

**Jandarma ve Sahil Güvenlik Akademisi**

**Güvenlik Bilimleri Enstitüsü**

**Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, 184-204**

**doi: 10.28956/gbd.1683533**

*Gendarmerie and Coast Guard Academy*

*Institute of Security Sciences*

*Journal of Security Sciences, Thematic Issue on Policing Practices and Security Technologies 184-204*

*Doi: 10.28956/gbd.1683533*

**Makale Türü ve Başlığı / Article Type and Title**

Derleme / Review Article

The Ethical Dimensions of Law Enforcement's Use of Facial Recognition Technology

Kolluk Kuvvetlerinin Yüz Tanıma Teknolojisini Kullanmasının Etik Boyutları

**Yazar(lar) / Writer(s)**

Müslüm KAYACI, Dr. Öğretim Üyesi, Dicle Üniversitesi İktisadi ve İdari Bilimler Fakültesi SBKY Bölümü, muslumkayaci@gmail.com ORCID: 0000-0002-6065-2734

**Bilgilendirme / Acknowledgement:**

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:

-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.

-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.

This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 25.04.2025

Makale Kabul Tarihi / Accepted : 09.10.2025

**Atıf Bilgisi / Citation:**

Kayacı M., (2025). The Ethical Dimensions Of Law Enforcement's Use Of Facial Recognition Technology, *Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı*, ss 184-204 doi: 10.28956/gbd.1683533

## THE ETHICAL DIMENSIONS OF LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

### Abstract

The purpose of this conceptual study is to comprehensively examine the ethical issues arising from the use of Facial Recognition Technology (FRT) and Artificial Intelligence (AI)-based security applications by law enforcement agencies. Without disregarding the opportunities offered by technological tools in ensuring public security and preventing crime, this study aims to discuss these tools' relationship with ethical concerns such as individual privacy, the risk of discrimination, the feeling of pervasive surveillance, transparency, and accountability. Conducted as a general review of the literature, this work seeks to provide a holistic assessment of how technological advancements like FRT can be implemented ethically in law enforcement services, emphasizing that liberties must not be overlooked while ensuring security. In this regard, the study also puts forward guiding recommendations for managing this complex relationship in a balanced manner. The study concludes that while law enforcement agencies collect individuals' facial biometric data for legitimate public purposes, such as maintaining public order and security, preventing crime, and tracking criminals, it has also been determined that this data can lead to erroneous and unethical practices for a variety of reasons.

**Keywords:** Facial Recognition Technology, Law Enforcement, Artificial Intelligence, Algorithm

## KOLLUK KUVVETLERİNİN YÜZ TANIMA TEKNOLOJİSİNİ KULLANMASININ ETİK BOYUTLARI

### Öz

Bu kavramsal çalışmanın amacı, 'Yüz Tanıma Teknolojisi' (YTT) ve yapay zekâ (YZ) tabanlı güvenlik uygulamalarının kolluk kuvvetleri tarafından kullanımı bağlamında ortaya çıkan etik sorunları kapsamlı bir şekilde incelemektir. Çalışma; kamu güvenliğinin sağlanmasında, suç işlenmesinin önlenmesinde, teknolojik araçların sunduğu fırsatları göz ardı etmeden bu araçların bireysel mahremiyet, ayrımcılık riski, yaygın gözetim hissi, şeffaflık ve hesap verebilirlik gibi etik meselelerle olan ilişkisini tartışmayı hedeflemektedir. Literatürün genel bir incelemesi şeklinde yürütülen bu derleme, kolluk hizmetlerinde YTT gibi teknolojik ilerlemelerin etik sorumlulukla uyumlu biçimde nasıl hayata geçirilebileceğine ve güvenlik sağlanırken özgürlüklerin de göz ardı edilmemesi gerektiğine dair bütüncül bir değerlendirme sunmayı amaçlamaktadır. Bu yönüyle çalışma, bu karmaşık ilişkinin dengeli bir şekilde yönetilmesi için rehber niteliğinde öneriler de ortaya atmaktadır. Kolluk kuvvetlerince kamu düzeni ve güvenliğinin sağlanması, suç işlenmesinin önlenmesi, suçluların takibi gibi meşru kamusal amaçlarla bireylerin yüzlerine ait biyometrik verilerin toplandığı sonucuna ulaşılmış ancak bu verilerin birtakım nedenlerle hatalı ve etik dışı uygulamalara kapı aralayacağı tespit edilmiştir.

**Anahtar Kelimeler:** Yüz tanıma teknolojisi, kolluk kuvvetleri, etik, yapay zekâ, algoritma

## **INTRODUCTION**

In order to ensure public security and develop more effective methods in the fight against crime, law enforcement agencies closely follow technological developments and implement innovative solutions to enhance their operational capacity. In this context, a wide range of digital technologies, from surveillance systems to unmanned aerial vehicles, have begun to be used in the field of security in recent years. Facial recognition technology (FRT) has emerged as one of the most prominent elements of this transformation among these. However, the use of such technologies in public security services should be addressed not only from a benefit-oriented perspective but also in light of ethical principles. While FRT provides law enforcement with significant advantages through functions such as identity verification, crime prevention, and tracking of offenders, it also entails various ethical risks, including the violation of individual privacy, the feeling of living under constant surveillance, and the possibility of false matches. Questions regarding how the data obtained through technological tools is collected, processed, and used give rise to serious ethical debates. Moreover, the risk that elements reflecting social diversity, such as cultural differences, forms of identity, and socioeconomic inequalities, may be reproduced in a biased manner by FRT systems. This situation necessitates that these systems should be evaluated not only in terms of their technical capabilities but also within the framework of ethical responsibility.

