Biometric Technology Today
ISSN (online): 1873-1880

Cross-Border Sharing of Biometric Data: Legal Complexities and Agreements

Dr. Yogita D. Bhise[1], Dr. Sourabh Sharma[2], Dr. Sukhvinder Singh Dari[3], Dr Amena Ansari[4], Dr. Omkaresh Kulkarn[5], Dr. Vilas S. Gaikwad[6]

[1]Assistant Professor, Computer Engineering, K. K. Wagh Institute of Engineering Education and Research, Nashik (MH). ydbhise@kkwagh.edu.in

[2]Independent Researcher, Jiwaji University, Gwalior, India. sourabhsharma08051980@gmail.com

[3]Professor, Symbiosis Law School, Nagpur Campus, Symbiosis International (Deemed University), Pune, India, Email Id-sukhvinder.dari@gmail.com.

[4]Asst Professor, Department of Civil Engineering ,Deogiri Institute of Engineering and Management Studies, Deogiri Campus, Railway Station Road, Aurangabad, Maharashtra 431005 amenatamboli2011@gmail.com

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

[6]Associate Professor and HOD, Department of Information TechnologyTrinity College of Engineering and Research Punevilasgaikwad11@gmail.com

Abstract: Cross-border sharing of biometric data presents a complex legal landscape characterized by diverse regulations, international agreements, and ethical considerations. As global connectivity increases, the exchange of biometric information—such as fingerprints, facial recognition data, and iris scans—across national boundaries has become a critical issue in fields ranging from law enforcement to immigration and cybersecurity. This abstract examines the legal complexities and frameworks governing the international transfer of biometric data, highlighting the challenges and potential solutions for achieving harmonized global practices. Biometric data, due to its sensitive and personal nature, is subject to stringent data protection laws in many jurisdictions. In the European Union, for example, the General Data Protection Regulation (GDPR) imposes rigorous restrictions on the processing and transfer of personal data, including biometric information. Similarly, other regions such as the United States and Asia have their own regulatory frameworks that vary significantly in terms of scope and enforcement. The lack of uniformity in data protection standards poses a significant challenge for international cooperation, as organizations must navigate a patchwork of legal requirements to ensure compliance. International agreements and treaties, such as the Convention on Cybercrime and various bilateral agreements, seek to address these challenges by providing frameworks for cooperation and mutual legal assistance. However, these agreements often fall short of addressing the specific nuances of biometric data transfer and the evolving nature of technology. The need for a comprehensive and standardized approach to cross-border biometric data sharing is evident, yet achieving such consensus remains elusive. In addition to legal and regulatory challenges, ethical considerations play a crucial role in the discourse on biometric data sharing. The potential for misuse or abuse of biometric data raises concerns about privacy, security, and human rights. Effective governance frameworks must therefore balance the benefits of cross-border cooperation with the need to protect individual rights and prevent discriminatory practices. This paper explores the current state of legal frameworks and international agreements related to cross-border biometric data sharing. It analyzes the implications of existing regulations, identifies gaps and inconsistencies, and proposes recommendations for creating a more coherent and secure system for international data exchange.

Keywords: Biometric Data, Data Protection Laws, International Agreements, Privacy and Security, Legal Compliance

I. Introduction

In an era of rapid globalization and technological advancement, the cross-border sharing of biometric data has emerged as a critical issue in the realm of international law and data protection. Biometric data, which includes unique identifiers such as fingerprints, facial recognition patterns, and iris scans, offers a level of precision in identification and security that is unmatched by traditional methods. However, the international exchange of such sensitive information introduces a complex web of legal and ethical challenges that must be carefully navigated to ensure both security and privacy. Biometric data is increasingly utilized across various sectors including law enforcement, immigration, and financial services. For instance, law enforcement agencies use biometric data to track and identify individuals across borders, while immigration authorities employ biometric systems to streamline border control processes and enhance security. In the financial sector, biometric authentication provides an added layer of security for transactions and personal accounts [1]. The growing use of biometric data highlights its value but also underscores the need for robust legal frameworks to regulate its cross-border transfer. The legal landscape governing the international sharing of biometric data is marked by significant variability. Different countries and regions have adopted diverse regulatory approaches, reflecting their respective concerns and priorities regarding data privacy and protection. For example, the European Union's General Data Protection Regulation (GDPR) imposes stringent rules on the processing and transfer of personal data, including biometric information. GDPR mandates that biometric data must be handled with a high level of protection and sets out specific conditions for transferring such data outside the EU. In contrast, jurisdictions like the United States have a more fragmented approach to data protection, with a mix of federal and state regulations that do not always align with international standards. This divergence in regulatory frameworks creates challenges for organizations engaged in cross-border biometric data transfers [2]. Companies and government agencies must navigate a complex array of legal requirements to ensure compliance, which can be both costly and time-consuming. Moreover, the absence of a global standard for biometric data protection exacerbates these challenges, making it difficult to establish a cohesive approach to international data sharing. International agreements and treaties have been established to address some of these challenges.

