Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Biometric Data Protection under International Law

Article History:

Name of Author:
Harry Davis[1] and Robert Cohen[2]

Affiliation: [1]Academic Coordinator, Department of Banking and Insurance, Holland International University, Netherlands
[2]Research Associate, Department of Commerce, Oceanic Research University, Netherlands
Corresponding Author: Harry Davis

How to cite this article: Harry Davis and Robert Cohen. Privacy by Design in International Software Compliance. *J Community Med* 2021;2(1);30-33.

Abstract: The increasing collection and utilization of biometric data—including facial recognition, fingerprints, iris scans, and behavioral identifiers—has elevated concerns about privacy, human rights, and data security across global jurisdictions. In 2025, biometric data is widely recognized as a uniquely sensitive and immutable form of personal information, requiring specialized legal treatment. This article explores the regulatory landscape shaping biometric data governance around the world, including landmark frameworks such as the EU's GDPR, China's PIPL, Brazil's LGPD, and India's DPDPA. It outlines foundational legal principles such as explicit consent, data minimization, security-by-design, and cross-border transfer restrictions. The article also examines emerging developments, including the Global Data Protection Standard (GDPS), new treaties governing international transfers, and AI regulations that mandate transparency and prohibit covert biometric profiling. Key challenges such as regulatory fragmentation, ethical tensions, surveillance risks, and technological threats like deepfakes are highlighted. Through comparative analysis and visual data, the article calls for greater international harmonization, human-centered oversight, and innovation to ensure that biometric data protections evolve in tandem with the accelerating pace of digital transformation and surveillance technology.

Keywords: Biometric data, GDPR, data privacy, facial recognition, fingerprints, iris scan, voice recognition, behavioral biometrics,

INTRODUCTION

The widespread collection and processing of **biometric data**—including fingerprints, facial images, voiceprints, iris scans, and behavioral patterns—has triggered a global debate about privacy, human rights, and data protection. As 2025 unfolds, the complexity and sensitivity of biometric data make robust international legal frameworks increasingly critical. This article examines the evolving landscape of biometric data protection across different jurisdictions, the challenges to cross-border enforcement, and the development of international standards.

WHAT IS BIOMETRIC DATA?

Biometric data refers to personal information derived from unique physiological or behavioral traits used to identify individuals. Examples include:

- Fingerprints and palm prints
- Facial recognition data
- Retinal and iris scans
- DNA samples
- Voice recognition
- Behavioral traits (gait, typing patterns)

Such data's permanence and unchangeable link to personal identity make its misuse especially threatening to individual privacy and autonomy[1].

The Rationale for Biometric Data Protection

Because biometric information is unique and essentially irreplaceable if compromised, unauthorized disclosure or exploitation can lead to irreversible harm, including identity theft, surveillance, discrimination, and loss of dignity. This foundational risk underpins the drive for **specific regulatory frameworks** to ensure its collection, processing, storage, and transfer only occur under strict legal control and with individual consent[2].

Key Principles in Global Biometric Data Regulation

1. Consent and Transparency

- **Explicit, informed consent** is universally emphasized for the collection and use of biometric data.
- Individuals must understand and agree to what data is being collected and for what purpose. There must be clear, accessible information and the right to withdraw consent at any time[3][4][5].

2. Data Minimization and Purpose Limitation

- Biometric data should only be collected when strictly necessary for a defined, legal purpose.
- Over-collection or retention beyond the specific purpose is widely prohibited, with requirements to delete data once its intended use has expired[3][5].

3. Security and Data Integrity

- Strong technical safeguards—mandatory encryption, access controls, and breach notification—are required by most up-to-date laws[5].
- Any data breach must be reported to individuals and authorities, often within tight timelines.

4. Individual Rights

- Right to access, rectify, or delete stored biometric data.
- Right to restriction of processing, data portability, and in some regimes, the right to object to automated profiling or AI-based decisions[5].

5. Restrictions on Cross-Border Transfers

- Biometric data cannot be freely transferred to countries that lack adequate privacy protections.
- Laws increasingly require government authorization and robust encryption for international transfers, especially for sensitive data like biometrics[5][6].

MAJOR INTERNATIONAL LEGAL FRAMEWORKS

European Union: GDPR

The **General Data Protection Regulation (GDPR)** is the global benchmark:

- Classifies biometric data as a "special category," meaning its processing is **prohibited by default** unless explicit consent or specific legal bases apply.
- Embeds the "right to be forgotten," strong enforcement (up to 4% of annual global turnover or €20 million in fines), and direct effect for non-EU companies processing European data[4][2].
- Recent legislative extensions (AI Act, new cross-border transfer rules) further restrict biometric data processing, especially with AI and surveillance applications[7][8].