When using FRT and other artificial intelligence (AI)-based applications, law enforcement must both consider operational efficiency and fundamental rights and freedoms. Particularly the right to privacy and individual autonomy should be considered. Therefore, it is of great importance that the state and law enforcement agencies bear ethical responsibilities throughout all processes, from the selection to the implementation of these technologies, and ensuring accountability in these processes. The lack of ethical oversight mechanisms can lead to serious risks, such as the violation of individuals' privacy rights, the reproduction of discrimination, and the erosion of trust in public authority. In this context, it is essential to develop a balanced approach between ensuring security and adhering to ethical principles.

The present study seeks to conduct a conceptual analysis of the ethical challenges associated with law enforcement deployment of facial recognition technology and AI-based security systems. While acknowledging the potential contributions of technological advancements in ensuring public safety and

preventing crime, the study also focuses on the tension between these applications and fundamental ethical principles, such as violations of individual privacy, the risk of discrimination, the feeling of constant surveillance, lack of transparency, and accountability. Based on existing literature, the analysis aims to provide a holistic perspective on how security technologies can be structured in alignment with societal values. In this context, the study first explains what FRT is and then examines the areas in which it is used and the benefits for law enforcement agencies. Subsequently, the ethical aspects of FRT usage are discussed comprehensively. Finally, the study concludes with the results and the recommendations.

## **1. FACIAL RECOGNITION TECHNOLOGY**

The first steps toward FRT were taken in the 19th century when law enforcement agencies began using manual identification methods based on facial images to determine individuals' identities. These practices became an indispensable part of various security procedures, such as tracking criminals, identity verification, and establishing record systems over time. In the 21st century, with the accelerating pace of technological advancements and the development of AI-based systems, a qualitative transformation and a revolution, has occurred in facial recognition processes. “Especially, during the last five years, it has emerged as one of the most flourishing research topic among image processing, computer vision, machine learning, artificial intelligence and visual surveillance due to broad social, scientific and commercial applications” (Ali, Tian, Din, Iradukunda, and Khan, 2021, p. 4826). During this period, alongside technological advancements, the identification and analysis of physical characteristics—such as facial features, nose size, mouth structure, and eyebrow thickness—along with individuals' demographic information, have become significantly more accessible. Consequently, it is now possible to identify and track individuals with a high degree of accuracy.

Facial recognition is a method for identifying individuals and is based on capturing a person's facial features, converting them into digital data, and using this data for identity verification through systematic analysis (Almeida, Shmarko, and Lomas, 2022, p. 378). Biometric facial recognition is a type of AI technique that involves the automatic extraction, digitization, and comparison of the spatial and geometric distribution of facial features to identify individuals. By using a digital photograph of a person's face, a geometric model of the position of facial features is converted into a digital template, and an algorithm

compares this facial image with images stored in a database in this technique (Smith and Miller, 2022, pp. 167-168). In other words, FRT uses computer algorithms to select specific and distinctive details of a person's face from a photograph, a series of photographs, or a video segment. Details such as the distance between the eyes or the shape of the jaw are converted into a mathematical representation and compared with data from other faces previously collected and stored in a facial recognition database. The data associated with a specific face is typically referred to as a 'facial template'. A facial template differs from a photograph because it is designed to contain only specific details that can be used to distinguish one face from another (Lynch, 2018, p. 5). Images can be collected from passport, ID, or driver's license photos, as well as from the numerous images uploaded to social media sites and the Internet. Additionally, security cameras and other surveillance systems enrich databases by recording facial images of individuals in public spaces.

Face recognition is "the ability to establish a subject's identity based on his facial characteristics" (Jain, Klare, and Park, 2011, p. 726). This process occurs in a three-stage structure; face detection, feature extraction, and facial recognition (Zhao, Chellappa, Phillips, and Rosenfeld, 2003, p. 406). In the first stage, the system processes a visual data source to detect human faces; accordingly, regions containing faces are automatically identified. In the second stage, distinctive anatomical features are extracted from the detected face; characteristic points of the face, such as the position of the eyes, the structure of the nose, and the jawline, are digitally analyzed and undergo a systematic encoding process. In the final stage, this encoded facial data is compared with patterns in existing databases to identify or verify an individual's identity (Kortli, Jridi, Falou, and Atri, 2020, p. 3).