For instance, the Convention on Cybercrime, also known as the Budapest Convention, provides a framework for international cooperation in combating cybercrime and includes provisions for the exchange of electronic evidence. However, these agreements often fall short in addressing the specific nuances of biometric data and may not fully account for the rapid evolution of technology. As biometric systems and data processing techniques continue to advance, existing agreements may become outdated, necessitating ongoing updates and revisions to ensure their relevance. Ethical considerations also play a crucial role in the discourse on cross-border biometric data sharing [3]. The use of biometric data raises concerns about privacy and the potential for misuse or abuse. For instance, the deployment of facial recognition technology by government agencies or private entities can lead to surveillance practices that infringe on individual rights and freedoms. Furthermore, the storage and handling of biometric data pose risks related to data breaches and unauthorized access. Effective governance frameworks must address these ethical concerns by implementing safeguards that protect individuals' rights and ensure responsible use of biometric information. As the global community continues to grapple with these issues, it is imperative to develop comprehensive and harmonized approaches to the cross-border sharing of biometric data. This requires a concerted effort to align international regulations, enhance transparency, and promote best practices in data protection [4]. By addressing the legal complexities and ethical challenges associated with biometric data, stakeholders can work towards creating a secure and equitable framework for international data exchange. The need for such a framework is underscored by the increasing reliance on biometric technology and the potential implications for privacy, security, and human rights.

II. Related Work

The discussion on cross-border sharing of biometric data has attracted considerable attention from legal scholars, policymakers, and industry experts. Several key studies and reports have examined the complexities associated with international data transfers and the legal frameworks governing such exchanges. One prominent body of work focuses on the regulatory landscape and its impact on cross-border biometric data sharing. Research provides a comprehensive analysis of the General Data Protection Regulation (GDPR) and its implications for biometric data transfer [5]. This work highlights the stringent requirements imposed by the GDPR, including the necessity for adequate protection levels and specific conditions for data transfers outside the EU. It underscores the

challenges faced by organizations operating internationally, particularly those dealing with biometric data, and suggests that harmonizing data protection standards could alleviate some of these difficulties. Additionally, studies explore the intersection of privacy law and technology in the context of biometric data. They emphasize the need for a balanced approach that addresses both security and privacy concerns.

Advocates for international agreements that align with global data protection norms while considering the diverse legal traditions of different countries. These findings highlight the importance of developing frameworks that not only safeguard individual rights but also facilitate effective international cooperation. The role of international treaties in addressing cross-border data sharing has also been a focus of scholarly attention. Analysis of instruments like the Convention on Cybercrime reveals that while such treaties offer a foundation for cooperation, they often fall short of addressing the specific nuances of biometric data and evolving technological advancements [6]. Industry reports provide practical perspectives on the challenges and solutions for cross-border biometric data sharing. These reports frequently discuss case studies and best practices, offering valuable insights into how organizations can navigate the complex legal environment. Reports on global data privacy trends highlight the growing need for consistency in data protection regulations and offer recommendations for aligning practices across borders to ensure secure and compliant data transfers.

