

Vladimir Medović*
Marijana Mladenov**
Milena Galetin***

Originalni naučni rad
UDK 342.7:(004.8+57.087.1)(497.11)(4-672EU)
doi: <https://doi.org/10.56461/rep280126.01.M>

FACE RECOGNITION: EU LEGAL APPROACH AND SERBIAN LEGAL APPROACH****

Abstract

The use of facial recognition technology is a very current topic that raises issues of human rights protection in this process. In the paper, after the introduction, the authors analyse legal framework in the European Union regarding the use of this technology, which is closely related to the protection of personal data, right to privacy and artificial intelligence, and the jurisprudence of the European Court of Human Rights, thereafter. The Serbian legal approach related to this issue is presented in a separate chapter. Finally, considering that the use of facial recognition technology in Serbia has no legal basis, in the concluding remarks the authors indicate in which direction Serbian legislator should act, in order to meet the established standards of human rights protection. Methods characteristic of social sciences – normative, positive law, comparative and case law analysis – are used in the paper.

Keywords: face recognition, biometric data, GDPR, AI Act, jurisprudence of the ECtHR.

* Full Professor, Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, Serbia, e-mail: vladimir.medovic@pravni-fakultet.info, ORCID: <https://orcid.org/0000-0001-5709-1538>

** Associate Professor, Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, Serbia, e-mail: alavuk@pravni-fakultet.info, ORCID: <https://orcid.org/0000-0002-4574-5159>

*** Associate Professor, Faculty of Law for Commerce and Judiciary in Novi Sad, University Business Academy in Novi Sad, Serbia, e-mail: milena.galetin@pravni-fakultet.info, ORCID: <https://orcid.org/0000-0002-1489-6050>

**** The paper is the result within the Jean Monnet Module “Application of EU values and digital transformation: Serbian perspective” (EUDIGVAL), funded by the European Union (ERASMUS-JMO-2024-HEI-TCH-RSCH, project number: 101175838). Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or the granting authority (European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

I Introduction

How to establish the fine balance between needs for public safety and security on one side and individual rights and freedoms on other side? This is the crucial issue which is subject to everlasting debates in democratic societies. The development of facial recognition technologies has reinvigorated this long-standing debate. When does the use of these technologies become means of mass surveillance rather than a tool for public safety? Where is the borderline between the legitimate interest in preventing and fighting crime and respect for individual rights and freedoms? Facial recognition technologies are a specific type of biometric technologies which are used for different purposes, ranging from the simple detection of the presence of a face in an image, to more complex such as verification, identification, and categorization or classification of individuals. These technologies are currently used by public and private actors for different purposes. While facial recognition systems have obvious benefits for public safety and security their pervasiveness and intrusiveness give rise to serious concerns with regard to fundamental rights and freedoms such as right to privacy, protection of personal data, freedom of assembly, freedom of association, freedom of expression. The European Union has comprehensive set of rules in order to regulate the use of facial recognition technologies. It adopted new legislation such as General Data Protection Regulation, Law Enforcement Directive, and AI Act to deal with this issue.

In the following sections of this article, we will present and analyze the EU legal framework for the protection of human rights, as well as legal rules concerning the use of the facial recognition technologies. We will also review the jurisprudence of the European Court of Human Rights, considering that European Convention for Protection of Human Rights and Fundamental Freedoms is part of the EU's legal acquis. A review of Serbian legislation regarding this issue is also presented in this paper. Finally, we will try to determine whether the existing legal framework is adequate and sufficient to prevent potential risks arising from the use of the facial recognition technology systems.