Facial recognition stands out as one of the most important components of AI-powered surveillance systems. Surveillance generally refers to the close monitoring and tracking of an individual, such as a criminal or a suspect. In this context, FRT has the most widespread application, particularly in security-related purposes. These developed systems are used with the aim of enhancing security in areas with high human traffic, both in open and closed spaces (Ali et al., 2021, p. 4834). Facial recognition-based surveillance systems applied in locations such as airport terminals, public squares, financial institutions, and border checkpoints that enable real-time monitoring of crowded environments and allow the rapid detection of potential threats. FRT is considered an almost

indispensable tool for law enforcement investigations in these days (Jain et al., 2011, p. 726).

## **2. AREAS OF USE AND BENEFITS OF FRT BY LAW ENFORCEMENT UNITS**

Today, FRT is utilized by law enforcement agencies for two primary functions: verifying a claimed identity (face verification) or identifying an unknown face (face identification) (Jones, 2021, p. 783). Law enforcement units employ FRT in various areas, including criminal detection, locating missing persons, ensuring public safety, and securing borders.

One of the most fundamental uses of facial recognition technology (FRT) for law enforcement units is in the identification of criminals. The strength of FRT lies in its ability to compare a large number of images in a short period of time (IJIS and IACP, 2019, p. 17). These systems can analyze images obtained from security cameras or other video sources and match them with profiles of suspects or criminals in a database. For example, the identity of a criminal can be quickly determined from images captured in an airport or a crowded public area. This provides a significant advantage to law enforcement, particularly in real-time situations. This speed becomes even more crucial in emergency situations, such as during a terrorist threat or the pursuit of a fugitive. FRT not only verifies the identity of individuals, but also allows for searches within large databases to be tracked previously recorded criminals. This enhances the operational efficiency of law enforcement units and provides a more effective approach to combat crime (Peterson, Jackson, Woods, and Treyger, 2023, p. 1)

FRT is also an effective tool in ensuring public security. The concept of security can hold different meanings at various levels. For example, national security aims to prevent harm to the public from events such as terrorist attacks. Community safety endeavors to prevent the disruption of law and order. In contrast, organizational security is dedicated to safeguarding an institution's confidential information and implementing measures against abuse or other illicit activities. In some cases, security refers to personal physical safety (Smith and Miller, 2022, p. 173). Public safety encompasses all measures aimed at protecting the general order, peace, and security of the society. The prevention of crime, response to emergencies, and ensuring the safety of lives and property are fundamental elements of this concept. Law enforcement agencies generally play an active role in ensuring public safety, and maintaining public security

stands as one of the most common applications of FRT within their units. Large-scale events, such as national or international festivals, sporting events, and crowded stations, often carry high security risks. Facial recognition systems can be used to detect potential threats among crowds at such events or locations (Lynch, 2018, p. 6). For example, in a stadium or concert venue, when the system detects an individual from a watchlist, law enforcement can take immediate action. This provides a proactive security approach and prevents potential crimes before they occur.

Border security is another area where FRT is extensively utilized by law enforcement units. This technology is employed to verify passenger identities and prevent illegal entries in international airports and border crossings (Ali et al., 2021, p. 4834). For example, facial recognition systems integrated with biometric passports quickly verify travelers' identities and enhance security while reducing waiting times. On the other hand, these systems scan a traveler's face, matching it with the information in their passport or other identification documents. In case of any inconsistencies, law enforcement units are alerted. This plays a crucial role, especially in combating international criminal networks.

Another significant and socially important application of FRT is the identification of missing persons. These technologies are highly functional in swiftly and safely locating vulnerable groups, such as missing children, elderly individuals, or people with cognitive disabilities. For example, when a law enforcement officer encounters an individual who has lost their way, they can capture the person's facial image and have the ability to match this data with a central missing persons database (IJIS and IACP, 2019, p. 10).

Such a matching process enables the rapid identification of missing individuals and the activation of appropriate intervention mechanisms. Similarly, for individuals who are unable to identify themselves due to various reasons, such as those experiencing loss of consciousness or those who have lost the ability to speak, FRT offers significant advantages in identity identification. Additionally, facial recognition systems can be an effective tool in identifying unidentified deceased individuals in forensic cases.

In addition to these fundamental uses, FRT is also used by law enforcement agencies in various other areas and contexts (IJIS and IACP, 2019, pp. 10-16). For example, FRT can help identify individuals attempting to conceal their

identities. Some individuals may seek privileges using fraudulent identity documents; to prevent such deception, FRT can alert authorities and support the identification process. Photo arrays can be automatically generated by using the suspect's photograph and other biometric data. These arrays may then be prepared for use in identification procedures with witnesses or victims. The photographs of a known suspect can be searched in traditional photo databases or specialized sources such as social media and security camera records. These searches can help identify individuals who resemble the suspect. FRT can also be used to verify whether witnesses, victims, or suspects were present at a specific crime scene or had any associations with a particular suspect or group. When monitoring high-risk areas, locations with high crime rates, or hazardous zones, the photographs of wanted individuals can be compared against security camera footage. This can help identify potential matches. FRT can also be used to verify the identities of individuals taken into custody. Additionally, it plays a role in confirming the identity of inmates before temporary or permanent release. Some examples of the implementation of these technologies around the world are as follows: (1) In the UK, the Metropolitan Police and South Wales Police are deploying Live Facial Recognition systems in real-time within crowded public spaces (Oxley et. al., 2024). (2) The New York Police Department has been using FRT in criminal investigations since 2011 (O'Neill, 2019). (3) China is actively using FRT (Smith and Miller, 2022).

