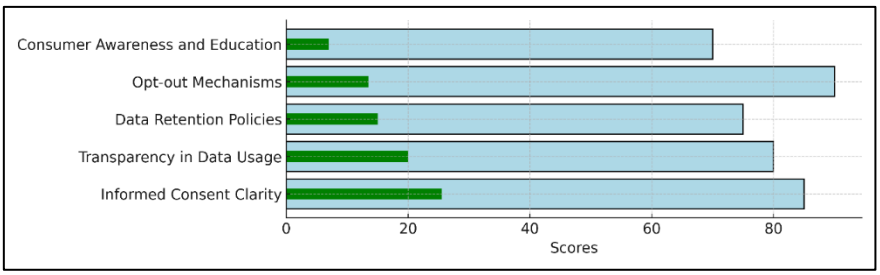

Figure 4: Scores of Privacy Features by Category

This is weighted heavily at 30%, as informed consent is a legal and ethical cornerstone in biometric data collection. Transparency in Data Usage, with a score of 80%, signifies that many biometric contracts provide clear information on how data will be used, but there is room for improvement.

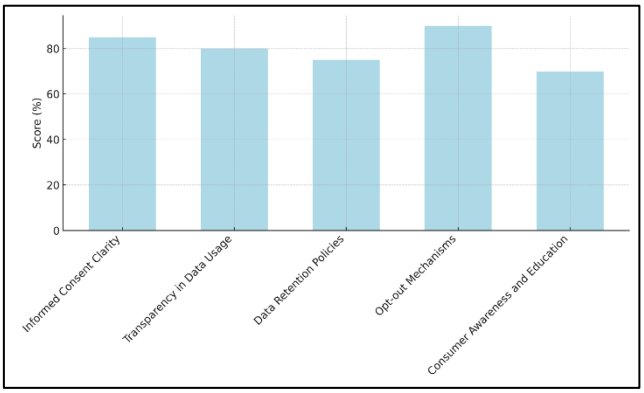

Figure 5: Evaluation of Data Privacy Policies

Weighted at 25%, transparency is critical to maintaining consumer trust and ensuring compliance with privacy regulations. Data Retention Policies scored 75% and were weighted at 20%. While organizations generally establish retention policies, there is often ambiguity about how long data is stored and when it will be deleted, which can affect compliance with privacy laws. Opt-out Mechanisms scored highly at 90%, demonstrating that many contracts provide effective methods for consumers to refuse or withdraw consent. This is weighted at 15%, as the ability to opt out is essential for consumer control over their data. Finally, Consumer Awareness and Education scored the lowest at 70%, weighted at 10%. This highlights the need for better communication and education efforts to help consumers understand the implications of biometric data collection and their rights

regarding it. The evaluation of biometric contracts based on data security and ownership focuses on critical areas such as encryption, ownership clarity, and breach response, all vital for protecting sensitive biometric data. The Data Encryption Standards scored 88%, with a significant weight of 35%, reflecting the priority given to securing biometric data. Strong encryption is essential to preventing unauthorized access and ensuring data remains safe, especially given the sensitive nature of biometric information.

