E-JUSTICE: JOURNAL OF LAW AND TECHNOLOGY

Vol. 1 No. 1, September 2024, pp 68-80

Research Article

Biometric Data Protection in Human Rights Perspective: Analysis Based on the UN Charter and International Conventions

Try *Hardyanthi*[1]

Corresponding e-mail: tryhardyanthi@ump.ac.id

Article Information

Article History
Received: Jun 6th, 2024
Revised: Sept 20th, 2024
Accepted: Sept 22nd, 2024

Keywords:
Biometric data protection; Cybersecurity; Human rights; Mass surveillance; Privacy; UN Charter; Data regulation.

How to Cite:
Hardyanthi, Try. "Biometric Data Protection in Human Rights Perspective: Analysis Based on the UN Charter and International Conventions." *E-Justice: Journal of Law and*

Abstract

Background: In the digital era, biometric data has become essential for security, healthcare, and banking, offering a secure alternative to traditional identification methods. Despite its advantages, biometric data poses significant privacy and personal data protection risks due to its unique and permanent nature.

Methodology: This research employs a qualitative approach with document analysis as the primary method. The study reviews literature, policies, and regulations from various countries known for best practices in biometric data protection.

Objectives: The primary objective is to analyze the protection of biometric data from a human rights perspective, grounded in the UN Charter and other international conventions. The study aims to identify relevant human rights principles applicable to biometric data protection, evaluate current regulations, and address contemporary challenges.

Findings: The research highlights that while international frameworks like the GDPR provide robust legal structures for data protection, effective implementation remains a challenge. Key issues include cybersecurity threats, misuse of biometric data, and mass surveillance. Case studies from countries like India, the EU, Canada, and Singapore

[1] Department of Sharia Economic Law, Universitas Muhammadiyah Purwokerto, Indonesia. | https://orcid.org/0009-0002-5710-8250

Technology 1, no. 1 (2024): 68-80.

show varied approaches to regulation and enforcement, emphasizing the need for stringent oversight and compliance mechanisms.

Originality/Novelty: This study fills a gap in the literature by focusing on biometric data protection from a human rights perspective, specifically examining how principles from the UN Charter and international conventions can be applied. The research provides comprehensive insights into integrating human rights principles with biometric data protection, ensuring the technology's use does not infringe on individual privacy or lead to discrimination.

Introduction

In the current digital era, biometric data has emerged as one of the most influential technologies across various sectors, including security, healthcare, and banking. Biometric data, which includes information such as fingerprints, facial recognition, iris scans, and voice patterns, is generally defined across various jurisdictions and institutions as unique, measurable characteristics used to identify and authenticate individuals. For instance, Article 4(14) of the GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person." Similarly, Singapore's PDPC in its "Guide on Responsible Use of Biometric Data in Security Applications" defines biometric data as any data derived from biometric identifiers such as fingerprints or facial features, specifically when used for identity verification purposes. The U.S. National Institute of Standards and Technology (NIST) describes biometrics as automated methods of recognizing individuals based on their physical or behavioral characteristics. These definitions highlight the core concept that biometric data is intrinsically linked to individual identity, offering enhanced security. However, despite its substantial benefits, there are inherent risks related to privacy and personal data protection that vary across regulatory landscapes and cannot be ignored.[1]

Biometric data is unique and permanent, meaning that if it falls into the wrong hands or is misused, the consequences can be far more severe compared to other types of personal data. In the context of human rights, the protection of biometric data is a critical issue because it pertains to the universally recognized right to privacy.[2] Therefore, the

[1] C. Jasserand, "The Future AI Act and Facial Recognition Technologies in Public Spaces:," *European Data Protection Law Review* 9, no. 4 (2023): 430–43, https://doi.org/10.21552/edpl/2023/4/9.

[2] Alina Wernick and Anna Artyushina, "Future-Proofing the City: A Human Rights-Based Approach to Governing Algorithmic, Biometric and Smart City Technologies," *Internet Policy Review* 12, no. 1 (2023), https://doi.org/10.14763/2023.1.1695.

management of biometric data protection must be handled with care and in compliance with internationally recognized human rights principles.