FRT presents remarkable potential, particularly in ensuring public security, due to its various benefits and positive attributes. As mentioned above, these technologies can be effectively used in many critical areas, such as identifying criminals, locating missing persons, and detecting potential threats in public spaces in advance. Thanks to advanced algorithms and AI-powered analysis systems, FRT enables faster and more systematic interventions in terms of public security, which significantly contributes to maintaining social order. However, the implementation and use of such powerful and widely applied technologies bring with them an important issue that must be carefully considered: ethical boundaries. While it is essential that the capabilities offered by technology are used to serve the public good, it is equally important to respect individuals' privacy, fundamental rights, and freedoms.

### **3. ETHICAL DIMENSIONS / BOUNDARIES**

AI-powered biometric systems, exemplified by FRT, are utilized across a broad spectrum, ranging from security and commerce to public surveillance and

individual identity verification. However, the rapid proliferation of these technologies has also brought significant ethical debates to the forefront, including concerns about privacy violations, racial and gender-based biases, transparency, consent, and informed use.

### **3.1. Privacy and Surveillance**

One of the most intensely debated aspects of FRT is the potential threats it poses to individuals' privacy rights. This technology can collect facial data without individuals' consent, and the biometric information in question can be processed for various purposes. Such applications, especially in public spaces, conducted without individuals' consent raise serious ethical concerns regarding the right to privacy. The risk of privacy violations increases as FRT becomes more widespread and pave the way for a societal structure where individuals are constantly under surveillance.

Although defining the concept of privacy clearly has never been an easy task, some fundamental elements can be highlighted within the general framework. Privacy can be considered a right that individuals hold in relation to other individuals, the state, and various organizations, and it takes shape around the following two dimensions: First, the acquisition of individuals' personal information, such as facial images and other biometric data, by third parties or institutions, and their storage in biometric databases. Secondly, the observation of individuals' behaviors, social relationships, and other private aspects by external actors, or their monitoring through surveillance systems that incorporate biometric facial recognition technologies (Smith and Miller, 2022, p. 171). In this context, personal privacy can be argued to represent the individual's right to control their own information without interference in their private life. Unauthorized use of biometric data violates this right, jeopardizing individuals' autonomy. Biometric samples can be collected either with or without the data owner's consent. For example, a data subject may knowingly and willingly present their biometric passport at a border, or their image may be recorded by a security camera without their awareness and without explicit consent (Ruhrmann, 2019, p. 24).

FRT, like other biometric systems, involves the collection, storage, sharing, and analysis of highly unique and sensitive personal information. Facial biometric data is an integral part of personal identity and carries a high security risk due to its immutable nature (Lynch, 2018, p. 7). Facial recognition systems

pose a higher level of privacy risk compared to other biometric technologies, as individuals have very limited ability to prevent the collection of such data. In daily life, people's faces are constantly visible in public spaces, and individuals frequently share these images on digital platforms, making them vulnerable to uncontrolled data collection. Under these conditions, remote identity recognition applications that can be conducted without individuals' knowledge or consent significantly weaken personal control over privacy and, in many cases, make it nearly impossible. Indeed, privacy is described as “one of the most significant and vital issues we face today” (Richards and King, 2014, p. 410).

The use of facial recognition technologies by governments and law enforcement agencies may lead to concerns among individuals about being under constant surveillance. The feeling of constant surveillance can reinforce individuals' tendency to censor their behavior, potentially creating profound impacts on both societal and individual freedoms. The concept of the Panopticon, as detailed in Michel Foucault's *Discipline and Punish* (2000), provides a powerful theoretical framework for analyzing this phenomenon. The Panopticon, conceived by philosopher Jeremy Bentham and drawn by architect Willey Reveley, was a prison design that enabled continuous surveillance of inmates from a central watchtower. Foucault interprets this structure not merely as a physical surveillance tool but as an internalized mechanism of power, where individuals, assuming they are constantly observed, voluntarily regulate their own behavior. In this context, the Panopticon serves as a symbolic representation of the modern surveillance society, which encourages self-regulation and a tendency to obey in individuals, even in the absence of actual oversight. The widespread use of FRT in public spaces and digital platforms today can be seen as a modern, technologically enhanced manifestation of the Panopticon metaphor. In this context, FRT can lead individuals to internalize the notion of being constantly monitored, prompting them to develop voluntary self-censorship in their behavior. This state of constant surveillance may heighten individuals' perceptions of threats to fundamental ethical values such as privacy and autonomy.

### **3.2. Algorithmic Bias and Discrimination**

The integration of AI technologies into decision-making processes offers various advantages, such as faster response times, cost efficiency, and improvements in service quality. However, the use of biometric-based systems

such as facial recognition within this framework also brings about significant ethical and security-related concerns. The increasing automation of decision-making processes and the growing complexity of the digital infrastructure that guides this operation raise various concerns regarding the reliability of algorithms. One of these concerns is the possibility that algorithms, much like humans, can carry biases and produce discriminatory outcomes. If not used carefully, algorithms can replicate existing patterns of discrimination, inherit biases from past decision-makers, or reflect prevalent societal prejudices. In some cases, they can even deepen existing inequalities by giving the impression that historically disadvantaged groups deserve more negative treatment (Barocas and Selbst, 2016, p. 674).

