Biometric Technology Today
ISSN (online): 1873-1880

Biometric Technology in National Security: Legal Boundaries and Ethical Issues

Pramod Ambadas Karole[1], Prof. Lasya Vyakaranam[2], Sangita Arun Mandlik[3], Dr. Hrushikesh Joshi[4], Shamim Alam[5], Dr. Uday Chandrakant Patkar[6]

[1]Sandip Institute of Technology & Reserch Centre, Nashik, Maharashtra, India. pramod.karole@sitrc.org.

[2]Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR) Symbiosis Law School (SLS) Symbiosis International (Deemed University), Pune, Maharashtra, India.

[3]Sandip University Nashik, Nashik, Maharashtra, India. sangita.mandlik@sandipuniversity.edu.in

[4]Vishwakarma Institute of Technology, Pune, Maharashtra, India. hrushikesh.joshi@vit.edu.

[5]Sandip University Sijoul, Madhubani, Bihar, India. shamim.alam@sandipuniversity.edu.in

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

Abstract: Biometric technology plays a crucial role in enhancing national security by providing advanced identification and surveillance methods. However, its use raises significant legal and ethical concerns. This paper examines the legal frameworks governing biometric technology in national security and explores the ethical issues surrounding its implementation. Through an analysis of international and national regulations, gaps in the current legal landscape are identified, highlighting the need for more comprehensive policies. Ethical considerations, including privacy invasion, informed consent, data security, and potential bias, are discussed to understand the impact on individual rights. Case studies are used to illustrate successful and controversial applications, offering insights into best practices for ensuring accountability and transparency. The paper concludes with policy recommendations to balance the benefits of biometric technology with the protection of civil liberties.

Keywords: Biometric Technology, National Security, Legal Frameworks, Ethical Issues, Privacy Concerns.

Introduction

Biometric technology has emerged as a powerful tool in national security, revolutionizing how governments identify, monitor, and verify individuals. Unlike traditional methods such as passwords or ID cards, biometrics use unique physical or behavioral characteristics—like fingerprints, facial features, and voice patterns—to accurately identify individuals. This technology provides a higher level of security, making it increasingly valuable for national security measures, including border control, surveillance, and identity verification[1].

In recent years, the integration of biometric systems into national security infrastructures has accelerated. Airports, border checkpoints, and law enforcement agencies worldwide have adopted biometric systems to enhance security and streamline operations. For instance, facial recognition technology is commonly used at international airports to verify the identity of travelers, reducing the risk of fraudulent identities and enhancing the efficiency of border processing. Similarly, law enforcement agencies employ biometric databases to quickly identify suspects and criminals, bolstering public safety efforts[2].

The significance of biometrics in national security lies in its potential to provide rapid, reliable, and accurate identification. This capability is crucial in an era where security threats are increasingly sophisticated and complex. By leveraging biometrics, authorities can more effectively manage border security, prevent unauthorized access to sensitive areas, and identify individuals involved in criminal activities or terrorism. However, the growing use of biometric technology in national security also raises critical legal and ethical concerns.

The objective of this paper is to explore these concerns in detail, examining the legal frameworks that govern the use of biometrics in national security and the ethical issues that arise from its deployment. While biometrics offers numerous benefits, such as enhanced security and efficient processing, it also presents significant challenges. Issues related to privacy, data security, consent, and potential misuse of biometric data must be addressed to ensure that the use of this technology aligns with societal values and legal standards[3].

This research seeks to answer two primary questions: What are the current legal frameworks governing the use of biometric technology in national security? And what ethical issues arise from its use in this context? By investigating these questions, this paper aims to contribute to the ongoing discourse on how to balance the advantages of biometric technology with the need to protect individual rights and uphold ethical principles in national security operations. The exploration of these aspects is crucial for developing policies and practices that support the responsible use of biometrics in national security.

Overview of Biometric Technology in National Security

Biometric technology has become a cornerstone in modern national security strategies, offering a range of methods to verify identities and monitor individuals. Various biometric technologies, such as facial recognition, fingerprinting, iris scanning, and voice recognition, are increasingly deployed in national security applications. These technologies provide a balance between improving security measures and offering unique benefits suited to different contexts. However, they also present several challenges that must be navigated to ensure ethical and responsible use. The table-1 below outlines key biometric technologies, their applications in national security, and the associated advantages and challenges.