III. Overview of Biometric Data

A. Definition and Types of Biometric Data

Biometric data refers to unique physiological or behavioral characteristics used to identify and authenticate individuals. These characteristics are inherently personal and are typically stable over time, making them highly reliable for security and identification purposes. The primary types of biometric data include physiological biometrics and behavioral biometrics. Physiological biometrics involve physical traits such as fingerprints, facial recognition, iris patterns, and DNA. Fingerprints are one of the most established forms of biometric identification, leveraging the unique ridges and patterns found on an individual's fingertips. Facial recognition technology uses the geometric features of the face, such as the distance between the eyes and the shape of the jawline, to identify individuals. Iris recognition analyzes the unique patterns in the colored part of the eye, which remains stable over a person's lifetime. DNA biometrics, though less common due to its complexity and privacy concerns, involves analyzing genetic material for identification purposes [10]. Behavioral biometrics, on the other hand, involve patterns of behavior such as voice recognition, keystroke dynamics, and gait analysis. Voice recognition systems analyze the unique vocal attributes of a person, including pitch and tone, while keystroke dynamics measure typing patterns, such as typing speed and rhythm. Gait analysis involves studying the way a person walks, which can be distinctive enough to serve as a biometric identifier. These types of biometric data offer various levels of security and convenience, often being used in combination to enhance accuracy and reliability. The choice of biometric modality depends on the application and the required level of security, as well as considerations of user convenience and privacy.

B. Applications of Biometric Data in Security, Healthcare, and Governance

Biometric data has found widespread application across several critical sectors, including security, healthcare, and governance. In security, biometric systems are employed for access control and authentication. They are used in both physical security, such as entry into buildings, and digital security, such as logging into computers and mobile devices. The ability of biometric data to provide accurate and non-repudiable authentication makes it a valuable tool in protecting sensitive information and assets. In healthcare, biometric data is increasingly used for patient identification and management [11]. Hospitals and clinics use biometric systems to accurately match patients with their medical records, reducing errors and enhancing patient safety. For example, fingerprint and iris recognition can ensure that the correct patient receives the appropriate treatment or medication.

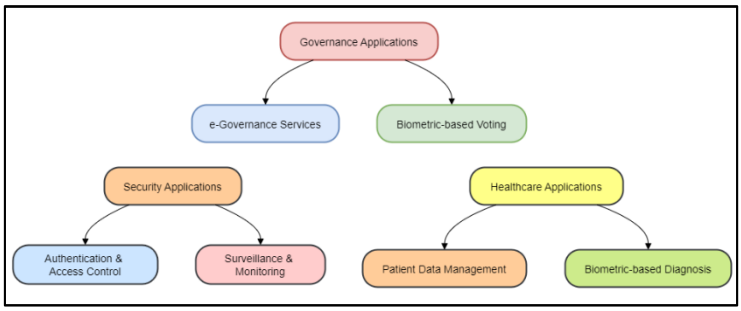

Figure 1: Applications of Biometric Data in Security, Healthcare, and Governance

Additionally, biometric data is used in telemedicine and remote health monitoring, enabling secure and personalized interactions between patients and healthcare providers. In the realm of governance, biometric data plays a significant role in improving public services and enhancing security. Governments use biometric systems for various purposes, including voter identification, passport control, and border security. Biometric identifiers help streamline administrative processes, prevent fraud, and ensure the integrity of public services. For instance, biometric passports contain embedded data that can be quickly verified, facilitating smoother and more secure international travel [12]. These applications highlight the versatility and importance of biometric data across different domains, offering solutions that enhance security, improve efficiency, and support accurate identification.

C. Rise of Biometric Technologies in a Global Context

The rise of biometric technologies has been driven by advancements in technology, increased global connectivity, and growing concerns about security and privacy. As biometric systems become more sophisticated and accessible, their adoption has expanded beyond traditional security applications into various other domains. Globally, the adoption of biometric technologies has been influenced by the increasing need for secure and efficient identity verification methods. For example, countries around the world are implementing biometric systems for national identification programs, enhancing border control, and improving public safety. In many developing countries, biometric technologies are being used to provide secure access to services and benefits, such as financial inclusion and healthcare. The proliferation of smartphones and other digital devices equipped with biometric sensors has further accelerated the adoption of these technologies [13]. Facial recognition and fingerprint scanners are now common features in consumer electronics, enabling convenient and secure user authentication. This widespread use of biometric technologies has raised awareness and acceptance among the general public. However, the global rise of biometric technologies also brings challenges related to privacy, data protection, and ethical considerations. The collection and storage of biometric data raise concerns about potential misuse and unauthorized access. As biometric systems become more pervasive, there is a growing need for international standards and regulations to address these concerns and ensure the responsible use of biometric data.