There are several reasons why algorithms can lead to bias and discrimination. Firstly, algorithms are artificial systems created through human intervention, and during this process, designers integrate specific assumptions, objectives, and value judgments into the system. Decisions regarding which data to use, which criteria to prioritize, and which output to consider as "correct" are not only technical but also reflect the value judgments and preferences of the designer. These value judgments and preferences determine how the algorithm operates and who will be placed in an advantageous or disadvantageous position. Algorithms used in sensitive social domains such as facial recognition may appear neutral but can systematically exclude or put certain groups in a disadvantage position. Therefore, the design and functionality of algorithms reflect the values of their designers and the intended areas of use (Mittelstadt, Allo, Taddeo, Wachter, and Floridi, 2016, p. 7). The designer's values, whether consciously or unconsciously, are embedded into the code, leading to the institutionalization of these values (Macnish, 2012, p. 158). Thus, it would not be incorrect to describe algorithmic bias and discrimination as a reality, where AI and data-driven technologies have the potential to produce biased outcomes in decision-making processes. Secondly, since algorithms are trained on historical data, they inherently carry the societal inequalities present in those datasets. While some groups may be underrepresented in training sets, others may be disproportionately emphasized (Buolamwini and Gebu, 2018, p. 78). Similarly, the overrepresentation of disadvantaged groups in datasets depicting violent behaviors or potential criminal activities (Pastaltzidis et al., 2022, p. 2303) leads algorithms to make systematic errors against certain identity groups. In FRT, lighter-skinned individuals are recognized accurately, whereas error rates increase significantly

for darker-skinned individuals. For instance, a visual tagging service reportedly classified a thermometer held by a lighter-skinned person as a ‘tool’, while identifying the same object in a darker-skinned hand as a ‘weapon’ (Wiggers, 2020). Disadvantaged groups are subjected to significantly higher levels of data collection compared to other groups when applying for public assistance, moving through heavily surveilled neighborhoods, accessing healthcare systems, or crossing national borders. These data further deepen existing inequalities by targeting these individuals as suspicious or subject to heightened scrutiny. Labeled as “undeserving” individuals, these groups become the focus of punitive public policies and intense surveillance. Consequently, the cycle of discrimination is continuously reinforced and becomes entrenched (Eubanks, 2018, p. 11). In the context of FRT, such practices give rise to serious ethical concerns as they can further deepen existing issues such as bias and discrimination. Particularly in critical decision-making areas like law enforcement, they carry the risk of facilitating significant human rights violations.

### **3.3. Transparency and Accountability**

Transparency refers to providing clarity on how FRT operates, what data is used, and how decision-making processes function. Accountability, on the other hand, involves determining who is responsible for the misuse or erroneous outcomes of these technologies and ensuring that responsibility is upheld. The transparency of FRT requires the clear documentation of algorithms and datasets. However, since FRT is developed by private companies, it is often characterized as a ‘black box’ (Diakopoulos, 2015; Von Eschenbach, 2021; Pasquale, 2015). Algorithms are often described as ‘black boxes’ because their complexity and lack of technical transparency render their inner workings obscure and ambiguous (Diakopoulos, 2015, p. 404). In the context of AI, the issue of algorithms functioning as black boxes refers to the inability to observe or understand a system’s or model’s internal workings and decision-making processes from the outside. This situation manifests as a problem of algorithmic interpretability (Burrell, 2016), along with challenges related to opacity and complexity (Pasquale, 2015, pp. 6–7). This problem, commonly encountered in machine learning and especially deep learning models, stems from the multi-layered architecture of these models and the complex relationships between inputs and outputs. These structural characteristics make it difficult to provide a clear and traceable justification for how the system arrives at a particular

outcome. Therefore, such models are often described as having a 'black box' nature. Given the increasing use of AI-based systems in highly sensitive domains such as security, healthcare, and public order, the transparency issue extends beyond a mere technical concern, evolving into an ethical and societal matter requiring urgent intervention (Von Eschenbach, 2021, p. 1608).

The characterization of algorithms as black boxes is fundamentally based on three main reasons: First, it stems from deliberate corporate secrecy practices maintained by system developers to protect intellectual property rights. Second, it arises from technical limitations due to the constraints of existing technological infrastructure and computational methods. Third, it is rooted in the high degree of inherent structural complexity and algorithmic autonomy found particularly in certain machine learning approaches, such as deep learning (Burrell, 2016, p. 3). When these three factors come together, they create a multi-layered transparency problem that significantly hinders the understanding and oversight of algorithmic inner workings. This aspect of AI is a frequently debated topic in the literature (see: Burrell, 2016; Diakopoulos, 2015; Von Eschenbach, 2021; Coglianese & Lehr, 2019; Etzioni & Etzioni, 2016) and it is worth to briefly address this debate without delving too deeply into the details.

