Arabian Journal of Science

ISSN:2308-5703

Impact factor:13.5 *International Multidisciplinary Online Journal* October, 2026

THE USE OF FACIAL RECOGNITION TECHNOLOGY WITHOUT CONSENT: THE LEGAL BOUNDARY BETWEEN PUBLIC SECURITY AND THE RIGHT TO PRIVACY

Xurramova Nozima Ikromovna
Student of the Faculty of Law, Termez State University
Doi: https://doi.org/10.5281/zenodo.23906481

Abstract: This article analyzes the legal implications of deploying facial recognition technology (FRT) in public spaces without the explicit consent of the data subject. The study delineates the technological and legal distinctions between conventional video surveillance and automated biometric identification, specifically focusing on the shift from 1:1 verification to 1:N mass identification. International standards are examined through the lens of the Constitution of the Republic of Uzbekistan, the European Union's Artificial Intelligence Act (AI Act), European Court of Human Rights (ECtHR) jurisprudence, and performance evaluations by the National Institute of Standards and Technology (NIST). The paper challenges the "implied consent" fallacy, arguing that presence in a public sphere does not constitute a waiver of biometric privacy. It concludes with practical legislative recommendations for establishing procedural safeguards, purpose limitation, and proportionality criteria to strike an equitable balance between public safety and fundamental privacy rights.

Keywords: facial recognition, biometric data, right to privacy, video surveillance, public safety, Artificial Intelligence Act, 1:N identification, procedural safeguards, ECtHR.

INTRODUCTION: Routine navigation through urban environments—whether commuting via public transit, entering educational institutions, or walking along city streets—is increasingly subjected to continuous video surveillance. While the general public often accepts closed-circuit television (CCTV) as a standard security measure, the integration of biometric analysis transforms passive observation into an active, automated identification process.

From a legal perspective, capturing a video recording of an incident and utilizing an algorithm to extract facial geometry for real-time cross-referencing against massive databases are fundamentally different procedures. The former documents an event; the latter systematically identifies and tracks individuals without their knowledge. This technological shift raises a critical legal question: does an individual's physical presence in a public space grant state or private entities the tacit authority to automatically extract their biometric data and process their identity? According to Article 31 of the Constitution of the Republic of Uzbekistan, the inviolability of private life and the protection of personal data are strictly guaranteed [1]. Furthermore, national legislation requires explicit legal grounds for processing such sensitive information [2]. The primary objective of this paper is to explore this boundary, challenging the assumption that public safety inherently overrides the right to privacy, and proposing a balanced legal framework for the deployment of FRT.

METHODOLOGY: This study employs a qualitative legal research design, utilizing comparative and analytical methods. The primary legal framework analyzed includes the national legislation on personal data and constitutional rights. To provide an international context, the research applies a comparative method to assess the European Union's Artificial Intelligence Act (AI Act) [3] and relevant ECtHR case law [4, 5]. Furthermore, empirical reports from the National Institute of Standards and Technology (NIST) are utilized to establish the factual error rates and algorithmic biases inherent in facial recognition systems [6]. The research is structured in accordance with the IMRAD format to systematically present the technological realities before engaging in normative legal discourse.

RESULTS : 3.1. Technological Dichotomy: 1:1 Verification vs. 1:N Identification In legal and public discourse, "facial recognition" is frequently treated as a monolithic concept. However, technological realities dictate a strict division into two categories with vastly different legal implications.

1:1 Verification: This involves a user actively providing a biometric sample to confirm a claimed identity (e.g., unlocking a smartphone). It is highly accurate, decentralized, and fundamentally relies on user consent.

1:N Identification: This occurs when a camera captures an unknown face in a crowd and compares it against a database of millions (N) to find a match. This is conducted remotely, en masse, and entirely without the subject's consent [7].