IV. Legal Frameworks Governing Biometric Data

A. International Laws and Regulations

International laws and regulations surrounding biometric data aim to establish guidelines and standards for its collection, use, and transfer across borders. One of the most significant international frameworks is the General Data Protection Regulation (GDPR) adopted by the European Union. The GDPR sets stringent rules for the processing of personal data, including biometric data, requiring that organizations implement robust safeguards to protect this sensitive information. It stipulates that biometric data can only be processed under specific conditions, such as obtaining explicit consent from individuals or if necessary for legal obligations or vital interests. Additionally, the GDPR mandates that data transferred outside the EU must meet certain adequacy standards to ensure equivalent levels of protection. Another important international framework is the Convention on Cybercrime, also known as the Budapest Convention [14]. This treaty, adopted by the Council of Europe, facilitates international cooperation in the investigation and prosecution of cybercrime, including the misuse of biometric data. The Convention provides mechanisms for mutual assistance among member states and establishes procedures for the exchange of information and evidence. However, its focus is broader than just biometric data

and does not specifically address all the nuances related to biometric privacy and protection. The Asia-Pacific Economic Cooperation (APEC) has also contributed to international efforts with its Privacy Framework and Cross-Border Privacy Rules (CBPR) System, which aim to promote data protection and privacy in the region [15]. The CBPR System allows businesses to demonstrate their commitment to data protection through certification, facilitating cross-border data flows while ensuring adequate protection measures are in place.

B. Regional and National Laws

Regional and national laws governing biometric data vary widely, reflecting differing priorities and levels of protection across jurisdictions. In the United States, biometric data is regulated by a patchwork of state laws, such as the Illinois Biometric Information Privacy Act (BIPA), which imposes strict requirements on the collection, storage, and usage of biometric data, including obtaining informed consent and implementing security measures. Other states have enacted similar laws, but there is no comprehensive federal legislation specifically addressing biometric data. In contrast, countries within the European Union are governed by the GDPR, which provides a unified regulatory framework for biometric data protection. GDPR's emphasis on data subject rights, such as the right to access and erase data, and its requirements for transparency and accountability have set a high standard for data protection globally. In China, the regulatory landscape includes the Personal Information Protection Law (PIPL) and the Cybersecurity Law, which impose stringent requirements on the collection and processing of personal data, including biometric information [16]. These laws emphasize the importance of obtaining consent and ensuring data security, reflecting China's growing focus on data protection.

C. Role of International Organizations

International organizations play a crucial role in shaping the global approach to biometric data governance and facilitating cooperation among nations. Organizations such as Interpol and the United Nations contribute to establishing standards, promoting best practices, and fostering collaboration in the realm of biometric data. Interpol, the International Criminal Police Organization, is instrumental in enhancing global law enforcement cooperation. Its involvement in biometric data primarily focuses on supporting the use of biometrics for criminal investigations and border security. Interpol facilitates the sharing of biometric data among member countries to aid in identifying criminals and preventing crime. It provides a secure platform for the exchange of biometric information, such as fingerprints and facial recognition data, which is crucial for cross-border criminal investigations. Interpol's efforts are aimed at improving the accuracy and efficiency of law enforcement operations while ensuring that member countries adhere to agreed-upon standards for data protection and privacy. The United Nations (UN), through various agencies and initiatives, also addresses the challenges associated with biometric data. The UN's efforts are often centered around promoting human rights and ensuring that biometric data practices do not infringe upon individual freedoms. For example, the UN Office of the High Commissioner for Human Rights (OHCHR) works to ensure that the use of biometric data in areas such as migration and refugee management respects international human rights standards. The UN has also initiated discussions on the ethical and legal implications of biometric technologies, aiming to provide guidance on balancing technological advancements with privacy rights. In addition to these organizations, the International Organization for Standardization (ISO) plays a significant role in developing global standards for biometric data.

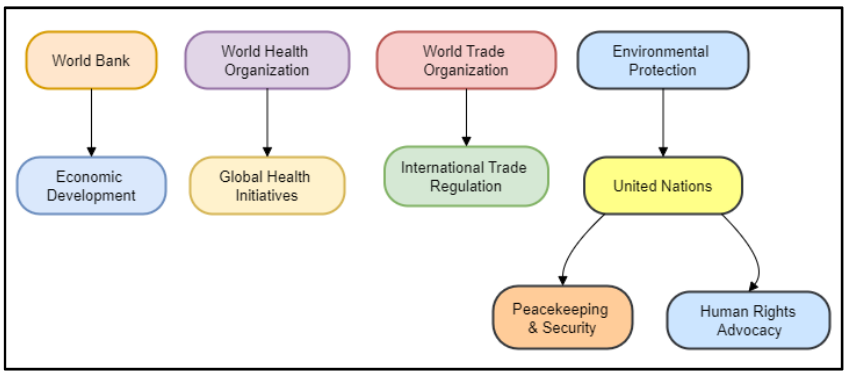

Figure 2: Illustrating Role of International Organizations

ISO's work includes creating standards for biometric performance, data quality, and interoperability, which help ensure that biometric systems are reliable and secure across different regions and applications. By establishing these standards, ISO helps promote consistency and reliability in biometric data usage worldwide.