Table 1 Key biometric technologies

Type of Biometric Technology	Applications in National Security	Advantages	Challenges
Facial Recognition[4]	Border security, surveillance, and public space monitoring	Rapid identification, contactless, and effective in large crowds	Privacy concerns, potential for misidentification, and ethical issues related to mass surveillance
Fingerprinting[5]	Criminal identification, access control, and verification at border checkpoints	High accuracy, widely accepted, and difficult to forge	Requires physical contact, can be affected by skin conditions, and risk of data breaches
Iris Scanning[6]	Secure access to sensitive areas, identity verification for high-security zones	Extremely accurate, difficult to spoof, and non-invasive	Expensive equipment, potential discomfort for users, and privacy concerns
Voice Recognition[7]	Telephone-based identity verification, monitoring communications	Non-invasive, can be used remotely, and useful for continuous authentication	Vulnerable to background noise, voice alteration, and privacy issues related to voice data storage

The integration of biometric technology into national security practices offers significant benefits in terms of enhanced security and efficiency. Each type of biometric technology brings unique advantages that make them suitable for different security applications, from border control to surveillance. However, these technologies also raise critical challenges, particularly concerning privacy, ethical considerations, and the risk of misuse. Addressing these challenges is essential to harness the full potential of biometrics while safeguarding individual rights and upholding ethical standards. Understanding the advantages and limitations of each technology is crucial for developing balanced and effective national security strategies.

Legal Frameworks Governing Biometric Technology

The use of biometric technology in national security is subject to various legal frameworks that aim to regulate its deployment, ensuring the protection of individual rights while addressing security needs. These frameworks are established at both international and national levels, providing guidelines for the collection, storage, and use of biometric data. However, despite the existence of these regulations, there remain significant gaps and inconsistencies that necessitate further examination[8], [9].

International Regulations

International regulations play a crucial role in setting standards for the use of biometric technology across different countries. The General Data Protection Regulation (GDPR) of the European Union is a prominent example. GDPR classifies biometric data as a special category of personal data, imposing strict rules on its processing. It requires explicit consent from individuals for the collection and use of their biometric information, and mandates robust security measures to protect such data. Additionally, it grants individuals the right to access, rectify, or erase their biometric data under certain conditions.

Other international guidelines include those established by the United Nations and the International Civil Aviation Organization (ICAO). The ICAO has set standards for the use of biometric identifiers in travel documents, such as e-passports, to enhance security in international travel. While these regulations aim to promote a uniform approach to biometric data protection, their implementation varies across countries, leading to differing levels of compliance and enforcement.

National Laws

At the national level, laws governing biometric technology vary widely. Some countries have enacted comprehensive legislation that addresses the use of biometrics in both public and private sectors. For instance, the United States has a patchwork of laws, including the Biometric Information Privacy Act (BIPA) in Illinois, which imposes strict requirements on the collection, storage, and use of biometric data, including obtaining informed consent and providing a private right of action for individuals.

In contrast, other countries have more limited or fragmented legal frameworks. For example, while India has implemented the Aadhaar Act to regulate the use of biometric data in its national identification system, concerns have been raised about the adequacy of data protection and the potential for misuse. This highlights the need for more comprehensive and uniform legal protections across different jurisdictions.

Case Studies

Several countries have implemented biometric technology within legal frameworks, providing useful case studies for understanding the complexities involved. In the United Kingdom, the use of facial recognition technology by law enforcement agencies has sparked significant debate and legal challenges. Courts have called for clearer regulations and oversight to address privacy concerns and potential biases in the technology.

In contrast, Japan has adopted a more cautious approach, implementing strict privacy regulations that limit the use of biometric data. The Act on the Protection of Personal Information (APPI) governs the collection and use of biometric data, requiring organizations to obtain explicit consent and implement security measures to protect the data.

Gaps in Legal Regulations

Despite the existence of international and national legal frameworks, significant gaps remain. One major area of concern is the lack of comprehensive regulations in many countries, leading to inconsistencies in how biometric data is handled. This creates potential loopholes that can be exploited, resulting in privacy violations and misuse of biometric technology[10].

Also, many existing regulations do not fully address the rapid advancements in biometric technology, such as the development of new forms of biometrics like gait or behavioral recognition. There is also a lack of specific guidelines on data retention periods, data sharing between agencies, and the use of biometric data in cross-border contexts.

Overall, while legal frameworks governing biometric technology in national security exist, they are often fragmented and insufficient to address the full range of ethical and privacy concerns. This underscores the need for more comprehensive, harmonized regulations that can adapt to technological advancements and provide clear guidelines for the responsible use of biometrics in national security.