3.2. Algorithmic Error Rates and Demographic Bias The assumption that computational algorithms act with objective infallibility is empirically false. NIST's comprehensive evaluations highlight the prevalence of "false positives" (identifying an innocent person as a suspect) and "false negatives" (failing to identify a targeted individual). Crucially, these errors are not distributed equally; algorithmic bias frequently results in higher misidentification rates for specific demographic groups based on race, gender, and age [6]. Consequently, relying on AI for automated legal or penal outcomes without human oversight directly jeopardizes the presumption of innocence.

DISCUSSION: 4.1. The "Implied Consent" and "Nothing to Hide" Fallacies A prevailing argument justifying mass FRT deployment is the notion of implied consent: by entering a public street, an individual visually exposes themselves and thereby allegedly waives their privacy rights. Legal doctrine firmly rejects this premise. Visual exposure in a public space does not equate to consent for algorithmic biometric profiling [8]. According to the European Data Protection Board Guidelines, consent for processing sensitive biometric data must be explicit, informed, and freely given—conditions impossible to meet in a crowded public area [7].

Furthermore, the "nothing to hide, nothing to fear" argument fundamentally misunderstands the nature of privacy. Privacy is not merely the concealment of illicit activities; it is a structural mechanism for limiting state power and preserving individual autonomy [9].

4.2. International Jurisprudence and Regulatory Approaches The ECtHR has consistently ruled that the systematic retention of biometric data from individuals not convicted of any crime violates the right to privacy, notably in the landmark case of S. and Marper v. the United Kingdom [5]. More recently, in Glukhin v. Russia (2023), the Court explicitly addressed FRT, ruling that utilizing facial recognition to identify and prosecute a peaceful demonstrator was highly intrusive and disproportionate, lacking adequate legal safeguards [4].

Legislatively, the European Union has taken a stringent approach. The newly enacted AI Act (Regulation EU 2024/1689) classifies the use of real-time remote biometric identification in publicly accessible spaces as an "unacceptable risk," effectively banning it for law enforcement purposes, with only a few narrowly defined, strictly limited exceptions that require prior judicial authorization [3]. Any data collected beyond these strict purposes must be immediately destroyed to prevent unauthorized surveillance [10].

CONCLUSION: Facial recognition technology undoubtedly offers powerful capabilities for maintaining public security. However, national security imperatives cannot serve as a blanket justification for the erosion of constitutional privacy rights. Based on the comparative analysis, the following criteria are recommended for implementation into the legal framework of the Republic of Uzbekistan:

Strict Legal Basis: The deployment of 1:N FRT in public spaces must be explicitly regulated by parliamentary law.

Purpose Limitation: Mass, untargeted biometric scanning should be prohibited. FRT should only be authorized for investigating serious felonies based on reasonable suspicion.

Mandatory Human Oversight: AI-generated biometric matches must never serve as the sole basis for an arrest; human verification is legally mandatory.
Strict Data Retention: Biometric data of individuals who generate a "no-match" result must be deleted instantaneously.
Judicial Authorization: Deploying real-time facial recognition in public areas must require a prior warrant from a judicial authority.
By codifying these safeguards, the state can utilize technological advancements for public safety while preserving the foundational human right to privacy.

REFERENCES

1. Constitution of the Republic of Uzbekistan. (2023). Article 31. Tashkent: "Uzbekistan".
2. Law of the Republic of Uzbekistan No. ZRU-547 "On Personal Data". (2019, July 2). National Database of Legislation.
3. European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series, 1-145.
4. European Court of Human Rights. (2023). Case of Glukhin v. Russia (Application no. 11519/20). Judgment of 4 July 2023.
5. European Court of Human Rights. (2008). Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04). Judgment of 4 December 2008.
6. National Institute of Standards and Technology (NIST). (2022). Face Recognition Technology Evaluation (FRTE): Demographic Effects (NISTIR 8280). US Department of Commerce.
7. European Data Protection Board (EDPB). (2022). Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Brussels.
8. Purshouse, C., & Campbell, A. (2021). "Privacy, facial recognition technology and law enforcement". The Cambridge Law Journal, 80(3), 421-449.
9. Solove, D. J. (2008). Understanding Privacy. Harvard University Press.
10. Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Strasbourg.