



“REGULATING FACIAL RECOGNITION: PRIVACY, SECURITY, AND HUMAN RIGHTS IN UZBEKISTAN”

Sadullayeva Shokhista Davron kizi

shoxistamirazova1999@gmail.com

<https://doi.org/10.5281/zenodo.18976438>

ARTICLE INFO

Received: 08th March 2026

Accepted: 10th March 2026

Online: 12th March 2026

KEYWORDS

personal data, authentication, security, digital technologies, photograph, video recording, biometric data

ABSTRACT

This article examines current issues related to the protection of privacy, data security, and citizens' constitutional rights in the context of the rapid development of biometric technologies. By assessing the advantages and potential risks of biometric authentication systems, the study emphasizes the necessity of regulating facial recognition technology from the perspective of human rights and the rule of law. In particular, the convenience and efficiency of facial recognition technologies, as well as the serious concerns they raise regarding security, privacy, and ethical considerations, are comprehensively analyzed.

Biometric identification, as a method of recognizing individuals based on their unique physical and behavioral characteristics, represents one of the most significant achievements of modern technology¹. This technology enables reliable identification by processing unique biometric data such as fingerprints, facial structure, iris patterns, and voice characteristics².

In facial recognition systems, elements such as the distance between the eyes, cheekbone structure, jawline, nose width, and mouth shape are analyzed to verify an individual's identity. This allows for the automatic identification of a person from digital images or video recordings³.

¹ Punia, M., Choudhary, A., Agarwal, S., & Shukla, V. (2024). Ethical considerations and legal frameworks for biometric surveillance systems: The intersection of AI, soft biometrics, and human surveillance. In *Lecture Notes in Networks and Systems* (p. 659). Springer International Publishing. https://doi.org/10.1007/978-981-97-0641-9_45

² Utegen, D., & Rakhmetov, B. (2023). Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models. *Journal of Digital Technologies and Law*, 1(3), 825. <https://doi.org/10.21202/jdtl.2023.36>

³ ERDİNÇ, G. H. (2020). Processing biometric data in the scope of adequacy principle and consent. *DergiPark (Istanbul University)*. <https://dergipark.org.tr/tr/pub/kvkd/issue/55487/738174>

Although facial recognition technologies can enhance security—particularly when used by law enforcement agencies—by analyzing these unique characteristics, they also raise serious debates regarding privacy, civil liberties, and the protection of human rights⁴.

The development of biometric systems demonstrates a transition from traditional state security systems to commercial and user-oriented applications. This process includes linking encryption keys and passwords to the biometric parameters of the subject⁵. Biometric technologies are rapidly evolving due to the increasing need to protect individuals' property and personal data⁶.

However, considering the sensitivity of biometric information, these processes create several challenges in ensuring data integrity and confidentiality. Therefore, it is essential to introduce strict security measures and legal regulatory mechanisms to prevent potential risks associated with the storage and use of biometric data, including data breaches and unauthorized access.

In particular, biometric authentication methods such as fingerprint and iris scanning play an important role in protecting patient data in the healthcare sector. Nevertheless, storing such information in centralized databases creates the potential risk of identity exposure due to data breaches or cyberattacks⁷.

The processing of biometric data may pose serious risks to the protection of citizens' rights and freedoms because such information allows individuals to be identified at any time based on their unique biological characteristics⁸. This situation directly affects the fundamental principles of the right to privacy, increasing the risk of unjustified interference in an individual's private life by the state or other actors⁹.