II Face recognition: EU legal framework

1. General legal framework for the protection of human rights

The European Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are com-

mon to the Member States, which are obliged to respect them. The EU Charter of Fundamental Rights is the most important legal document that consolidates and articulates the fundamental rights and freedoms that are protected within the European Union. The Charter was solemnly proclaimed on 7 December 2000 in Nice. It became part of EU primary law and legally binding with the Treaty of Lisbon in 2009. According to Article 6(1) of the Treaty on the European Union (TEU), the Charter has the same legal value as the Treaties. The Charter is addressed to the institutions, bodies and agencies of the EU and to the Member States when they are implementing the EU law. Apart from the Charter, in accordance with Article 6(3) of the TEU, the EU and the Member States are obliged to observe the fundamental rights, as guaranteed by the European Convention on the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, as a part of the general principles of the EU.

Considering that many of the provisions of the EU Charter are identical to the provisions of the ECHR, Article 52(3) of the Charter defines the relationship between these two legal documents. In order to ensure consistent interpretation, this article provides that the scope and the meaning of the rights contained in the Charter, which correspond to the rights guaranteed by the ECHR, shall be the same as those laid down by the later. This provision shall not prevent the EU law providing more extensive protection.

Similar rules apply to the rights and freedoms guaranteed by the Charter which results from the constitutional traditions common to the Member States. Those rights shall be interpreted in harmony with these traditions.¹

Fundamental rights and freedoms contained in the EU Charter and European convention are also applicable in the digital environment. On 23 January 2023, the European Commission, the Council of the EU and the European Parliament proclaimed joint Declaration on Digital Rights and Principles for the Digital Decade.² With this Declaration the EU spells out how its values and fundamental rights should be applied in the digital environment. According to the Declaration, digital transformation should not entail regression of the rights. It set out general principle that “what is illegal offline, is illegal online”.³

¹ Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities* C 346, 18.12.2000, Article 52(4).

² European Declaration on Digital Rights and Principles for the Digital Decade, *Official Journal of the European Union*, C23/1, 23.1.2023.

³ *Ibid.*, paragraph 3 of the Preamble.

The use of facial recognition technologies might pose the risk of adverse impact on fundamental human rights and freedoms guaranteed under the EU law, such as freedom of assembly, freedom of association, and freedom of expression that are the key elements of democracy. However, the rights which might be most affected are the right to privacy and right to protection of personal data. For example, indiscriminate mass surveillance could make it impossible to move anonymously in public space and lead to conformism detrimental to free will. The risk of misuse of the data collected by the facial recognition systems is also high. How this data will be processed and for what purposes, who will have access to it are some of the questions which must be addressed.

2. Specific legal framework: right to privacy and right to protection of personal data

The existing legal framework addresses some of the issues raised by the potential use of facial recognition systems. Article 7 of the Charter of Fundamental Rights provides that everyone has the right to respect for his private and family life, home and communications. On the other hand, the right to protection of personal data is enshrined in the Treaty on the Functioning of the EU (TFEU). According to Article 16 TFEU, everyone has the right to the protection of personal data concerning them. This right is further elaborated in Article 8 of the Charter, which provides that everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly, for specified purposes, and on the basis of the consent of the persons concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

In order to provide further protection of the rights established by the Treaty on the Functioning of the EU and the EU Charter of Fundamental Rights, the Union has adopted a range of legislative acts. The issue of protection of personal data is regulated by the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) adopted on 27 April 2016.⁴ The Regulation lays down the rules relating to the protection of natural

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), *OJ L 119*, 4.5.2016.

persons with regard to the processing of personal data and rules relating to the free movement of personal data.⁵ It applies to the processing of personal data wholly or partly by automated means and to processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.⁶

The Regulation sets out the principles that apply to the processing of personal data. According to Article 5(1) of the Regulation, personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

As a general rule, the processing of personal data is lawful if the data subject has given consent to his or her personal data for one or more specific purposes. Without such consent, the processing is lawful if it is in order to protect the vital interest of the data subject or of another natural person or if it is necessary for the purpose of the legitimate interests pursued by the controller or by third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is child.⁷

The European Union and the Member States may, by way of a legislative measures, restrict the scope of rights and obligations provided by the provisions of

⁵ GDPR, Article 1(1).