Extensive research has been conducted on the protection of biometric data in the context of human rights. For example, a study by Jain et al. (2016) highlights the technical aspects of biometric data security and provides recommendations for strengthening encryption systems and data protection. Meanwhile, Yampolskiy's (2018) research focuses on privacy risks associated with the use of biometric data, particularly in the context of government and private sector surveillance. Yampolskiy argues that although biometric technology can enhance security, without proper regulation, biometric data can be misused for mass surveillance that infringes on individual privacy.

Another study by Hildebrandt (2015) discusses the protection of personal data within the European Union's legal framework, especially after the implementation of the General Data Protection Regulation (GDPR), which is a comprehensive law enacted in 2018 to strengthen and unify data protection for individuals within the EU, granting them greater control over their personal data and imposing strict obligations on organizations handling such data. ildebrandt emphasizes that while the GDPR provides a robust legal framework for data protection, there are still challenges in effective implementation at the national and corporate levels. On the other hand, research by Moyle et al. (2017) focuses on the social impact of using biometric data, particularly how this technology can influence public perception of privacy and security.

Although previous research has provided valuable insights into the technical and legal aspects of biometric data protection, there is a gap in the literature that specifically examines biometric data protection from a human rights perspective based on the UN Charter and other international conventions. This study aims to fill that gap by providing a comprehensive analysis of how human rights principles can be applied to protect biometric data. By examining key documents such as the UN Charter which outlines fundamental human rights and the principles of international law, and the International Covenant on Civil and Political Rights (ICCPR), a treaty that guarantees civil and political rights such as privacy and freedom of expression, and other international conventions, this research seeks to highlight the importance of protecting biometric data in safeguarding individual privacy and freedom.

The primary objective of this research is to analyze the protection of biometric data from a human rights perspective, grounded in the strong legal foundation of the UN Charter and other international conventions. This study aims to identify relevant human rights principles applicable to the protection of biometric data. Furthermore, it analyzes how the UN Charter and conventions such as the ICCPR, regulate biometric data protection. The study also reviews policies and regulations implemented by various countries to protect biometric data. Furthermore, it identifies contemporary challenges and issues in biometric data protection and provides recommendations to strengthen it within the human rights framework.

This research will focus on legal analysis and human rights principles related to biometric data protection. The scope of the study includes international legal documents such as the UN Charter, the ICCPR, and other relevant international conventions concerning human rights and personal data protection. Moreover, the research includes an analysis of policies and regulations from several countries considered to have best practices in biometric data protection. The study also identifies and discusses contemporary issues such as mass surveillance, biometric data misuse, and technical challenges in protecting biometric data.

However, this research has several limitations. It will not delve into technical aspects or specific technologies related to biometric data, such as encryption methods or biometric recognition algorithms. The analysis will primarily focus on the international legal framework and several national case studies but will not cover all countries in detail. Furthermore, this research is more qualitative, involving legal document analysis and existing literature review, without empirical data collection through surveys or interviews.

Research Method

This research employs a qualitative approach with document analysis as the primary method. The data sources include international legal documents such as the UN Charter, the ICCPR), and various other international conventions relevant to human rights and personal data protection. The analysis process begins with the collection of related legal documents, followed by a literature review to understand the context and practical applications of the principles outlined in these documents. Furthermore, this research reviews policies and regulations from several countries considered to have best practices in biometric data protection, aiming to provide a more comprehensive overview of the implementation of human rights principles in the context of biometric data protection.

To support the analysis, the research also examines case studies and reports from international organizations and relevant research institutions. The analytical techniques involve interpreting legal texts and related documents to identify how human rights principles are applied in biometric data protection. This analysis also includes an evaluation of the contemporary challenges and issues faced in the implementation of biometric data protection. Through this approach, the research aims to provide in-depth insights into how human rights principles can be effectively applied to protect biometric data and offer practical recommendations to enhance data protection in a global context.