*Strategic corporate confidentiality measures implemented to safeguard proprietary intellectual property rights:* The technical transparency of facial recognition systems requires a clear presentation of the operational mechanisms of the algorithms, the datasets used for training, and how various variables are evaluated throughout these processes (Almeida et al., 2022, p. 380). This kind of transparency is of great importance both for evaluating the system's performance and for identifying potential biases and systematic errors. However, many facial recognition systems avoid publicly sharing details about their algorithms and training data, citing trade secrets, intellectual property rights, and the need to maintain competitive advantage in practice (Engstrom, Ho, Sharkey, & Cuéllar, 2020, p. 89). Similarly, law enforcement agencies, as consumers in the facial recognition technology (FRT) market, often find themselves at the mercy of technology providers. This leads to law enforcement to be restricted to the solutions offered by the market, while vendors' inclination to protect their commercial interests creates an additional layer of secrecy that conflicts with principles of transparency and accountability within these agencies (Joh, 2017, p. 130). This closed structure makes it difficult to analyze the impact of systems on different demographic groups and to assess the risk of

discrimination, thereby restricting both scientific oversight and public accountability. Especially when such systems are used in public services and law enforcement, the lack of transparency can lead to significant ethical concerns.

*Technical limitations arising from the constraints of existing technological infrastructure and computational methods:* The black box nature of algorithmic systems can largely be explained by technical factors rooted in their structural complexity and their continuously evolving, dynamic nature (Burrell, 2016, p. 4). For certain algorithms, precisely determining the contribution of specific inputs to their outputs poses considerable challenges for both practitioners and regulatory actors. The analysis of these systems necessitates not only significant time and resource allocation but also specialized expertise and interdisciplinary technical knowledge (Coglianese and Lehr, 2019, p. 30). Advanced algorithmic models, such as machine learning and deep learning, rely on multi-layered data processing processes and complex mathematical operations, presenting an abstract structure that significantly complicates the task of tracing their decision-making logic. Such systems, while learning patterns within data, establish highly multidimensional networks of relationships that are beyond direct human comprehension. Additionally, their dynamic nature, continuously updating with real-time data streams and transforming their internal parameters over time, further limits the explainability and traceability of their inner workings (Etzioni and Etzioni, 2016, p. 138). The use of AI technologies with such technical limitations by law enforcement in public spaces introduces serious risks, including arbitrary intervention, discrimination, and misidentification. This, in turn, undermines the balance between justice, accountability, and security. Hence, the use of facial recognition systems should be addressed not only on the basis of technical efficiency but also in light of ethical principles such as transparency.

*Algorithmic autonomy:* Algorithmic autonomy can be defined as the ability of machine learning models to evolve over time by learning from the data they acquire and the outputs they generate. Although these systems are initially programmed by humans, they do not operate based on fixed, predefined rules. Instead, they extract patterns from large datasets and they autonomously develop their decision-making processes based on these inferences (Burrell, 2016). Unlike traditional software systems, these algorithms do not operate based on fixed rules; instead, they learn from datasets, continuously updating

their model structures and refining their decision-making mechanisms accordingly. Machine learning and deep learning methods, as the fundamental tools of this process, enable systems to continuously adapt to new data (LeCun, Bengio, and Hinton, 2015). In other words, AI applications can eventually learn on their own. The use of FRT by law enforcement agencies carries significant ethical risks due to the algorithms continuously evolving over time as they are fed with data. This evolutionary process can lead to a lack of transparency in algorithmic decision-making mechanisms, thereby increasing the risk of potential discrimination and erroneous decisions.

The use of AI-based FRT by law enforcement carries particular significance in terms of adherence to ethical principles and accountability, as it operates in a domain where public authority is directly exercised over individuals. In this context, ensuring transparency regarding how algorithms operate, what data they are trained on, and the basis of their decision-making processes is not only a technical necessity but also a reflection of the rule of law in democratic societies. Transparency, by ensuring that the mechanisms behind decisions affecting individuals' fundamental rights and freedoms are understandable, enables accountability for both citizens and oversight institutions. As mentioned above, such systems can learn and reproduce biases present in datasets. If information about how the system operates is not publicly available, detecting and addressing discriminatory practices becomes nearly impossible. For example, findings regarding biases in FRT against marginalized or disadvantaged groups have been revealed through transparency. Therefore, ensuring that algorithmic decision-making processes are auditable and subject to reassessment is essential for both the establishment of justice and the construction of public trust. Transparency enables the protection of individuals' rights and the provision of fair practices by making the decision-making processes of algorithmic systems visible and understandable. In this regard, it is not merely a technical design choice but also forms the foundation of public responsibility and ethical accountability. In this context, when facial recognition systems do not openly disclose the datasets they are trained on, the conditions under which they operate, and the processes behind their decision-making, erroneous matches or biased outcomes can lead to serious ethical consequences. Therefore, transparency is an indispensable prerequisite for law enforcement agencies to use these technologies in a responsible, legitimate manner that does not undermine public trust.