United States

There is **no single federal law** for biometric data. Instead:

- Some states (Illinois' BIPA, Texas, California's CCPA/CPRA) enforce strict opt-in, retention, and security rules, including private rights of action for breaches[4][2].
- Enforcement and protection levels vary state by state, resulting in a "patchwork" approach that complicates cross-border compliance.

China

China's **Personal Information Protection Law (PIPL)**:

- Sets out strong requirements for user consent and use limitation, combining privacy with broad state authority over national security interests.
- Consent and purpose limitation are explicit but coexist with rules that allow extensive state access and use[2].

Canada, India, Brazil, Asia-Pacific

- Canada and Brazil: Robust privacy laws extend to biometric data, with heavy fines for misuse and requirements for registration, privacy impact assessments, and explicit consent[3][2].
- India: The new Digital Personal Data Protection Act and pending biometric guidelines stress consent and storage limitation for biometric data.
- Asia-Pacific: Jurisdictions have introduced stricter rules on cross-border transfers and mandatory security standards for biometric databases[6].

Recent Developments and the Push for Global Standards (2025)

Global Data Protection Standard (GDPS) and New Treaties

- **GDPS**, introduced in 2025, harmonizes local regulations with baseline global standards: single consent form, strong penalties, right to edit/delete data, and 24-hour breach notification[5].
- International treaties restrict the transfer and processing of biometric data to only those countries with adequate legal protections.

Artificial Intelligence Regulation

- New rules ban the automatic collection of biometric data via AI without explicit user permission and require algorithmic transparency for biometric processing purposes[5][8].

Chart: Worldwide Biometric Data Regulatory Coverage (2025)

[image:1]

Sample bar chart illustrating the percentage of countries by region with comprehensive biometric data laws as of 2025.

Digital Consumer Rights Expansion

- Laws in many regions now grant the right to refuse collection, receive compensation for misuse, and demand human intervention in automated profiling decisions involving biometrics.

Core Challenges in Biometric Data Protection

- **Fragmentation:** Lack of harmonization across regions complicates compliance.
- **Transborder Data Flows:** Balancing the needs of security, public interest, and privacy in international contexts remains difficult[9].
- **Ethical Dilemmas:** Even with legal compliance, ethical concerns about consent, transparency, profiling, and redress persist[10].
- **Emergence of AI and Deepfakes:** New technology raises the threat of misuse beyond existing legal safeguards[5][8].
- **Inclusion and Access:** Overly strict or poorly designed biometric laws may exclude marginalized populations from public benefits and services.

Table: Comparative Legal Approaches to Biometric Data (2025)

Region	Legal Basis	Consent	User Rights	Restrictions on Transfer
EU (GDPR)	Special Category	Explicit, opt-in	Access, erasure, objection	Strict, adequacy required
US (State)	State Laws/patchwork	Varies	Limited; stronger in some	Limited; state/fed gaps
China (PIPL)	Comprehensive	Explicit	Access, correction, deletion	State access prioritized
Brazil	Comprehensive (LGPD)	Explicit	Full user control	Adequacy/strong rules
India	Sectoral/emerging	Consent	Growing focus on rights	Cross-border limits coming

Infographic: The Biometric Data Protection Lifecycle

[image:2]

Infographic showing stages: data collection (consent), secure storage (encryption), usage (purpose limitation), sharing (restriction), deletion (user right), breach response (notification).

CONCLUSION

Biometric data protection is now a central pillar of international privacy law, continually evolving in response to technological innovation and social concern. While the EU's GDPR sets the global gold standard, new harmonization efforts such as the GDPS (2025) signal a global convergence toward explicit consent, security safeguards, robust user rights, and international accountability.

Yet, gaps—especially in cross-border flows and ethics—require ongoing international dialogue, oversight, and innovation to protect human dignity and autonomy in the digital age.

"Because biometric data is literally a part of ourselves, its careless or wrongful use risks our very identity, autonomy, and freedom."
[image:1]
[image:2]

REFERENCES:

1. https://wilj.law.wisc.edu/wp-content/uploads/sites/1270/2022/09/39.2_365-390_Odden.pdf
2. https://jlsda.com/index.php/lsda/article/view/26
3. https://www.tcwglobal.com/blog/international-biometric-data-laws
4. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data
5. https://lumiversesolutions.com/data-privacy-new-laws-in-2025-whats-changing-copy/
6. https://securiti.ai/privacy-roundup/may-2025/
7. https://trustarc.com/resource/european-union-data-privacy-whats-next-for-2025/
8. https://bigid.com/blog/2025-global-privacy-ai-and-data-security-regulations/
9. https://www.elsevier.es/en-revista-mexican-law-review-123-articulo-legal-challenges-biometric-immigration-control-S1870057816300063?redirectNew=true
10. https://www.daon.com/resource/the-ethics-and-concerns-of-biometric-data-collection/