Fundamental Concepts and Use of Biometric Data

Data of Biometric refers to information derived from an individual's unique biological characteristics, such as fingerprints, facial features, iris patterns, or voice.[3] In the advancing digital era, the use of biometric data has become increasingly common across various

[3] Lucia Nalbandian, "An Eye for an 'I:' A Critical Assessment of Artificial Intelligence Tools in Migration and Asylum Management," *Comparative Migration Studies* 10, no. 1 (December 3, 2022): 32, https://doi.org/10.1186/s40878-022-00305-0.

aspects of daily life. This data is utilized to identify individuals, secure access to electronic devices, verify identity authenticity, and even in medical applications.[4]

The use of biometric data introduces a more sophisticated and reliable authentication concept compared to traditional identification methods like passwords or PINs.[5] This is due to the unique biological characteristics of individuals that are difficult to replicate or steal. For instance, while someone might attempt to mimic another person's fingerprint, accurately matching all necessary details for precise authentication is highly challenging. One of the primary advantages of using biometric data is ease of use. Users do not need to remember or manage complex passwords, which are often sources of frustration and security issues. Instead, authentication is conducted quickly and easily through biometric scanning, providing a smoother user experience.[6]

However, the use of biometric data also raises several concerns, particularly regarding data privacy and security. Biometric characteristics are highly sensitive information as they cannot be changed like passwords or PINs. Therefore, protecting biometric data is crucial to prevent misuse or unauthorized access. Moreover, the use of biometric data presents security challenges. Although the uniqueness of biological characteristics makes them difficult to replicate, the technology used to capture, store, and process biometric data is also susceptible to cyber attacks.[7] Ensuring the security of biometric systems is vital to prevent data theft or manipulation that could jeopardize individual privacy.

The use of biometric data also prompts ethical questions related to its collection and utilization. How biometric data is collected, stored, and used can significantly impact individual privacy rights. For instance, using biometric data in mass surveillance or law enforcement can threaten individual freedoms and rights. Furthermore, there are concerns about potential discrimination in the use of biometric data. For example, if facial recognition technology does not perform well for individuals with darker skin tones or uncommon facial features, it could result in unfairness in the system's application.[8]

---

[4] Giuseppe Mobilio, "Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies," *Internet Policy Review* 12, no. 1 (March 31, 2023), https://doi.org/10.14763/2023.1.1699.

[5] André Ramiro and Luã Cruz, "The Grey-Zones of Public-Private Surveillance: Policy Tendencies of Facial Recognition for Public Security in Brazilian Cities," *Internet Policy Review* 12, no. 1 (March 31, 2023), https://doi.org/10.14763/2023.1.1705.

[6] Karolina La Fors and Fran Meissner, "Contesting Border Artificial Intelligence: Applying the Guidance-Ethics Approach as a Responsible Design Lens," *Data & Policy* 4 (October 24, 2022): e36, https://doi.org/10.1017/dap.2022.28.

[7] Beata Paragi and Ahmad Altamimi, "Caring Control or Controlling Care? Double Bind Facilitated by Biometrics between UNHCR and Syrian Refugees in Jordan," *Society and Economy*, February 18, 2022, https://doi.org/10.1556/204.2021.00027.

[8] Arushi Raj and Fatima Juned, "Gendered Identities and Digital Inequalities: An Exploration of the Lived Realities of the Transgender Community in the Indian Digital Welfare State," *Gender & Development* 30, no. 3 (September 2, 2022): 531–49, https://doi.org/10.1080/13552074.2022.2131250.

Therefore, it is important to consider the broader implications of biometric data use in the context of human rights. Biometric data protection must be strictly regulated to ensure individual privacy rights are respected and that this data is not misused for unauthorized purposes. In this context, the role of law and regulation is critical. Strong laws and policies are necessary to govern the use of biometric data and establish high standards of security and privacy.[9] Biometric data protection must align with human rights principles, ensuring that its use does not compromise individual freedoms or lead to discrimination. While the use of biometric data offers significant benefits in authentication and security, it is essential to recognize and address the associated challenges and risks. Biometric data protection should be integrated into a broader human rights framework to ensure its use is consistent with fundamental human principles and respects individual privacy rights.