## **CONCLUSION**

The collection of biometric data, particularly through FRT, is a complex issue at the center of ethical, legal, and political debates in modern societies. While these technologies necessitate the collection of individuals' biometric data for legitimate public purposes such as public order, national security, and the efficiency of government services, they can also conflict with democratic values such as individual privacy, personal data protection, and autonomy. In fact, the long-standing freedom-security dilemma lies at the core of this tension. The freedom-security dilemma refers to the delicate balance between protecting individuals' fundamental rights and freedoms and ensuring public order and security. States have the authority to restrict certain individual freedoms in order to ensure public security. However, these limitations must be legitimate, proportionate, and legally justified. In the context of FRT, the freedom-security dilemma raises concerns about intrusions into individual privacy in the name of enhancing security in public spaces. While states use these technologies for legitimate reasons such as crime prevention and maintaining public order, principles such as respect for individuals' privacy, data security, and consent can often be sidelined. This situation poses the risk of excessively restricting freedoms in democratic regimes in the name of security. Therefore, the use of FRT should be considered within the framework of purpose suitability, proportionality, and accountability principles.

FRT, by its very nature, relies on individuals' unique and immutable biometric data, particularly facial data. Unlike ordinary personal data, such information cannot be anonymized, and once recorded, it is exceedingly difficult to erase or render ineffective. Such a characteristic can pave the way for serious violations of individuals' right to privacy. Privacy is a core value in contemporary ethical theories, encompassing an individual's right to define and limit their own autonomous space. FRT blurs the distinction between public and private spaces, exposing individuals' subjectivity and presence in public life to constant surveillance. Especially in cases where individuals' explicit and informed consent is not obtained, their rights over data control are eliminated, and they are unknowingly incorporated into surveillance processes. Additionally, FRT has been found to contain systematic errors across different demographic groups. Error rates have been shown to increase significantly, particularly for socially disadvantaged groups such as women, older individuals, and ethnic minorities. Such technological biases perpetuate systemic

discrimination, posing serious ethical risks. Therefore, it is crucial for law enforcement to be aware of these biases and ethical violations when using FRT and to carry out their duties with this awareness.

Finally, a set of recommendations/advice/principles centered on the ethical use of FRT by law enforcement can be outlined as follows: (1) The use of FRT should be based solely on legitimate, proportionate, and necessary security justifications; mass surveillance for arbitrary and unsubstantiated purposes must not be conducted. (2) Only the necessary data should be collected and processed; unnecessary facial images or biometric data should not be recorded. (3) Biases based on gender, age, origin, and socioeconomic status must be prevented, and to this end, systems should be regularly tested for fairness and equity. (4) Law enforcement agencies should transparently share when, where, and how FRT is used with the public. (5) The operational processes of these systems should be regularly monitored and audited by independent oversight bodies. (6) Collected facial data should be safeguarded according to high security standards to minimize the risks of unauthorized access, leaks, and misuse. (7) Collected data should be used solely for the designated security purpose and must not be repurposed for other uses, such as commercial or political objectives. (8) Individuals should be informed about areas where FRT is used, and whenever possible, their voluntary consent should be obtained. (9) Public authorities should be held accountable for any harm caused by misidentification or recognition errors in FRT, and redress mechanisms should be developed. (10) Facial data should be retained only for the necessary duration and securely deleted thereafter. (11) Law enforcement agencies should be accountable to the public and oversight bodies for all decisions and implementations related to the use of this technology. (12) Law enforcement personnel should receive regular training on the ethical, technical, and legal dimensions of FRT to ensure that they understand its limitations and risks.

## REFERENCES

- Ali, W. Tian, W. Din, S. U. Iradukunda, D. and Khan, A. A. (2021). Classical and modern face recognition approaches: a complete review. *Multimedia Tools and Applications*, 80, 4825-4880. <https://doi.org/10.1007/s11042-020-09850-1>
- Almeida, D. Shmarko, K. and Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), 377-387. <https://doi.org/10.1007/s43681-021-00077-w>
- Barocas, S. and Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671-732.
- Buolamwini, J. and Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency (pp. 77-91). <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> (12.03.2025).
- Burrell, J. (2016). How the machine ‘thinks’: understanding opacity in machine learning algorithms, *Big Data and Society*, 3(1), 1-12. DOI: 10.1177/2053951715622512
- Coglianese, C. and Lehr, D. (2019). Transparency and algorithmic governance, *Administrative Law Review*, 71(1), 1-56.
- Diakopoulos, N. (2015). Algorithmic accountability: journalistic investigation of computational power structures, *Digital Journalism*, 3(3), 398-415. DOI: 10.1080/21670811.2014.976411
- Engstrom, D. F. Ho, D. E. Sharkey, C. M. and Cuéllar, M. F. (2020). Government by algorithm: artificial intelligence in federal administrative agencies. NYU School of Law, Public Law Research Paper, (pp. 20-54).
- Etzioni, A. ve Etzioni, O. (2016), Keeping AI legal, *Vanderbilt Journal of Entertainment and Technology Law*, 19(1), 133-146.
- Eubanks, V. (2018). Automating inequality: how high-tech tools profile, police, and punish the poor. New York: St. Martin's Press.