V. Case Studies of Cross-Border Biometric Data Sharing

A. Case Study: U.S.-EU Data Transfer and Privacy Concerns

The transfer of biometric data between the United States and the European Union has been a focal point in discussions about international data privacy and security. The U.S.-EU data transfer framework is primarily governed by agreements such as the Privacy Shield Framework and its predecessor, the Safe Harbor Agreement. These frameworks were designed to facilitate data exchanges while ensuring adequate protection of personal information. The Privacy Shield Framework, established in 2016, aimed to address concerns about U.S. data protection practices, which were deemed insufficient by EU standards. It included provisions for stronger data protection safeguards, such as enhanced transparency and accountability measures for U.S. companies handling EU data. However, the framework faced significant scrutiny, particularly regarding the U.S. government's surveillance practices, which many EU officials and privacy advocates argued did not align with EU standards of privacy and data protection. In July 2020, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield Framework, citing concerns over U.S. surveillance practices and the lack of legal recourse for EU citizens. This decision, known as the Schrems II ruling, highlighted the ongoing tension between the U.S. and EU regarding data privacy and the challenges of ensuring that biometric data transfers comply with stringent European regulations. Following this ruling, both regions have been negotiating new frameworks to address these concerns and restore the flow of data while ensuring adequate protections are in place.

B. Case Study: India's Aadhaar and Its Cross-Border Implications

India's Aadhaar program, one of the world's largest biometric identification systems, has significant implications for cross-border data sharing. Aadhaar, launched in 2009, involves the collection of biometric data, including fingerprints and iris scans, to provide a unique identification number to Indian residents. The program aims to enhance access to services and benefits while streamlining administrative processes. However, Aadhaar's extensive data collection and its use have raised concerns about privacy and security, especially in the context of international data sharing. Critics argue that the centralized nature of the Aadhaar database and the potential for data breaches pose significant risks. There have been instances where Aadhaar data was leaked or misused, raising questions about its adequacy for international data exchanges. The Indian government has implemented measures to address these concerns, such as the Aadhaar Act and various data protection regulations. However, the program's cross-border implications remain complex. The sharing of Aadhaar data with foreign entities, including international organizations and businesses, raises issues related to data sovereignty and privacy. Balancing the benefits of Aadhaar's global integration with the need to protect individuals' personal information continues to be a challenge.

C. Case Study: International Collaboration in Counter-Terrorism

International collaboration in counter-terrorism often involves the sharing of biometric data to enhance security and prevent terrorist activities. One notable example is the use of biometric databases by agencies such as Interpol and the European Border and Coast Guard Agency (Frontex) to track and identify individuals involved in terrorism or related activities. Interpol's biometric databases facilitate the exchange of fingerprints, facial recognition data, and other biometric information among member countries. This collaboration aims to identify known terrorists, track their movements, and prevent potential threats. For instance, Interpol's Database of Stolen Works of Art includes biometric data linked to stolen artworks, which helps in recovering these items and preventing their illegal sale. Frontex, which oversees border control operations within the EU, uses biometric data to enhance border security and manage immigration effectively. The agency's biometric systems help verify identities, detect fraudulent documents, and identify individuals who may pose security risks. The use of biometric data in these contexts is intended to improve the efficiency and effectiveness of counter-terrorism efforts, while also addressing concerns about privacy and the potential for misuse of data.