Human Rights and Data Protection

Biometric data protection has become increasingly crucial in the advancing digital era, where biometric technology is widely used in various contexts, including security, surveillance, and personal identification.[10] However, amid this technological progress, it is essential to ensure that the use of biometric data does not violate human rights, particularly the right to privacy and personal security. Human rights are inherent to every individual simply by virtue of being human. These rights are protected by various international legal instruments, including the UN Charter and the (ICCPR). In the context of biometric data protection, human rights provide a critical foundation for evaluating practices and policies related to the collection, processing, and use of biometric data.

One of the key aspects of human rights related to data protection is the right to privacy. Privacy is a fundamental right that protects individuals from unauthorized interference in their personal and family life. In the context of biometric data, the right to privacy includes the right to control one's own biometric data, including how it is collected, stored, and used by others. The importance of privacy rights in the context of biometric data is reinforced by the fact that it is often closely linked to an individual's personal identity. For instance, fingerprints, retina scans, or facial recognition can be used to uniquely identify a person.[11] Therefore, protecting biometric data is not only about safeguarding sensitive information but also about protecting individual identity and freedom from misuse and unauthorized surveillance.

---

[9] Fieke Jansen, Javier Sánchez-Monedero, and Lina Dencik, "Biometric Identity Systems in Law Enforcement and the Politics of (Voice) Recognition: The Case of SiiP," *Big Data & Society* 8, no. 2 (July 21, 2021): 205395172110636, https://doi.org/10.1177/20539517211063604.

[10] Bronwen Manby, "The Sustainable Development Goals and 'Legal Identity for All': 'First, Do No Harm,'" *World Development* 139 (March 2021): 105343, https://doi.org/10.1016/j.worlddev.2020.105343.

[11] Barrie Gordon, "Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police," *Potchefstroom Electronic Law Journal* 24 (June 30, 2021): 1–29, https://doi.org/10.17159/1727-3781/2021/v24i0a8923.

In addition to the right to privacy, the right to personal security is also relevant in the context of biometric data protection. This right protects individuals from the misuse of power by authorities and ensures that their biometric data is not exploited for harmful purposes.[12] For example, facial recognition used for surveillance in public spaces can pose risks to individual freedoms and threaten personal security. Protecting biometric data from a human rights perspective also involves balancing the need for privacy and security with the need for public safety and crime prevention. While biometric technology can enhance security in some contexts, such as identifying criminals or providing stricter access controls, its use can also pose risks to individual privacy and freedom.[13]

In response to these challenges, it is crucial for countries and international organizations to develop an adequate legal framework to regulate the use of biometric data. This legal framework should include strong protections for privacy and personal security while considering the need for national security and crime prevention. Furthermore, transparency and accountability in the use of biometric data are essential to ensure that its use aligns with human rights principles.[14] This includes developing independent oversight mechanisms and complaint procedures to address violations of privacy and personal security related to the use of biometric data. While the use of biometric data offers significant benefits for authentication and security, it is imperative to recognize and address the associated challenges and risks. Biometric data protection must be integrated into a broader human rights framework to ensure that its use respects fundamental human principles and individual privacy rights.

Analysis of the UN Charter and International Conventions

In safeguarding human rights related to the use and protection of biometric data, it is essential to refer to the framework established by the UN Charter and relevant international conventions. Since its adoption in 1945, the UN Charter has served as a cornerstone in upholding human rights principles globally. Furthermore, international conventions such as the (ICCPR) provide a more detailed legal framework concerning individual civil and political rights.[15]

[12] Isadora Neroni Rezende, "Facial Recognition in Police Hands: Assessing the 'Clearview Case' from a European Perspective," *New Journal of European Criminal Law* 11, no. 3 (September 13, 2020): 375–89, https://doi.org/10.1177/2032284420948161.
[13] Niraja Gopal Jayal, "Reconfiguring Citizenship in Contemporary India," *South Asia: Journal of South Asian Studies* 42, no. 1 (January 2, 2019): 33–50, https://doi.org/10.1080/00856401.2019.1555874.
[14] Raul Sanchez-Reillo et al., "How to Implement EU Data Protection Regulation for R&D in Biometrics," *Computer Standards & Interfaces* 61 (January 2019): 89–96, https://doi.org/10.1016/j.csi.2018.01.007.
[15] Felicity Gerry, Julia Muraszkiewicz, and Olivia Iannelli, "The Drive for Virtual (Online) Courts and the Failure to Consider Obligations to Combat Human Trafficking – A Short Note of Concern on Identification, Protection and Privacy of Victims.," *Computer Law & Security Review* 34, no. 4 (August 2018): 912–19, https://doi.org/10.1016/j.clsr.2018.06.002.