⁴ Mahmoud, M. (2025). Facial recognition technology in law enforcement: Navigating the balance between security and civil liberties in the UK and Europe. 22(2). <https://doi.org/10.36394/jls.v22.i2.4>

⁵ Kulikov, A. A. (2021). Application of biometric systems in face identification technologies. *Russian Technological Journal*, 9(3), 7–14. <https://doi.org/10.32362/2500-316x-2021-9-3-7-14>

⁶ Abdulla, W. H., Marattukalam, F., & Krivokuća, V. (2023). Exploring Human Biometrics: A Focus on Security Concerns and Deep Neural Networks. *APSIPA Transactions on Signal and Information Processing*, 12(1). <https://doi.org/10.1561/116.00000021>

⁷ Çiçek, M. (2024). Türkiye’de biyometrik veri güvenliği: Kişisel verilerin korunması kanunu çerçevesinde etik bir değerlendirme. *DergiPark* (Istanbul University). <https://dergipark.org.tr/en/pub/kvkd/issue/88721/1578815>

⁸ Rassolov, I. M., Chubukova, S. G., & Mikurova, I. V. (2019). Biometrics in the context of personal data and genetic information: Legal issues. *Lex Russica*, 1, 108–118. <https://doi.org/10.17803/1729-5920.2019.146.1.108-118>

⁹ Lucero, B., Saracini, C., Mora, M., & Muñoz-Quezada, M. T. (2020). Aspectos éticos del uso de identificadores biométricos. *Acta Bioethica*, 26(1), 43–52. <https://doi.org/10.4067/s1726-569x2020000100043>

Moreover, the centralized collection and storage of such data creates the possibility that, in the event of data breaches or unauthorized use, individuals' identities may be irreversibly exposed¹⁰.

International Experience and National Legislation

The challenge of finding a balance between security and freedom has led to different solutions and approaches in various countries. Each national legal system faces its own specific challenges related to the use of biometric data¹¹.

In particular, it is crucial to obtain explicit and informed consent from individuals before collecting biometric data, adopt data minimization policies that ensure only necessary data are collected, and store data securely through encryption. Additionally, the principle of transparency—explaining how and why data are collected—along with strict legal regulation, has the potential to prevent problems in this field.

The European Union's **General Data Protection Regulation (GDPR)** serves as a leading example in this area by establishing clear requirements for consent, user control over personal data, and significant penalties for violations. However, it is impossible to fully replicate the European experience in every country because national legislation must be adapted to local cultural, political, and technological contexts¹².

Nevertheless, international legal instruments such as the **International Covenant on Civil and Political Rights** and the **European Convention on Human Rights** provide a strong foundation for the protection of digital rights.

Regarding data processing, the Republic of Kazakhstan adopted a national payment system development program. The program envisages the introduction of biometric authentication during payment transactions. As part of this initiative, mechanisms for obtaining the subject's consent to data processing were introduced to enhance personal data security. As a result, individuals must be informed about the procedure for applying for public services, the purpose of the application, and must have the ability to grant or withdraw consent for access to their personal data.

However, analyses of legal documents and regulatory acts in Kazakhstan show that the existing legislation only partially complies with international human rights standards. Moreover, the mere existence of laws does not guarantee effective protection. Particular attention must therefore be paid to the rules governing the collection, processing, and storage of biometric data¹³.

¹⁰ Çiçek, M. (2024). Türkiye’de biyometrik veri güvenliği: Kişisel verilerin korunması kanunu çerçevesinde etik bir değerlendirme. *DergiPark* (Istanbul University). <https://dergipark.org.tr/en/pub/kvkd/issue/88721/1578815>

¹¹ Saidov, A. Kh. (2025). Legal evolution of human rights protection in Uzbekistan amid digital transformation. *Legal Issues in the Digital Age*, 1. <https://doi.org/10.17323/2713-2749.2025.1.53.82>

¹² Saidov, A. Kh. (2025). Legal evolution of human rights protection in Uzbekistan amid digital transformation. *Legal Issues in the Digital Age*, 1. <https://doi.org/10.17323/2713-2749.2025.1.53.82>

¹³ Research of the probable economic, social and legal consequences of the Law of the Republic of Kazakhstan “On dactyloscopic and genome registration.” (2021, June 23). *Soros Kazakhstan Foundation*. www.soros.kz

In Indonesian legislation, the scope of personal rights includes, inter alia:

- a) matters related to an individual's personality, family, personal property, and reputation;
- b) the right to perform or refrain from performing certain actions;
- c) the inviolability of private residence;
- d) private communications¹⁴.

