Biometric Technology Today
ISSN (online): 1873-1880

Biometric Data and Privacy Laws: Navigating Global Regulations

Megha Sanket Kulkarni[1], Yogesh Dharangutti[2], Kanchan Rahul Jamnik[3], Preeti Sharma[4], Devika A. Verma[5], Dr. Uday Chandrakant Patkar[6]

[1]Sandip University Nashik, Nashik, Maharashtra, India. megha.Kulkarni@sandipuniversity.edu.in

[2]Symbiosis Law School (SLS) Symbiosis International (Deemed University) (SIU) Vimannagar, Pune, Maharashtra, India. yogesh.d@symlaw.ac.in

[3]Sandip Institute of Engineering & Management, Nashik, Maharashtra, India. kanchan.jamnik@siem.org.in

[4]Sandip University Nashik, Nashik, Maharashtra, India. preeti.sharma@sandipuniversity.edu.in

[5]Vishwakarma Institute of Technology, Pune, Maharashtra, India. devika.verma@viit.ac.in

[6]Bharati Vidyapeeth's College of Engineering Lavale, Pune, Maharashtra, India. uday.patkar@bharatividyapeeth.edu

Abstract: Biometric data, including fingerprints, facial recognition, and iris scans, is increasingly integrated into various industries, offering convenience and security benefits. However, its collection, storage, and usage raise significant privacy concerns, prompting global efforts to regulate its protection. This paper explores the complex landscape of privacy laws governing biometric data, focusing on key regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Biometric Information Privacy Act (BIPA) in the United States. Additionally, it examines regulations across Asia, Latin America, and other regions, highlighting challenges in achieving regulatory harmony amidst diverse legal frameworks. The paper addresses the implications of non-compliance, including litigation risks, and considers emerging trends in the evolving biometric privacy regulatory environment. Through a comparative analysis, this research underscores the critical need for cohesive global standards and technological advancements to protect biometric data and ensure ethical usage. Recommendations for organizations and policymakers are also provided.

Keywords: Biometric Data, Privacy Laws, GDPR, BIPA, Regulatory Compliance.

Introduction

Biometric data, comprising unique identifiers such as fingerprints, facial recognition, and retina scans, has become an integral part of modern technology. These identifiers are increasingly used to authenticate individuals and provide secure access across various industries. From healthcare systems that use biometric information to ensure patient safety and prevent fraud, to financial institutions and security sectors relying on biometric authentication to safeguard sensitive data, the utility of this technology is widespread. The accuracy and convenience of biometrics have made them a preferred method over traditional forms of identification, such as passwords or cards[1], [2].

However, the rise in the use of biometric technologies has brought significant concerns regarding privacy. Unlike passwords, biometric traits cannot be altered if compromised, which increases the risk of misuse and breaches. Ethical concerns emerge as these technologies, if mismanaged, can lead to surveillance overreach, data exploitation, and the violation of individuals' rights to privacy. These challenges have triggered debates about how biometric data should be managed, stored, and protected, especially given its sensitive nature. Privacy laws are crucial in this context, establishing boundaries on the collection and use of biometric data to prevent misuse. Regulations such as the GDPR and the BIPA aim to safeguard individuals by enforcing stringent rules on the processing and handling of biometric information[3].

This research paper aims to explore the global landscape of privacy regulations governing biometric data, analyzing differences between regions and the complexities involved in compliance. The objective is to offer

insights into how regulations across various jurisdictions address these challenges and to assess the extent to which they protect individuals. By navigating these regulatory frameworks, this research highlights the ongoing efforts and obstacles to achieving a unified approach to biometric data protection.

Biometric Data: Definition and Use Cases

Biometric data refers to the unique, measurable characteristics of individuals that can be used for identification and authentication purposes. These characteristics are broadly classified into two categories: physical and behavioral biometrics. Physical biometrics include inherent traits such as fingerprints, facial recognition, iris and retina scans, and DNA. These are static, measurable features that are difficult to alter and are frequently used for identity verification. Behavioral biometrics, on the other hand, refer to patterns in human activities, such as voice recognition, typing rhythm, gait analysis, and even signature patterns, which can also be utilized to verify identity[4].