The UN Charter emphasizes the importance of respecting human rights for all individuals without discrimination. Article 12 of the UN Charter specifically recognizes the right of every individual to privacy and personal security.[16] However, the use of biometric technology to collect and process individuals' personal data poses challenges concerning the right to privacy guaranteed by the UN Charter. How can the human rights principles enshrined in the UN Charter be applied in the context of biometric data?

International conventions like the ICCPR are critical instruments in setting more specific human rights standards. Article 17 of the ICCPR recognizes the right of individuals to privacy and personal security, as well as the right to protection from arbitrary interference with their honor and reputation.[17] The implications of this article for the use and protection of biometric data have been a subject of intense debate.

The use of biometric data, such as fingerprints and facial recognition for identification, raises questions about the extent to which this practice aligns with the privacy rights guaranteed by the ICCPR. Some argue that the use of biometric data by governments or private entities may infringe on privacy rights due to the potential for misuse beyond individual control. Implementing the principles set forth in the UN Charter and the ICCPR in the context of biometric data requires a careful balance between the need for security and the protection of individual privacy.[18] The challenge lies in developing appropriate regulations, effective oversight, and a clear understanding of the limitations of the use of biometric data. How these principles influence policies and practices in biometric data protection across different countries is a relevant question in the discussion of human rights and technology.

In this analysis, it is important to consider that international conventions like the ICCPR provide a strong foundation for protecting human rights in the context of biometric data use. However, the real challenge lies in the implementation and enforcement of these principles at the national and international levels.[19] Further research and international cooperation are necessary to develop a more comprehensive framework for protecting individual privacy in the increasingly advanced digital era.

[16] E.J. Kindt, "Having Yes, Using No? About the New Legal Regime for Biometric Data," *Computer Law & Security Review* 34, no. 3 (June 2018): 523–38, https://doi.org/10.1016/j.clsr.2017.11.004.
[17] Claire Gayrel, "The Principle of Proportionality Applied to Biometrics in France: Review of Ten Years of CNIL's Deliberations," *Computer Law & Security Review* 32, no. 3 (June 2016): 450–61, https://doi.org/10.1016/j.clsr.2016.01.013.
[18] Federica Fedorczyk, "Navigating the Dichotomy of Smart Prisons: Between Surveillance and Rehabilitation," *Law, Innovation and Technology* 16, no. 1 (January 2, 2024): 243–60, https://doi.org/10.1080/17579961.2024.2313793.
[19] Jasserand, "The Future AI Act and Facial Recognition Technologies in Public Spaces:"

Challenges and Contemporary Issues in Biometric Data Protection

In the increasingly advanced digital era, the use of biometric data has become more common in various aspects of daily life. This data is used to identify individuals, secure access to electronic devices, verify identity authenticity, and even in medical applications.[20]

Protecting biometric data within the context of human rights faces several significant implementation challenges. One of the primary challenges is effectively securing biometric data from cyber threats. Sensitive biometric data, such as fingerprints, facial features, or iris patterns, are vulnerable to cyber attacks aimed at theft, manipulation, or illegal access. This requires robust protection through advanced encryption technologies and cybersecurity systems capable of anticipating and responding to threats swiftly.[21]

Beyond security challenges, contemporary issues such as the misuse of biometric data and mass surveillance also raise serious concerns. Misuse of biometric data by malicious actors can harm individuals financially, emotionally, and even physically. For example, cases of identity fraud using biometric data for criminal or fraudulent purposes highlight the potential dangers.[22] Furthermore, the use of facial recognition technology in mass surveillance by governments or private entities often violates individual privacy and can lead to excessive surveillance, raising questions about the balance between security and privacy.