In addition, a number of laws adopted in various sectors establish the necessity of protecting personal rights, including provisions prohibiting unlawful interception of communications and regulating the obligations of data collectors to ensure the confidentiality of collected personal information. Article 26 of the Law on Information and Electronic Transactions explicitly prohibits the transfer of personal data without the consent of the data subject¹⁵.

At least 32 laws regulating the protection of citizens' personal data have been adopted. Most of these laws grant state and private organizations the authority to collect and manage citizens' data, including the right to apply intrusive measures under certain exceptions. The scope of regulation covers sectors ranging from telecommunications, finance and banking, taxation, population registration, and archives to law enforcement, security, and healthcare¹⁶.

Legal Framework for Biometric Data Processing in Uzbekistan

In Uzbekistan, the rapid implementation of digital transformation has made the integration of biometric technologies increasingly significant. While these technologies offer potential benefits in terms of security and efficiency, they also create serious challenges related to privacy and data protection.

The legal framework regulating biometric data in Uzbekistan is still developing, and international standards and best practices in personal data protection are currently being studied.

The collection, storage, and provision of biometric data of citizens in Uzbekistan are regulated by the **Law of the Republic of Uzbekistan "On Personal Data" No. ORQ-547 of July 2, 2019**. According to this law, biometric data refers to personal data that characterize the anatomical and physiological features of the subject. The processing of biometric data is lawful only with the consent of the biometric data subject.

However, the current legislation of Uzbekistan does not contain a separate law specifically regulating biometric data processing. Instead, biometric data processing is carried out in accordance with general rules governing the processing of personal data. These include actions such as collecting, systematizing, storing, modifying, supplementing, using, providing, disseminating, transferring, anonymizing, and destroying personal data (Article 4 of the Law "On Personal Data").

¹⁴ Hope, L., Anakwah, N., Antfolk, J., Brubacher, S. P., Flowe, H., Gabbert, F., et al. (2022). Urgent issues and prospects at the intersection of culture, memory, and witness interviews: Exploring the challenges for research and practice. *Legal and Criminological Psychology*, 27(1), 1–31.

¹⁵ Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3).

¹⁶ Kiss, B., Sekulova, F., Hörschelmann, K., Salk, C. F., Takahashi, W., & Wamsler, C. (2022). Citizen participation in the governance of nature-based solutions. *Environmental Policy and Governance*, 32(3), 247–272.

Although Uzbekistan has adopted several laws related to personal data protection, they do not yet contain detailed provisions specifically addressing biometric data. The use of biometric data in workplaces and public spaces creates unique challenges that require careful consideration of employees' rights, employers' obligations, and the balance between security interests and privacy rights.

These laws establish basic guarantees against unlawful data processing, emphasize confidentiality, and provide sanctions for parties that fail to comply with established standards¹⁷ (Saidov, 2025).

Conclusion

The introduction of facial recognition technology represents an important development in the modern world, offering significant benefits in areas such as public services, business, and security. However, its use also raises a number of challenges related to privacy, security, and ethics.

Addressing these challenges requires improved regulatory guidelines and policies. In the Republic of Uzbekistan, the following proposals can be identified for further improving legislation:

- Clearly defining types of biometrics as well as methods of authentication and identification of individuals in information systems;
- Adopting a separate law regulating the processing of biometric and genetic data and improving the normative legal framework in this field;
- Increasing the population's legal and technical awareness regarding biometric data in the context of rapid information technology development and growing cybercrime, as well as prohibiting mass surveillance using video monitoring systems;
- Legally regulating procedures and mechanisms for linking biometric and personal databases of individuals with the information systems of state bodies and private organizations, and prohibiting the use of images obtained from public sources to populate biometric databases of citizens of Uzbekistan;
- Following the example of artificial intelligence regulation in the European Union, establishing lists of material information carriers that exclude unauthorized access when storing citizens' biometric data according to high and low risk levels;
- Prohibiting the real-time use of biometric identification systems by all users except law enforcement agencies.

When using facial recognition systems in Uzbekistan, state authorities must ensure the implementation of the principles of transparency, legality, and necessity, and develop policies governing the processing of third-party data. As biometric technologies continue to evolve, legal and ethical considerations must remain a continuous priority in order to safeguard human rights and protect personal privacy.