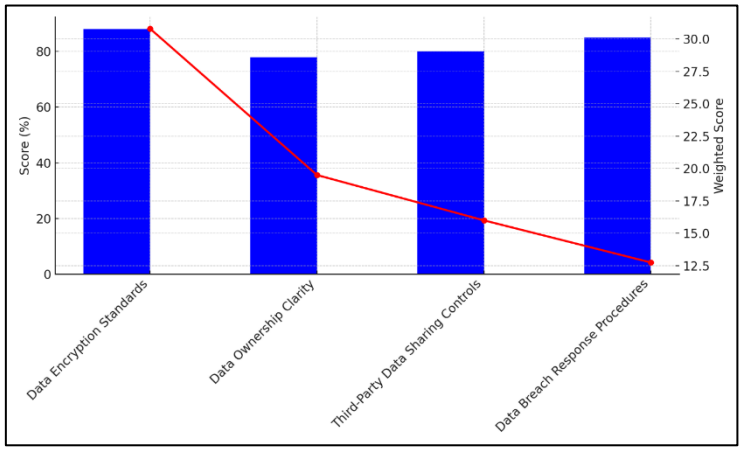

Figure 6: Data Security Standards and Breach Response Performance

Data Ownership Clarity, scoring 78% and weighted at 25%, highlights that while most contracts define who owns the biometric data, there is still some ambiguity. Clear definitions of ownership are necessary to ensure consumers maintain control over their biometric information and understand how it can be used by service providers. Third-Party Data Sharing Controls scored 80%, with a 20% weight, indicating a generally strong performance in regulating how biometric data is shared with third parties. This is crucial for ensuring that third-party vendors comply with the same privacy and security standards as the original collectors of the data. Finally, Data Breach Response Procedures scored 85%, with a 15% weight. This shows that while most biometric contracts have plans in place for responding to breaches, there is still room for improvement, particularly in providing timely notifications to affected consumers.

VIII. Conclusion

Biometric technologies offer significant advancements in security and user convenience, but their integration into consumer services introduces complex legal considerations. Biometric contracts emerge as a vital tool for addressing these challenges, ensuring that both consumers' rights and technological advancements are adequately managed. The existing legal frameworks, such as the General Data Protection Regulation (GDPR) and the Biometric Information Privacy Act (BIPA), provide essential guidelines but often fall short in addressing the full scope of biometric data management. These regulations emphasize the importance of consent, privacy, and data protection but need further refinement to keep pace with technological innovations. Biometric contracts must be meticulously crafted to cover specific aspects of biometric data handling, including obtaining informed consent, defining data ownership, and establishing robust data protection measures. These contracts should ensure that individuals are fully aware of how their biometric data is collected, used, and protected. Moreover, they should provide clear mechanisms for individuals to access, correct, and delete their data, thereby reinforcing consumer rights. As biometric technologies evolve, so too must biometric contracts. Future contracts will need to address new types of biometric data and adapt to emerging privacy and security standards. This necessitates ongoing updates to contractual terms and the development of new legal frameworks that address the unique challenges posed by advanced biometric systems. Additionally, international cooperation is crucial to harmonize biometric regulations across jurisdictions, ensuring consistent protection for consumers worldwide. Policymakers and legal experts must work together to develop adaptive legal strategies that balance innovation with robust privacy protections.

References

[1] Rathee, G.; Kerrache, C.A.; Ferrag, M.A. A Blockchain-Based Intrusion Detection System Using Viterbi Algorithm and Indirect Trust for IIoT Systems. J. Sens. Actuator Netw. 2022, 11, 71.

[2] Rathee, G.; Ahmad, F.; Sandhu, R.; Kerrache, C.A.; Azad, M.A. On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. Inf. Process. Manag. 2021, 58, 102526.

[3] McGhin, T.; Choo, K.K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. J. Netw. Comput. Appl. 2019, 135, 62–75.

[4] Barka, E.; Dahmane, S.; Kerrache, C.A.; Khayat, M.; Sallabi, F. STHM: A Secured and Trusted Healthcare Monitoring Architecture Using SDN and Blockchain. Electronics 2021, 10, 1787.

[5] Antwi, M.; Adnane, A.; Ahmad, F.; Hussain, R.; Habib ur Rehman, M.; Kerrache, C.A. The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain Res. Appl. 2021, 2, 100012.

[6] Shi, S.; He, D.; Li, L.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Comput. Secur. 2020, 97, 101966.

[7] Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J. Inf. Secur. Appl. 2020, 50, 102407.

[8] Fatima, N.; Agarwal, P.; Sohail, S.S. Security and Privacy Issues of Blockchain Technology in Health Care—A Review. In ICT Analysis and Applications; Springer: Singapore, 2022; pp. 193–201.

[9] Luo, J.; Hu, F.; Wang, R. 3D face recognition based on deep learning. In Proceedings of the 2019 IEEE International Conference on Mechatronics and Automation (ICMA), Tianjin, China, 4–7 August 2019; pp. 1576–1581.

[10] 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.

[11] Li, Y.; Huang, X.; Zhao, G. Joint Local and Global Information Learning With Single Apex Frame Detection for Micro-Expression Recognition. IEEE Trans. Image Process. 2021, 30, 249–263.

[12] Yao, L.; Xiao, X.; Cao, R.; Chen, F.; Chen, T. Three stream 3D CNN with SE block for micro-expression recognition. In Proceedings of the 2020 International Conference on Computer Engineering and Application (ICCEA), Guangzhou, China, 27–29 March 2020; pp. 439–443.