Biometric data has found widespread use in a variety of sectors. In security, biometrics are employed for border control, surveillance, and law enforcement to track and identify individuals. For instance, biometric databases help governments monitor security threats by quickly identifying persons of interest. In commercial applications, biometrics are widely used in consumer electronics like mobile phones and computers for unlocking devices or verifying customer identities during financial transactions. Many businesses also leverage biometric systems to enhance user experience by simplifying authentication processes. Healthcare is another significant domain where biometric technologies are used for medical identification, helping to ensure patient data security and streamline healthcare delivery by reducing the likelihood of identity fraud and errors in patient records[5].

However, despite its numerous benefits, the use of biometric data presents certain risks and vulnerabilities. A primary concern is the potential for data breaches, where sensitive biometric information could be exposed or misused. Unlike passwords, biometric traits cannot be changed once compromised, leading to long-term risks. Furthermore, the misuse of biometric data can result in privacy violations, unauthorized surveillance, or identity theft, raising ethical and security concerns. Consequently, safeguarding this data has become crucial as its applications continue to expand across industries.

Global Privacy Laws on Biometric Data

Biometric data, given its sensitive and unique nature, is governed by a variety of privacy laws across different regions of the world. The regulatory landscape is fragmented, with countries adopting distinct approaches to protect biometric information, ensuring both individuals' privacy and the responsible use of biometric technologies. Key regulations, such as the GDPR in the European Union, BIPA in Illinois, and various laws across Asia, shape the way biometric data is handled, particularly concerning consent, processing, and individual rights. Below table-1 is a summary of the global legal frameworks addressing biometric data[6]–[10]:

Table 1 Various global legal frameworks summary

Region	Regulation	Key Provisions	Individual Rights	Consent Requirements
European Union	GDPR	Biometric data as sensitive data, requires protection.	Right to access, correct, and delete data.	Explicit consent required for processing.
United States (IL)	BIPA	Requires informed consent before data collection.	Right to know usage and security obligations.	Written consent mandatory.
United States (CA)	California Consumer Privacy Act	Extends consumer rights to biometric data.	Right to delete and opt-out of data sale.	Implied consent, with opt-out options.
Japan	Act on the Protection of	Strict rules on biometric data	Right to data security and protection.	Consent required for collection and transfer.

	Personal Information	processing and transfer.		
India	Aadhaar Act	Governs biometric collection for identification.	Limited rights to opt out and data privacy concerns.	Mandatory consent for Aadhaar use.
China	China's Personal Information Protection Law	Strict governance of biometric data use.	Right to informed use and secure storage.	Informed consent required for specific purposes.

Emerging trends in biometric data privacy regulation show a move towards stricter controls and more comprehensive data protection frameworks worldwide. While regions like the European Union have set high standards through GDPR, other jurisdictions are catching up. In the U.S., the lack of federal regulation has prompted states like Illinois and California to take independent action. Meanwhile, countries in Asia, particularly China and Japan, are implementing tighter rules to address growing concerns over biometric data misuse and surveillance.

There is also a trend towards harmonization of global standards, with cross-border data flows becoming more common. However, differences in enforcement and scope of regulations remain a significant challenge. As biometric technologies evolve, it is expected that governments will introduce updated privacy laws to address new risks associated with biometric identification and AI-driven biometric systems.

Challenges in Harmonizing Global Biometric Privacy Laws

The global landscape of biometric privacy laws presents significant challenges due to the divergence in regulatory approaches across different jurisdictions. Various countries have different definitions and requirements for handling biometric data. For instance, what constitutes "biometric data" and how it is categorized (e.g., sensitive vs. non-sensitive) varies widely. This makes it difficult to create a uniform standard for compliance, especially as some regions, such as the European Union under GDPR, require explicit consent, while others have more lenient rules[11].

Balancing innovation and privacy remains another challenge. The rapid development of biometric technologies, like facial recognition and DNA sequencing, brings both security advancements and privacy risks. Laws must strike a balance between enabling technological innovation and ensuring individual privacy, a complex task given the fast pace of biometric technology adoption across sectors like healthcare and security.

Cross-border data transfer further complicates compliance, as multinational companies face difficulties adhering to local regulations in each country they operate in. This challenge is exacerbated by differing standards for securing biometric data and obtaining user consent, making it hard to establish a cohesive data handling approach.

Finally, data minimization and purpose limitation are areas where regulations diverge. Some laws, like GDPR, mandate that organizations only collect biometric data necessary for a specific purpose, whereas other regions lack stringent rules in this regard. This creates inconsistencies in how biometric data is collected, stored, and processed, resulting in challenges for companies operating across multiple jurisdictions to comply with varying legal expectations.