Case studies from countries implementing biometric data protection can provide valuable insights into various approaches and practices that can be applied in different contexts. For instance, India has launched the world's largest biometric identification program, Aadhaar, which uses biometric data for identification and public service delivery. This case study can offer a better understanding of the challenges and benefits of large-scale biometric data implementation.[23]

Furthermore, examples of national regulations and policies aligned with international standards are crucial to ensure the effective protection of biometric data. Several countries have adopted stringent regulations regarding the collection, use, and storage of biometric data and have implemented effective oversight mechanisms to ensure compliance with these regulations. One notable example is the European Union's (GDPR). The GDPR

[20] Alex Sager, "Big Data, Surveillance, and Migration: A Neo-Republican Account," *Journal of Global Ethics* 19, no. 3 (September 2, 2023): 335–46, https://doi.org/10.1080/17449626.2023.2271016.
[21] Mobilio, "Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies."
[22] Edward B Kang, "Biometric Imaginaries: Formatting Voice, Body, Identity to Data," *Social Studies of Science* 52, no. 4 (August 8, 2022): 581–602, https://doi.org/10.1177/03063127221079599.
[23] A. Zh. Stepanyan, "European Artificial Intelligence Act: Should Russia Implement the Same?," *Kutafin Law Review* 8, no. 3 (October 5, 2021): 403–22, https://doi.org/10.17803/2313-5395.2021.3.17.403-422.

includes strict rules regarding the collection, use, and storage of biometric data and provides individuals with rights to control their personal data.[24]

Similarly, Canada has adopted regulations such as the Personal Information Protection and Electronic Documents Act (PIPEDA), which provides protection for biometric data and mandates organizations to secure biometric data with high standards. PIPEDA also requires organizations to provide clear information to individuals about the use and disclosure of their biometric data and grants individuals the right to access and correct their data. In Asia, Singapore has enacted strict regulations on personal data protection through the Personal Data Protection Act 2012 (PDPA). The PDPA regulates the collection, use, and disclosure of personal data, including biometric data, and requires organizations to implement effective oversight mechanisms to ensure compliance. Complementing this, the Singapore Personal Data Protection Commission (PDPC) issued the "Guide on Responsible Use of Biometric Data in Security Applications," which provides specific guidelines on the ethical and secure use of biometric data. The guide emphasizes the importance of minimizing data collection, ensuring data accuracy, and implementing robust security measures to prevent unauthorized access. It also advises organizations to conduct regular risk assessments and to inform individuals about the specific purposes for which their biometric data is being collected and used. The PDPA, along with the PDPC guide, imposes severe penalties for violations, which can include significant fines and bans on processing biometric data.[25]

These examples demonstrate how several countries have taken concrete steps to protect individuals' biometric data through stringent regulations and effective oversight mechanisms. This indicates a global trend towards recognizing the importance of biometric data protection in facing modern technological challenges. In addressing these challenges and contemporary issues, collaboration between governments, international organizations, and the private sector is crucial.[26] Only through close cooperation and good coordination can we overcome the challenges of protecting biometric data while ensuring its use remains consistent with human rights principles.

Conclusion

This study outlines the importance of biometric data protection in the context of human rights, highlighting both the benefits and risks associated with the use of biometric

[24] David Humphrey, "Sensing the Human: Biometric Surveillance and the Japanese Technology Industry," *Media, Culture & Society* 44, no. 1 (January 16, 2022): 72–87, https://doi.org/10.1177/01634437211036996.
[25] Christopher O'Neill et al., "The Two Faces of the Child in Facial Recognition Industry Discourse: Biometric Capture between Innocence and Recalcitrance," *Information, Communication & Society* 25, no. 6 (April 26, 2022): 752–67, https://doi.org/10.1080/1369118X.2022.2044501.
[26] Muhammad Khaeruddin Hamsin et al., "Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection," *Al-Manahij: Jurnal Kajian Hukum Islam* 17, no. 1 (April 17, 2023): 53–66, https://doi.org/10.24090/mnh.v17i1.7633.