Ethical Issues in the Use of Biometric Technology for National Security

The deployment of biometric technology in national security raises several ethical concerns, primarily related to privacy, consent, data security, potential discrimination, and the overarching challenge of balancing security with individual rights. These issues necessitate careful consideration to ensure that the use of biometrics aligns with ethical standards and respects fundamental human rights.

Privacy Concerns

One of the most significant ethical issues associated with biometric technology is the potential invasion of personal privacy. Biometric data, such as fingerprints, facial features, and iris patterns, is inherently personal and unique to each individual. The collection and storage of this data by government agencies for national security purposes can lead to concerns about surveillance and the misuse of such information. Unlike passwords or ID cards, biometric data cannot be changed if compromised, making its protection paramount. There is a risk that this data could be used beyond its intended purpose, leading to unauthorized tracking or profiling of individuals without their knowledge or consent[11], [12].

Consent and Autonomy

The issue of consent is central to the ethical use of biometric technology. In many national security contexts, individuals are often required to provide their biometric data without fully understanding how it will be used, stored, or shared. This raises questions about the autonomy of individuals to make informed decisions regarding their personal information. Informed consent should ideally involve a clear explanation of the purpose of data collection, how the data will be used, and the potential risks involved. However, in practice, obtaining meaningful consent in situations like border control or public surveillance can be challenging, as individuals may feel they have little choice but to comply.

Data Security and Surveillance

Biometric data is highly sensitive and, if breached, can have severe consequences. The centralization and storage of large biometric databases make them attractive targets for cyberattacks. Unauthorized access to these databases can result in the misuse of biometric information, leading to identity theft or other forms of exploitation. Additionally, the use of biometrics for mass surveillance raises ethical concerns about the potential for a 'surveillance state,' where individuals are constantly monitored, eroding their sense of freedom and privacy. The lack of transparency about how and where biometric data is being used further exacerbates these concerns[13].

Discrimination and Bias

Biometric systems have been shown to exhibit biases, particularly in the case of facial recognition technology. Studies have indicated that these systems can be less accurate in identifying individuals from certain demographic groups, such as women and people of color. This inaccuracy can lead to discriminatory practices, including wrongful identification and unjust treatment by security and law enforcement agencies. The deployment of biased biometric systems can disproportionately impact marginalized communities, leading to ethical concerns about fairness and equality in the use of this technology.

Balancing Security and Ethics

A key ethical dilemma in using biometric technology for national security is balancing the need for enhanced security with the protection of individual rights. While biometrics offer significant advantages in identifying and managing security threats, their use must be weighed against the potential infringement on personal freedoms and privacy. Policymakers and authorities must navigate this balance, ensuring that the implementation of biometric systems is accompanied by robust safeguards, transparency, and accountability measures. This includes establishing clear guidelines on data use, retention, and sharing, as well as mechanisms for individuals to challenge and rectify potential misuse of their biometric data[14], [15].

In conclusion, the ethical issues surrounding the use of biometric technology in national security are complex and multifaceted. Addressing these concerns requires a nuanced approach that respects individual rights while acknowledging the legitimate need for enhanced security. A responsible and ethical deployment of biometric technology necessitates not only robust legal frameworks but also a commitment to transparency, fairness, and the protection of personal autonomy.

Policy Recommendations and Best Practices

Given the complexities and ethical considerations surrounding the use of biometric technology in national security, it is crucial to establish robust policies and best practices to ensure that these technologies are used responsibly and ethically. The following recommendations aim to provide a balanced approach that enhances security while protecting individual rights[16].

Developing Robust Legal Frameworks

To address the legal and ethical concerns of biometric technology, it is imperative to develop comprehensive and robust legal frameworks. These frameworks should include:

- Clear Regulations on Data Collection and Use: Legislation should clearly define the scope of biometric data collection, ensuring it is only used for legitimate security purposes. Limitations on data use, including restrictions on secondary use or sharing with third parties, must be established to prevent misuse.
- Data Protection and Retention Policies: Laws should mandate stringent data protection measures, including encryption and secure storage of biometric data. Additionally, clear guidelines on data retention periods should be implemented to ensure data is not held indefinitely without justification.
- Cross-Border Data Transfer Protections: Given the global nature of national security operations, international cooperation and harmonization of legal frameworks are necessary to regulate the transfer of biometric data across borders, ensuring consistent protection standards.