Legal Implications of Non-Compliance

Non-compliance with biometric data regulations can result in significant legal and financial consequences. Under laws like the GDPR and BIPA, violations attract severe fines and penalties. For instance, the GDPR can impose fines of up to 4% of a company's global annual revenue, while BIPA allows for substantial penalties for each instance of unauthorized data collection. These strict regulations have prompted numerous litigation risks, including high-profile class-action lawsuits. The rise in biometric privacy-related litigation reflects the growing public concern over data privacy and security[6], [12]. Companies that fail to comply face not only financial

penalties but also reputational damage, leading to changes in corporate policies. Many businesses have been forced to reassess their approach to biometric technology adoption to mitigate legal risks, ensuring compliance with stringent privacy laws to avoid costly legal battles and settlements. Following table-2 are the major case Studies of Notable Legal Actions:

Table 2 Summary of major notable legal actions

Case	Law Violated	Settlement/Outcome	Key Takeaway
Facebook (BIPA)	BIPA (Illinois)	$650 million settlement in class-action.	Highlighted the risks of non-consensual biometric data collection.
Clearview AI (BIPA)	BIPA (Illinois)	Ongoing litigation.	Legal challenges over scraping facial recognition data.
Google (BIPA)	BIPA (Illinois)	$100 million settlement.	Reinforced the need for clear, informed consent in biometric data use.
TikTok (BIPA)	BIPA (Illinois)	$92 million settlement.	Addressed unauthorized use of biometric identifiers in app features.

The legal implications of non-compliance with biometric data regulations are significant and far-reaching. Companies face not only steep fines and penalties under laws such as GDPR and BIPA, but also the risk of costly litigation and class-action lawsuits[13], [14]. These legal challenges can lead to financial losses and reputational damage, prompting organizations to reassess their data handling practices. The growing number of cases highlights the increasing scrutiny over biometric data usage and the need for businesses to prioritize compliance. As biometric technologies continue to evolve, adherence to privacy regulations will remain critical for safeguarding individual rights and maintaining public trust in these systems.

Future Trends in Biometric Privacy Laws

As biometric technologies evolve, emerging technologies such as AI-driven biometrics and deep learning models are raising new privacy challenges. These advanced systems, which include facial recognition and behavioral analytics, increase the risk of data misuse and surveillance, leading to growing concerns over individual privacy rights. As these technologies become more widespread, regulatory frameworks are expected to evolve, focusing on stronger protections and stricter requirements for transparency, consent, and data security. Governments will need to keep pace with these developments to ensure that laws adequately address the complexities introduced by these advanced biometric systems[15].

Efforts are already underway to harmonize global regulations and create consistent international standards. Organizations like the United Nations, the World Economic Forum, and ISO are playing a pivotal role in pushing for a more unified regulatory approach to biometric data privacy. This will help address the challenges posed by cross-border data flows and the increasing use of biometrics in global markets.

Technological solutions are also emerging to enhance privacy compliance. Privacy-enhancing technologies (PETs), such as encryption, anonymization, and federated learning, are being developed to securely handle biometric data while minimizing privacy risks. These solutions can allow companies to use biometric data for authentication and other purposes without directly exposing sensitive information, helping to safeguard individual rights in an increasingly data-driven world. With these advancements, biometric privacy regulations are expected to become more sophisticated, ensuring that both innovation and privacy are protected.

Conclusion and Recommendations

The global regulatory landscape surrounding biometric data is complex and varied, with laws such as the GDPR in Europe and BIPA in Illinois setting high standards for privacy protection. These regulations underscore the critical importance of protecting biometric data due to its unique and sensitive nature. However, the divergence in legal frameworks across different regions poses significant compliance challenges, particularly for multinational organizations. The implications of non-compliance, including substantial fines and legal risks, highlight the need for robust regulatory adherence.

Importance of Privacy Laws in Protecting Biometric Data

Privacy laws play a crucial role in safeguarding individual rights by setting clear guidelines on the collection, use, and storage of biometric data. As biometric technologies continue to advance, these regulations are vital in preventing misuse and ensuring that individuals retain control over their personal information. The importance of these laws is magnified by the irreversible nature of biometric data breaches, as compromised biometric identifiers cannot be changed like passwords.

Call for Ongoing Research and Policy Development

Given the rapid evolution of biometric technologies, there is a pressing need for continuous research and policy development to address emerging privacy risks. Governments and regulatory bodies must remain vigilant, adapting laws to keep pace with technological advancements. Ongoing research is also needed to develop privacy-enhancing technologies that can ensure compliance while maintaining the integrity of biometric systems.