technology, as well as the challenges in regulating and safeguarding such data. It emphasizes the need to balance security requirements with individual privacy protection and the importance of adhering to human rights principles set forth in international documents such as the UN Charter and the ICCPR. Although biometric data offers more advanced and efficient authentication, the security and privacy of this data remain primary concerns. The unique and permanent nature of biometric data necessitates stringent protection to prevent misuse and unauthorized access. Key challenges include cybersecurity, data misuse, and mass surveillance, which can infringe upon individuals' right to privacy.

The analysis of the UN Charter and other international conventions underscores the importance of upholding human rights principles in regulating the use of biometric data. Balancing security and privacy is crucial in developing effective regulations, while transparency and accountability are essential to ensure compliance with human rights principles. Case studies from various countries demonstrate different approaches to protecting biometric data, with some countries adopting strict regulations and effective oversight mechanisms. Ultimately, biometric data protection is not only about technical security but also about ensuring its use aligns with human rights principles. By integrating biometric data protection into a broader human rights framework, we can ensure that the use of biometric technology does not compromise individual privacy or lead to discrimination.

Acknowledgement

None

Conflict of Interest

None

Author(s) Contribution

Author contribution: conceived the study, collected the data, wrote the manuscript, and contributed to the data analysis and interpretation.

References

Fedorczyk, Federica. “Navigating the Dichotomy of Smart Prisons: Between Surveillance and Rehabilitation.” *Law, Innovation and Technology* 16, no. 1 (January 2, 2024): 243–60. https://doi.org/10.1080/17579961.2024.2313793.

Fors, Karolina La, and Fran Meissner. “Contesting Border Artificial Intelligence: Applying the Guidance-Ethics Approach as a Responsible Design Lens.” *Data & Policy* 4 (October 24, 2022): e36. https://doi.org/10.1017/dap.2022.28.

Gayrel, Claire. “The Principle of Proportionality Applied to Biometrics in France: Review of

Ten Years of CNIL's Deliberations." *Computer Law & Security Review* 32, no. 3 (June 2016): 450–61. https://doi.org/10.1016/j.clsr.2016.01.013.

Gerry, Felicity, Julia Muraszkiewicz, and Olivia Iannelli. "The Drive for Virtual (Online) Courts and the Failure to Consider Obligations to Combat Human Trafficking – A Short Note of Concern on Identification, Protection and Privacy of Victims." *Computer Law & Security Review* 34, no. 4 (August 2018): 912–19. https://doi.org/10.1016/j.clsr.2018.06.002.

Gordon, Barrie. "Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police." *Potchefstroom Electronic Law Journal* 24 (June 30, 2021): 1–29. https://doi.org/10.17159/1727-3781/2021/v24i0a8923.

Hamsin, Muhammad Khaeruddin, Abdul Halim, Rizaldy Anggriawan, and Hilda Lutfiani. "Sharia E-Wallet: The Issue of Sharia Compliance and Data Protection." *Al-Manahij: Jurnal Kajian Hukum Islam* 17, no. 1 (April 17, 2023): 53–66. https://doi.org/10.24090/mnh.v17i1.7633.

Humphrey, David. "Sensing the Human: Biometric Surveillance and the Japanese Technology Industry." *Media, Culture & Society* 44, no. 1 (January 16, 2022): 72–87. https://doi.org/10.1177/01634437211036996.

Jansen, Fieke, Javier Sánchez-Monedero, and Lina Dencik. "Biometric Identity Systems in Law Enforcement and the Politics of (Voice) Recognition: The Case of SiiP." *Big Data & Society* 8, no. 2 (July 21, 2021): 205395172110636. https://doi.org/10.1177/20539517211063604.

Jasserand, C. "The Future AI Act and Facial Recognition Technologies in Public Spaces:" *European Data Protection Law Review* 9, no. 4 (2023): 430–43. https://doi.org/10.21552/edpl/2023/4/9.