Ethical Guidelines for Biometric Technology

Establishing ethical guidelines is crucial for guiding the development and implementation of biometric systems. These guidelines should focus on:

- Principles of Fairness and Non-Discrimination: Biometric systems should be designed and tested to minimize biases and ensure equitable treatment of all individuals, regardless of demographic characteristics. Regular audits and updates to these systems are necessary to mitigate potential discriminatory effects.
- Informed Consent and Autonomy: Where feasible, individuals should be provided with clear information about the collection and use of their biometric data and given the opportunity to provide informed consent. In situations where consent is not practical, such as in public surveillance, transparent policies and oversight mechanisms should be in place.
- Minimal Data Collection: Ethical guidelines should emphasize the principle of data minimization, collecting only the necessary biometric data required for specific security purposes to reduce privacy risks.

Ensuring Accountability and Transparency

Mechanisms for oversight and transparency are essential to ensure that the use of biometric technology is accountable and subject to public scrutiny. Key recommendations include:

- Independent Oversight Bodies: Establish independent oversight bodies to monitor and review the use of biometric technology in national security. These bodies should have the authority to investigate complaints, conduct audits, and enforce compliance with legal and ethical standards.
- Transparency Reports: Regular transparency reports should be published by agencies using biometric technology, detailing how and why biometric data is collected, stored, and used. This openness fosters public trust and allows for informed discussions about the implications of biometric surveillance.

Promoting Public Awareness and Engagement

Public understanding and engagement are crucial in shaping the responsible use of biometric technology. Efforts should be made to[17]:

- Educate the Public: Governments and organizations should conduct public education campaigns to inform citizens about biometric technology, its uses in national security, and the associated risks and benefits. This knowledge empowers individuals to make informed decisions about their personal data.
- Facilitate Public Discourse: Creating forums for public discourse and consultation on the use of biometric technology allows for diverse perspectives and concerns to be heard. This engagement can guide the development of policies that reflect societal values and priorities.
- Encourage Stakeholder Involvement: Involving a wide range of stakeholders, including civil society organizations, human rights advocates, and technology experts, in the policymaking process ensures that multiple viewpoints are considered and helps build consensus on the ethical use of biometrics.

Implementing these policy recommendations and best practices is vital for the responsible and ethical use of biometric technology in national security. By developing robust legal frameworks, establishing ethical guidelines, ensuring accountability and transparency, and promoting public awareness, we can harness the benefits of biometrics while safeguarding individual rights and maintaining public trust.

Conclusion and future scope

This paper has explored the intricate legal and ethical landscape of biometric technology in national security, highlighting both its transformative potential and the significant challenges it poses. Key legal issues identified include the lack of comprehensive international and national regulations governing the use of biometric data, particularly in ensuring data protection, consent, and the prevention of misuse. Ethical concerns revolve around privacy invasion, the potential for mass surveillance, the need for informed consent, and the risks of discrimination and bias inherent in biometric systems. These findings underscore the necessity for robust legal frameworks, ethical guidelines, and mechanisms to safeguard individual rights.

The use of biometric technology in national security is expected to grow, driven by advancements in technology and the increasing need for efficient and reliable security measures. Future applications may involve more sophisticated forms of biometrics, such as behavioral and gait recognition, expanding the capabilities of surveillance and identification. However, this evolution will likely intensify existing ethical and legal challenges, particularly regarding privacy and potential abuse of power. As biometric systems become more integrated into national security infrastructure, there will be a pressing need for evolving legal frameworks that can keep pace with technological developments, ensuring that the use of biometrics remains aligned with democratic values and human rights principles. International collaboration will be crucial in establishing standards and norms to guide the ethical and lawful use of biometric technology.

Balancing the benefits of biometric technology with the protection of individual rights is a complex but essential endeavor. While biometrics offer significant advantages for national security, including enhanced accuracy and efficiency in identifying threats, they also present profound ethical dilemmas and legal challenges. The potential for misuse, privacy violations, and discriminatory practices necessitates a cautious and considered approach to the implementation of biometric systems. Ensuring that these technologies are deployed transparently, ethically, and within a robust legal framework is vital to maintaining public trust and upholding the principles of justice and equality. Policymakers, technologists, and society must work collaboratively to navigate this balance, fostering an environment where biometric technology can be harnessed responsibly for the greater good.

Looking forward, there is a need for ongoing research into the development of fair and unbiased biometric systems, as well as methods for enhancing the security of biometric data against emerging cyber threats. Furthermore, exploring the societal implications of increasingly pervasive biometric surveillance, including its impact on personal freedoms and social dynamics, will be crucial. Developing adaptive legal frameworks and ethical guidelines that can accommodate the rapid evolution of biometric technology will be essential in ensuring that its use in national security serves to protect society without compromising fundamental human rights.