¹⁷ Saidov, A. Kh. (2025). Legal evolution of human rights protection in Uzbekistan amid digital transformation. *Legal Issues in the Digital Age*, 1. <https://doi.org/10.17323/2713-2749.2025.1.53.82>

References:

- Abdulla, W. H., Marattukalam, F., & Krivokuća, V. (2023). Exploring Human Biometrics: A Focus on Security Concerns and Deep Neural Networks. *APSIPA Transactions on Signal and Information Processing*, 12(1). <https://doi.org/10.1561/116.00000021>
- Çiçek, M. (2024). Türkiye’de biyometrik veri güvenliği: Kişisel verilerin korunması kanunu çerçevesinde etik bir değerlendirme. *DergiPark* (Istanbul University). <https://dergipark.org.tr/en/pub/kvkd/issue/88721/1578815>
- ERDİNÇ, G. H. (2020). Processing biometric data in the scope of adequacy principle and consent. *DergiPark* (Istanbul University). <https://dergipark.org.tr/tr/pub/kvkd/issue/55487/738174>
- Hogenhout, L., & Wangmo, R. (2025). Protecting persona biometric data: The case of facial privacy. *arXiv* (Cornell University). <https://doi.org/10.48550/arxiv.2510.03035>
- Hope, L., Anakwah, N., Antfolk, J., Brubacher, S. P., Flowe, H., Gabbert, F., et al. (2022). Urgent issues and prospects at the intersection of culture, memory, and witness interviews: Exploring the challenges for research and practice. *Legal and Criminological Psychology*, 27(1), 1–31.
- Kiss, B., Sekulova, F., Hörschmann, K., Salk, C. F., Takahashi, W., & Wamsler, C. (2022). Citizen participation in the governance of nature-based solutions. *Environmental Policy and Governance*, 32(3), 247–272.
- Kulikov, A. A. (2021). Application of biometric systems in face identification technologies. *Russian Technological Journal*, 9(3), 7–14. <https://doi.org/10.32362/2500-316x-2021-9-3-7-14>
- Lucero, B., Saracini, C., Mora, M., & Muñoz-Quezada, M. T. (2020). Aspectos éticos del uso de identificadores biométricos. *Acta Bioethica*, 26(1), 43–52. <https://doi.org/10.4067/s1726-569x2020000100043>
- Mahmoud, M. (2025). Facial recognition technology in law enforcement: Navigating the balance between security and civil liberties in the UK and Europe.22(2). <https://doi.org/10.36394/jls.v22.i2.4>
- Punia, M., Choudhary, A., Agarwal, S., & Shukla, V. (2024). Ethical considerations and legal frameworks for biometric surveillance systems: The intersection of AI, soft biometrics, and human surveillance. In *Lecture Notes in Networks and Systems* (p. 659). Springer International Publishing. https://doi.org/10.1007/978-981-97-0641-9_45
- Rassolov, I. M., Chubukova, S. G., & Mikurova, I. V. (2019). Biometrics in the context of personal data and genetic information: Legal issues. *Lex Russica*, 1, 108–118. <https://doi.org/10.17803/1729-5920.2019.146.1.108-118>
- Research of the probable economic, social and legal consequences of the Law of the Republic of Kazakhstan “On dactyloscopic and genome registration.” (2021, June 23). Soros Kazakhstan Foundation. www.soros.kz
- Sarabdeen, J. (2022). Protection of the rights of the individual when using facial recognition technology. *Heliyon*, 8(3).
- Utegen, D., & Rakhmetov, B. (2023). Facial recognition technology and ensuring security of biometric data: Comparative analysis of legal regulation models. *Journal of Digital Technologies and Law*, 1(3), 825. <https://doi.org/10.21202/jdtl.2023.36>

Saidov, A. Kh. (2025). Legal evolution of human rights protection in Uzbekistan amid digital transformation. Legal Issues in the Digital Age, 1. <https://doi.org/10.17323/2713-2749.2025.1.53.82>