VI. Challenges and Future Prospects

A. Harmonizing Global Legal Standards

One of the foremost challenges in the realm of cross-border biometric data sharing is harmonizing global legal standards. The diverse regulatory frameworks across countries and regions create a fragmented landscape that complicates international data transfers. The European Union's General Data Protection Regulation (GDPR) sets a high standard for data protection, but its stringent requirements are not universally adopted. Conversely, many countries, particularly those in regions such as the United States and parts of Asia, have less comprehensive regulations, leading to discrepancies in how biometric data is protected and handled. Efforts to harmonize these standards involve international collaborations and agreements aimed at bridging regulatory gaps. Initiatives like the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System seek to create a uniform set of data protection standards that can facilitate international data flows while ensuring adequate privacy protections. However, achieving global consensus remains challenging due to differing national interests, legal traditions, and levels of technological advancement. The varying approaches to data protection, from rigorous standards in the EU to more flexible frameworks elsewhere, underscore the difficulties in establishing a cohesive global standard. To address these challenges, there is a growing call for multilateral agreements that can set international benchmarks for biometric data protection. Such agreements would need to balance the needs of various stakeholders, including governments, businesses, and individuals, to create a framework that ensures privacy while enabling the efficient exchange of data. The future of harmonizing global legal standards hinges on international cooperation and the willingness of countries to align their regulations with agreed-upon global norms.

B. Balancing National Security and Individual Privacy

Balancing national security and individual privacy is a critical challenge in the context of cross-border biometric data sharing. On one hand, biometric data can significantly enhance national security by aiding in the identification and tracking of individuals involved in criminal activities or terrorism. It enables more accurate and efficient border controls, enhances law enforcement capabilities, and supports counter-terrorism efforts. On the other hand, the collection and sharing of biometric data raise significant privacy concerns. The potential for misuse or abuse of sensitive biometric information poses risks to individuals' rights and freedoms. Privacy advocates argue that extensive biometric data collection can lead to surveillance overreach and erosion of civil liberties. The challenge lies in ensuring that security measures do not disproportionately infringe on privacy rights and that biometric data is used responsibly and transparently. To address this challenge, governments and organizations must implement robust data protection measures and establish clear guidelines on the use and sharing of biometric data. Legal frameworks should include provisions for accountability, oversight, and redress mechanisms to protect individuals' rights. Balancing national security with privacy requires a nuanced approach that considers both the benefits of biometric data for public safety and the need to safeguard personal freedoms.

VII. Result and Discussion

The cross-border sharing of biometric data reveals a complex legal landscape characterized by fragmented regulations and varying standards across jurisdictions. While international frameworks like the GDPR and the Convention on Cybercrime provide foundational guidelines, they often fall short of addressing the specific challenges posed by biometric data. The discrepancies between stringent European standards and more lenient practices elsewhere highlight the need for harmonized global legal standards. Balancing national security needs with privacy concerns remains a persistent issue, with advancements in biometric technologies further complicating legal and ethical considerations. Future efforts must focus on creating cohesive international agreements and adapting legal frameworks to accommodate evolving technologies while protecting individual rights and facilitating secure data exchanges. The evaluation of data protection compliance across different regions highlights significant variations in standards and practices. The European Union stands out with the highest levels of data privacy protection (95%) and legal framework maturity (90%). This is reflected in their stringent regulatory environment, particularly under the GDPR, which ensures robust cross-border data sharing regulation compliance (85%) and effective risk mitigation (80%).

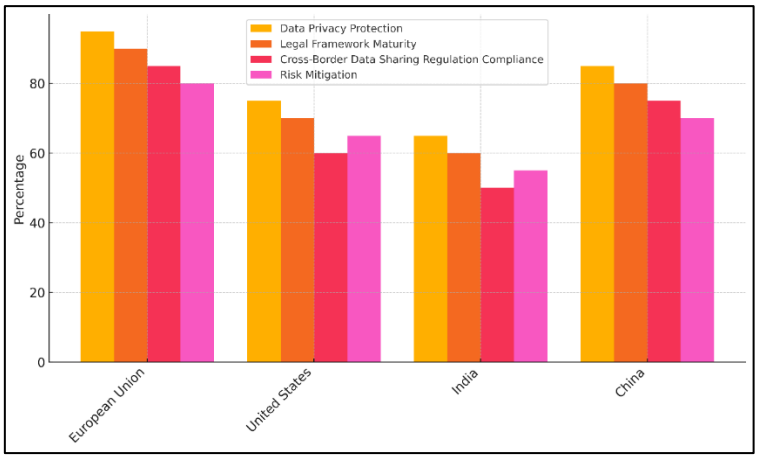

Figure 3: Comparison of Data Protection and Regulation Compliance by Region

These metrics illustrate the EU's comprehensive approach to safeguarding personal data and managing cross-border exchanges. In contrast, the United States shows lower scores across all parameters, with data privacy protection at 75% and legal framework maturity at 70%. The U.S. faces challenges in regulatory compliance for cross-border data sharing (60%) and risk mitigation (65%), largely due to its fragmented legal landscape and varying state-level regulations.