References

[1] M. M. Kavanagh, S. D. Baral, M. Milanga, and J. Sugarman, "Biometrics and public health surveillance in criminalised and key populations: policy, ethics, and human rights considerations," *Lancet HIV*, vol. 6, no. 1, pp. e51–e59, Jan. 2019, doi: 10.1016/S2352-3018(18)30243-1.

[2] A. North-Samardzic, "Biometric Technology and Ethics: Beyond Security Applications," *J. Bus. Ethics*, vol. 167, no. 3, pp. 433–450, 2020, doi: 10.1007/s10551-019-04143-6.

[3] P. Datta, S. Bhardwaj, S. N. Panda, S. Tanwar, and S. Badotra, "Survey of Security and Privacy Issues on Biometric System BT - Handbook of Computer Networks and Cyber Security: Principles and Paradigms," B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, Eds. Cham: Springer International Publishing, 2020, pp. 763–776.

[4] Vandana and N. Kaur, "Face and Fingerprint recognizing multimodal biometrics system," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 2022, pp. 1771–1776, doi: 10.1109/ICACITE53722.2022.9823836.

[5] A. Makrushin, A. Uhl, and J. Dittmann, "A Survey on Synthetic Biometrics: Fingerprint, Face, Iris and Vascular Patterns," *IEEE Access*, vol. 11, pp. 33887–33899, 2023, doi: 10.1109/ACCESS.2023.3250852.

[6] S. S. and V. S. K. Reddy, "Multi-modal Biometric System for Face and Fingerprint using Convolutional Neural Network," in *2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC)*, 2021, pp. 1–6, doi: 10.1109/AESPC52704.2021.9708535.

[7] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: a survey," *Artif. Intell. Rev.*, vol. 56, no. 8, pp. 8647–8695, 2023, doi: 10.1007/s10462-022-10237-x.

[8] D. Carpenter, A. McLeod, C. Hicks, and M. Maasberg, "Privacy and biometrics: An empirical examination of employee concerns," *Inf. Syst. Front.*, vol. 20, no. 1, pp. 91–110, 2018, doi: 10.1007/s10796-016-9667-5.

[9] A. De Keyser, Y. Bart, X. Gu, S. Q. Liu, S. G. Robinson, and P. K. Kannan, "Opportunities and challenges of using biometrics for business: Developing a research agenda," *J. Bus. Res.*, vol. 136, pp. 52–62, 2021, doi: https://doi.org/10.1016/j.jbusres.2021.07.028.

[10] R. V. Virgil Petrescu, "Face Recognition as a Biometric Application," *J. Mechatronics Robot.*, vol. 3, no. 1, pp. 237–257, 2019, doi: 10.3844/jmrsp.2019.237.257.

[11] M. Sharif, M. Raza, J. H. Shah, M. Yasmin, and S. L. Fernandes, "An Overview of Biometrics Methods BT - Handbook of Multimedia Information Security: Techniques and Applications," A. K. Singh and A. Mohan, Eds. Cham: Springer International Publishing, 2019, pp. 15–35.

[12] J. Preciozzi *et al.*, "Fingerprint Biometrics From Newborn to Adult: A Study From a National Identity Database System," *IEEE Trans. Biometrics, Behav. Identity Sci.*, vol. 2, no. 1, pp. 68–79, 2020, doi: 10.1109/TBIOM.2019.2962188.

[13] U. Gawande and Y. Golhar, "Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques," *Int. J. Biom.*, vol. 10, no. 2, pp. 142–175, Jan. 2018, doi: 10.1504/IJBM.2018.091629.

[14] N. Khan and M. Efthymiou, "The use of biometric technology at airports: The case of customs and border protection (CBP)," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100049, 2021, doi: https://doi.org/10.1016/j.jjimei.2021.100049.

[15] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry*, vol. 11, no. 2. 2019, doi: 10.3390/sym11020141.

[16] U. Rao and V. Nair, "Aadhaar: Governing with Biometrics," *South Asia J. South Asian Stud.*, vol. 42, no. 3, pp. 469–481, May 2019, doi: 10.1080/00856401.2019.1595343.

[17] M. Debos, "Biometrics and the disciplining of democracy: technology, electoral politics, and liberal interventionism in Chad," *Democratization*, vol. 28, no. 8, pp. 1406–1422, Nov. 2021, doi: 10.1080/13510347.2021.1907349.