- Foucault, M. (2000). Hapishanenin doğuşu. (2. Basım), (Çev. M. A. Kılıçbay), İstanbul: İmge Yayınları.
- Gates, K. A. (2011). Our biometric future: Facial recognition technology and the culture of surveillance. New York: New York University Press.
- International Justice and Public Safety Network (IJIS), & International Association of Chiefs of Police (IACP). (2019). Facial recognition use case catalogue (LEITTF White Paper). [https://www.theiacp.org/sites/default/files/2019-10/IJIS\\_IACP%20WP\\_LEITTF\\_Facial%20Recognition%20UseCasesRpt\\_20190322.pdf](https://www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf) (15.03.2025)
- Jain, A. K. Klare, B. and Park, U. (2011). Face recognition: Some challenges in forensics. In 2011 IEEE International Conference on Automatic Face and Gesture Recognition. (pp. 726-733).
- Joh, E. E. (2017). The undue influence of surveillance technology companies on policing. *New York University Law Review*, 92, 101–130.
- Jones, C. (2021). Law enforcement use of facial recognition: bias, disparate impacts on people of color, and the need for federal legislation. *North Carolina Journal of Law and Technology*, 22(4), 777-816.
- Kortli, Y. Jridi, M. Al Falou, A. and Atri, M. (2020). Face recognition systems: A survey. *Sensors*, 20(2), 1-36. <https://doi.org/10.3390/s20020342>
- LeCun, Y. Bengio, Y. ve Hinton, G. (2015). Deep Learning, *Nature*, 521(7553), 436-444.
- Lynch J. (2018). Face off: Law enforcement use of face recognition technology. Electronic Frontier Foundation. [https://www.eff.org/files/2020/04/20/face-offreport-2020\\_1.pdf](https://www.eff.org/files/2020/04/20/face-offreport-2020_1.pdf) (30.03.2025)
- Macnish, K. (2012). Unblinking eyes: the ethics of automating surveillance. *Ethics and Information Technology*, 14(2), 151-167. DOI 10.1007/s10676-012-9291-0
- Mann, M. and Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal*, 40(1), 121-145.
- Mittelstadt, B. D. Allo, P. Taddeo, M. Wachter, S. and Floridi, L. (2016). The ethics of algorithms: mapping the debate. *Big Data and Society*, 3(2), 1-21. DOI: 10.1177/2053951716679679

- O'Neill, J. (2019). How facial recognition makes you safer. <https://ebac2018.sites.pomona.edu/classes/cs181s/2020fa/lectures/14-privacy/NYT-ONeill.pdf> (23.07.2025).
- Oxley, G. Uwazuruike, A. Lalic, M. Samuel, H. Downs, W. (2024). Police use of live facial recognition technology. <https://researchbriefings.files.parliament.uk/documents/CDP-2024-0144/CDP-2024-0144.pdf> (23.07.2025).
- Pasquale, F. (2015), *The black box society: the secret algorithms that control money and information*, Cambridge, Massachusetts: Harvard University Press.
- Pastaltzidis, I. Dimitriou, N. Quezada-Tavarez, K. Aidinlis, S. Marquenie, T. Gurzawska, A. and Tzovaras, D. (2022). Data augmentation for fairness-aware machine learning: Preventing algorithmic bias in law enforcement systems. In *Proceedings of the 2022 ACM conference on fairness, accountability, and transparency* (pp. 2302-2314).
- Peterson, S, Jackson, B. A. Woods, D. and Treyger, E. (2023). Finding a broadly practical approach for regulating the use of facial recognition by Law Enforcement. [https://www.rand.org/content/dam/rand/pubs/research\\_reports/RRA2200/RR A2249-1/RAND\\_RRA2249-1.pdf](https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2200/RR A2249-1/RAND_RRA2249-1.pdf) (15.03.2025).
- Richards, N. M. and King, J. H. (2014). Big data ethics. *Wake Forest Law Review*, 49(2), 393-432.
- Ruhrmann, H. (2019). Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement. [https://discovery.ucl.ac.uk/id/eprint/10148887/1/Facing-the-Future\\_Ruhrmann\\_CITRIS-Policy-Lab.pdf](https://discovery.ucl.ac.uk/id/eprint/10148887/1/Facing-the-Future_Ruhrmann_CITRIS-Policy-Lab.pdf) (25.03.2025).
- Smith, M. and Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI and Society*, 37(1), 167-175. <https://doi.org/10.1007/s00146-021-01199-9>
- Von Eschenbach, W. J. (2021). Transparency and the black box problem: why we do not trust AI, *Philosophy and Technology*, 34(4), 1607-1622. <https://doi.org/10.1007/s13347-021-00477-0>
- Wiggers, K. (2020). Researchers show that computer vision algorithms pretrained on ImageNet exhibit multiple, distressing biases.

<https://venturebeat.com/business/researchers-show-that-computer-vision-algorithms-pretrained-on-imagenet-exhibit-multiple-distressing-biases/>  
(25.03.2025)

Zhao, W. Chellappa, R. Phillips, P. J. and Rosenfeld, A. (2003). Face recognition: a literature survey. *ACM Computing Surveys*, 35(4), 399-458.