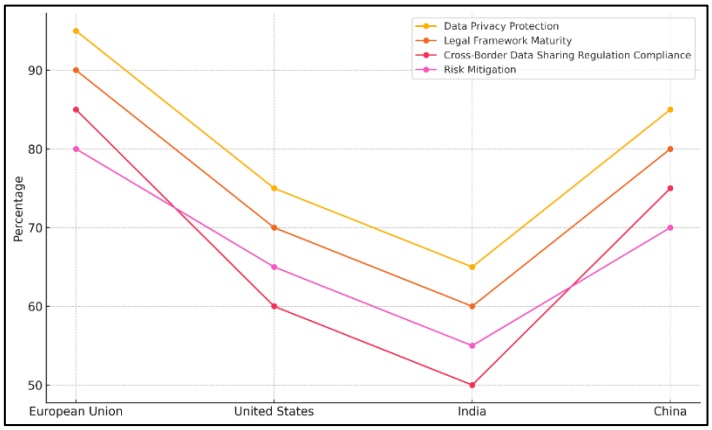

Figure 4: Trends in Data Protection and Regulatory Compliance Across Regions

This lower score indicates difficulties in aligning with international standards and ensuring consistent data protection. India exhibits even lower performance, with data privacy protection (65%) and legal framework maturity (60%) significantly behind the EU. Cross-border data sharing compliance (50%) and risk mitigation (55%) are also weak, reflecting the ongoing development of its data protection infrastructure and limited international integration. China demonstrates strong performance with data privacy protection at 85% and legal framework maturity at 80%. Cross-border data sharing regulation compliance (75%) and risk mitigation (70%) are relatively high, indicating robust national regulations and growing global alignment, although not as stringent as the EU. This positions China as a significant player in global data protection while still working toward full international compliance. The evaluation of biometric technologies reveals notable differences in their effectiveness and security profiles. Fingerprint scanning stands out with the highest effectiveness in security measures (90%) and cross-border interoperability (85%). Its low risk of data breach (20%) and moderate user privacy protection (75%) reflect its maturity and reliability, making it a preferred choice for secure identification across borders.

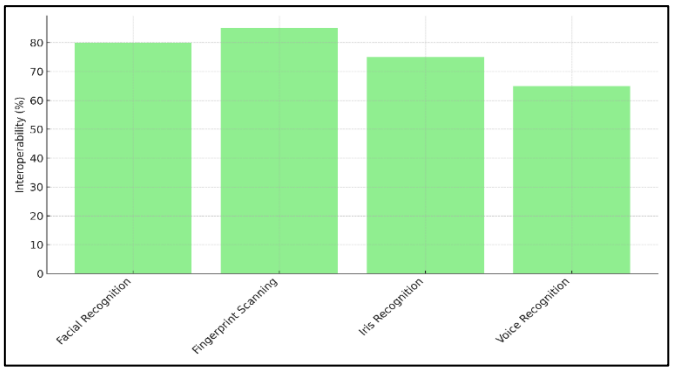

Figure 5: Interoperability of Biometric Recognition Systems

Iris recognition also shows strong performance, with a security measures effectiveness of 88% and a low risk of data breach (25%). However, its cross-border interoperability (75%) lags slightly behind fingerprint scanning. User privacy protection is relatively high (80%), highlighting its effectiveness in safeguarding personal information while being less universally compatible than fingerprint systems. Facial recognition demonstrates good security measures effectiveness (85%) and a higher cross-border interoperability (80%) compared to iris and voice recognition. Despite this, it faces a moderate risk of data breach (30%) and lower user privacy protection (70%).