Best Practices for Organizations Handling Biometric Data

Organizations must adopt best practices to ensure compliance with biometric privacy laws:

- Transparency: Clearly communicate the purpose and scope of biometric data collection to individuals.
- Consent Mechanisms: Obtain explicit consent before collecting biometric information.
- Secure Data Storage: Implement strong security measures to protect biometric data from breaches.
- Privacy by Design and Default: Incorporate privacy considerations at the initial design stages of systems handling biometric data.

Policy Recommendations

- Global Regulatory Cooperation: Encourage international collaboration to harmonize biometric privacy laws, facilitating easier compliance for global companies.
- Consistent and Clear Standards: Advocate for the development of unified global standards to address the complexities of biometric data use and ensure uniform protection across regions.

By adopting these measures, organizations and policymakers can create a more secure and privacy-conscious environment for the use of biometric technologies.

References

[1] S. Tanwar, S. Tyagi, N. Kumar, and M. S. Obaidat, “Ethical, Legal, and Social Implications of Biometric Technologies BT - Biometric-Based Physical and Cybersecurity Systems,” M. S. Obaidat, I. Traore, and I. Woungang, Eds. Cham: Springer International Publishing, 2019, pp. 535–569.

[2] M. Smith and S. Miller, “The ethical application of biometric facial recognition technology,” *AI Soc.*, vol. 37, no. 1, pp. 167–175, 2022, doi: 10.1007/s00146-021-01199-9.

[3] M. Phillips, “International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR),” *Hum. Genet.*, vol. 137, no. 8, pp. 575–582, 2018, doi: 10.1007/s00439-018-1919-7.

[4] A. Beduschi, “Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights,” *Big Data Soc.*, vol. 6, no. 2, p. 2053951719855091, Jun. 2019, doi: 10.1177/2053951719855091.

[5] X. Wang, Y. C. Wu, M. Zhou, and H. Fu, “Beyond surveillance: privacy, ethics, and regulations in face

recognition technology," *Front. Big Data*, vol. 7, 2024, doi: 10.3389/fdata.2024.1337465.

[6] S. Chatterjee, "Is data privacy a fundamental right in India?," *Int. J. Law Manag.*, vol. 61, no. 1, pp. 170–190, Jan. 2019, doi: 10.1108/IJLMA-01-2018-0013.

[7] C. J. Bennett, "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?," *Inf. Polity*, vol. 23, no. 2, pp. 239–246, 2018, doi: 10.3233/IP-180002.

[8] I. Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)," *Smart Cities*, vol. 5, no. 3. pp. 1129–1150, 2022, doi: 10.3390/smartcities5030057.

[9] P. Singh, "Aadhaar and data privacy: biometric identification and anxieties of recognition in India," *Information, Commun. Soc.*, vol. 24, no. 7, pp. 978–993, May 2021, doi: 10.1080/1369118X.2019.1668459.

[10] N. Gruschka, V. Mavroeidis, K. Vishi, and M. Jensen, "Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 5027–5033, doi: 10.1109/BigData.2018.8622621.

[11] A. Ioannou, I. Tussyadiah, and Y. Lu, "Privacy concerns and disclosure of biometric and behavioral data for travel," *Int. J. Inf. Manage.*, vol. 54, p. 102122, 2020, doi: https://doi.org/10.1016/j.ijinfomgt.2020.102122.

[12] E. J. Kindt, "Having yes, using no? About the new legal regime for biometric data," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 523–538, 2018, doi: https://doi.org/10.1016/j.clsr.2017.11.004.

[13] B. Meden *et al.*, "Privacy–Enhancing Face Biometrics: A Comprehensive Survey," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 4147–4183, 2021, doi: 10.1109/TIFS.2021.3096024.

[14] K. Michael, S. Kobran, R. Abbas, and S. Hamdoun, "Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals," in *2019 IEEE International Symposium on Technology and Society (ISTAS)*, 2019, pp. 1–13, doi: 10.1109/ISTAS48451.2019.8937956.

[15] P. Arora, "General data protection regulation—a global standard? Privacy futures, digital activism, and surveillance cultures in the global south," *Surveill. Soc.*, vol. 17, no. 5, pp. 717–725, 2019, doi: 10.24908/ss.v17i5.13307.