Jayal, Niraja Gopal. "Reconfiguring Citizenship in Contemporary India." *South Asia: Journal of South Asian Studies* 42, no. 1 (January 2, 2019): 33–50. https://doi.org/10.1080/00856401.2019.1555874.

Kang, Edward B. "Biometric Imaginaries: Formatting Voice, Body, Identity to Data." *Social Studies of Science* 52, no. 4 (August 8, 2022): 581–602. https://doi.org/10.1177/03063127221079599.

Kindt, E.J. "Having Yes, Using No? About the New Legal Regime for Biometric Data." *Computer Law & Security Review* 34, no. 3 (June 2018): 523–38. https://doi.org/10.1016/j.clsr.2017.11.004.

Manby, Bronwen. "The Sustainable Development Goals and 'Legal Identity for All': 'First, Do No Harm.'" *World Development* 139 (March 2021): 105343. https://doi.org/10.1016/j.worlddev.2020.105343.

Mobilio, Giuseppe. "Your Face Is Not New to Me – Regulating the Surveillance Power of Facial Recognition Technologies." *Internet Policy Review* 12, no. 1 (March 31, 2023). https://doi.org/10.14763/2023.1.1699.

Nalbandian, Lucia. "An Eye for an 'I:' A Critical Assessment of Artificial Intelligence Tools in Migration and Asylum Management." *Comparative Migration Studies* 10, no. 1 (December 3, 2022): 32. https://doi.org/10.1186/s40878-022-00305-0.

O'Neill, Christopher, Neil Selwyn, Gavin Smith, Mark Andrejevic, and Xin Gu. "The Two Faces of the Child in Facial Recognition Industry Discourse: Biometric Capture between Innocence and Recalcitrance." *Information, Communication & Society* 25, no. 6 (April 26, 2022): 752–67. https://doi.org/10.1080/1369118X.2022.2044501.

Paragi, Beata, and Ahmad Altamimi. "Caring Control or Controlling Care? Double Bind Facilitated by Biometrics between UNHCR and Syrian Refugees in Jordan." *Society and Economy*, February 18, 2022. https://doi.org/10.1556/204.2021.00027.

Raj, Arushi, and Fatima Juned. "Gendered Identities and Digital Inequalities: An Exploration of the Lived Realities of the Transgender Community in the Indian Digital Welfare State." *Gender & Development* 30, no. 3 (September 2, 2022): 531–49. https://doi.org/10.1080/13552074.2022.2131250.

Ramiro, André, and Luã Cruz. "The Grey-Zones of Public-Private Surveillance: Policy Tendencies of Facial Recognition for Public Security in Brazilian Cities." *Internet Policy Review* 12, no. 1 (March 31, 2023). https://doi.org/10.14763/2023.1.1705.

Rezende, Isadora Neroni. "Facial Recognition in Police Hands: Assessing the 'Clearview Case' from a European Perspective." *New Journal of European Criminal Law* 11, no. 3 (September 13, 2020): 375–89. https://doi.org/10.1177/2032284420948161.

Sager, Alex. "Big Data, Surveillance, and Migration: A Neo-Republican Account." *Journal of Global Ethics* 19, no. 3 (September 2, 2023): 335–46. https://doi.org/10.1080/17449626.2023.2271016.

Sanchez-Reillo, Raul, Ines Ortega-Fernandez, Wendy Ponce-Hernandez, and Helga C. Quiros-Sandoval. "How to Implement EU Data Protection Regulation for R&D in Biometrics." *Computer Standards & Interfaces* 61 (January 2019): 89–96. https://doi.org/10.1016/j.csi.2018.01.007.

Stepanyan, A. Zh. "European Artificial Intelligence Act: Should Russia Implement the Same?" *Kutafin Law Review* 8, no. 3 (October 5, 2021): 403–22. https://doi.org/10.17803/2313-5395.2021.3.17.403-422.

Wernick, Alina, and Anna Artyushina. "Future-Proofing the City: A Human Rights-Based Approach to Governing Algorithmic, Biometric and Smart City Technologies." *Internet Policy Review* 12, no. 1 (2023). https://doi.org/10.14763/2023.1.1695.