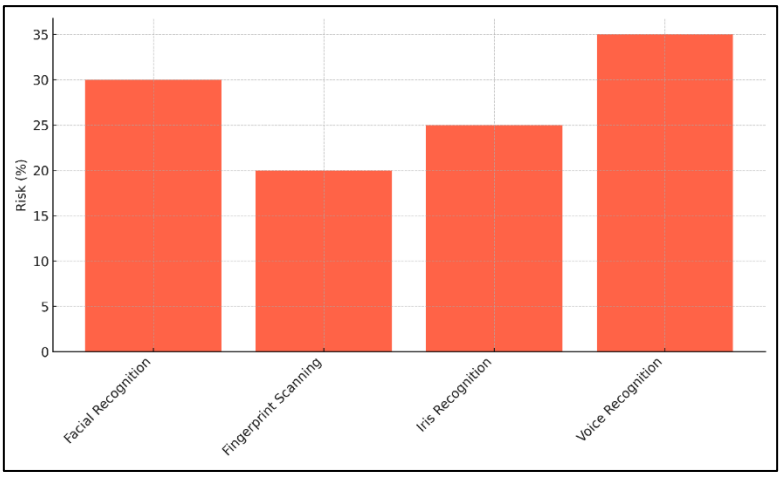

Figure 6: Risk Levels Associated with Biometric Recognition Systems

These factors indicate that while facial recognition is widely used and effective, it presents higher privacy and security concerns than fingerprint scanning. Voice recognition shows the lowest effectiveness in security measures (75%) and cross-border interoperability (65%). It also has the highest risk of data breach (35%) and the lowest user privacy protection (60%). These lower scores suggest that voice recognition, while useful in certain contexts, may be less reliable and secure compared to other biometric technologies, affecting its overall effectiveness and suitability for sensitive applications.

VIII. Conclusion

The cross-border sharing of biometric data is fraught with legal complexities that stem from the diverse regulatory environments and evolving technological landscape. As biometric technologies become increasingly integral to security, healthcare, and governance, the need for robust and coherent legal frameworks has never been more pressing. Current international agreements and regional regulations, such as the GDPR and the Convention on Cybercrime, provide foundational guidelines but often fall short in addressing the unique challenges associated with biometric data. The fragmentation of data protection standards across jurisdictions complicates compliance for organizations and creates gaps in data security and privacy protection. Balancing national security with individual privacy remains a significant challenge. While biometric data offers powerful tools for enhancing security and streamlining processes, it also raises profound privacy concerns. Additionally, there is a need for

ongoing dialogue among stakeholders, including governments, industry leaders, and privacy advocates, to develop adaptive legal frameworks that address the evolving nature of biometric technologies.

References

[1] Saha, R.; Kumar, G.; Geetha, G.; Conti, M.; Buchanan, W.J. Application of Randomness for Security and Privacy in Multi-Party Computation. IEEE Trans. Dependable Secur. Comput. 2021, 1, 1–12.

[2] Rupa, C.; Greeshmanth Shah, M.A. Novel secure data protection scheme using Martino homomorphic encryption. J. Cloud Comp. 2023, 12, 47.

[3] Yang, W.; Wang, S.; Cui, H.; Tang, Z.; Li, Y. A Review of Homomorphic Encryption for Privacy-Preserving Biometrics. Sensors 2023, 23, 3566.

[4] Shah, P.; Prajapati, P. Provable data possession using additive homomorphic encryption. J. King Saud Univ.-Comput. Inf. Sci. 2022, 34, 3448–3453.

[5] Turan, F.; Roy, S.S.; Verbauwhede, I. HEAWS: An accelerator for homomorphic encryption on the Amazon AWS FPGA. IEEE Trans. Comput. 2020, 69, 1185–1196.

[6] Mahmood, Z.; Ibrahem, M. Fully Homomorphic Encryption Scheme Over Integers Based on DGHV Scheme. Control. Syst. Optim. Lett. 2023, 1, 169–173.

[7] Albrecht, M.; Chase, M.; Chen, H.; Ding, J.; Goldwasser, S.; Gorbunov, S.; Halevi, S.; Hoffstein, J.; Laine, K.; Lauter, K.; et al. Homomorphic encryption standard. In Protecting Privacy through Homomorphic Encryption; Springer: Cham, Swizerland, 2021; pp. 31–62.

[8] Feng, T.; Yang, P.; Liu, C.; Fang, J.; Ma, R. Blockchain data privacy protection and sharing scheme based on zero-knowledge proof. Wirel. Commun. Mob. Comput. 2022, 2022, 1040662.

[9] 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.

[10] de Terwangne, C. Council of Europe convention 108+: A modernised international treaty for the protection of personal data. Comput. Law Secur. Rev. 2021, 40, 105497.

[11] Bellanova, R.; Carrapico, H.; Duez, D. Digital/sovereignty and European security integration: An introduction. Eur. Secur. 2022, 31, 337–355.