⁶ GDPR, Article 2(1).

⁷ GDPR, Article 6(1).

Regulation when such restrictions respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: national security, defense, public security, the prevention, investigation, or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.⁸

The European Parliament and the Council also adopted the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data (Law Enforcement Directive) on 27 April 2016.⁹ Although both General Data Protection Regulation and Law Enforcement Directive apply to automated processing of personal data and to manual processing forming part of filing system, the Directive is more specific in scope and applies to cases where the personal data are collected and processed by law enforcement agencies for the purpose of the prevention, investigation and prosecution of criminal offences. However, data processing by law enforcement agencies is subject to the same principles set out by Article 5 of the General Data Protection Regulation. With regard to the principle of lawfulness the Article 8 of the Law Enforcement Directive provides that the data processing carried out by the authorities of the Member States will be considered lawful only if, and to extent that, processing is necessary for the performance of a task carried out by the competent authority for the purposes of prevention, investigation and prosecution of criminal offences, and that is based on Union or Member State law. Member State law regulating processing shall specify at least the objectives of the processing, personal data to be processed, and the purpose of the processing. Video surveillance may be based on the Article 8 of the Directive, "but if it is used to process special categories of data, the processor must (additionally) satisfy strict requirements of the Directive".¹⁰ This is because face recognition technologies usually process

⁸ GDPR, Article 23(1).

⁹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119*, 4.5.2016.

¹⁰ T. Madiega, H. Mildebrath, *Regulating facial recognition in the EU*, European Parliament, Brussels 2021, 11.

data relating to physical, physiological or behavioral characteristics automatically for the purpose uniquely identifying natural person, and its use therefore qualifies as processing of biometric data. Consequently, such processing will need to fulfill the strict requirements of Article 10 of the Directive which provides that this shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of data subjects, and only:

1. where authorized by Union or Member State law;
2. to protect vital interests of the data subject or of another natural person;
or
3. where such processing relates to data which are manifestly made public by data subject.¹¹

In addition, Article 11 of the Directive prescribes that decisions based solely on automated processing shall be prohibited unless authorized by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject - at least the right to obtain human intervention on the part of the controller.

Furthermore, in the European Union, along with the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), the AI Act¹² is the most important legal instrument regulating the use of facial recognition technologies, bearing in mind that the use of facial recognition technology is mainly put in the context of the use of artificial intelligence¹³. In this document it is stated that *'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data and it can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons*. Article 5 of the AI Act lays down cases when the use of AI is prohibited. Among other things, the ban refers to creating or expanding facial recognition databases through the untargeted scraping of

¹¹ *Ibid.*

¹² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), *OJ L*, 2024/1689, 12.7.2024.

¹³ N. Ružić, Tehnologija prepoznavanja lica i prava i slobode lica - slučaj Republike Srbije, *Savremene studije bezbednosti* (2024)1, 95.

facial images from the internet or CCTV footage because it can lead to gross violations of fundamental rights, including the right to privacy; emotion recognition, biometric categorization and the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, with certain exceptions (e. g. serious crimes, such as terrorism, murder, kidnapping, rape, sexual exploitation of children, and child pornography, trafficking in human beings, illicit trafficking in narcotic drugs or psychotropic substances, in weapons, munitions or explosives, illicit trade in human organs or tissue; see Annex II AI Act)¹⁴. This means that *law enforcement authorities are prohibited from using real-time facial recognition systems in the street based on general security, crime prevention and overcrowding concerns*¹⁵.

In the Commission Guidelines on prohibited artificial intelligence practices established by AI Act, in the first mentioned case cumulative conditions must be fulfilled for the prohibition:

- (i) *The practice must constitute the 'placing on the market', 'the putting into service for this specific purpose' or the 'use' of an AI system;*
- (ii) *for the purpose of creating or expanding facial recognition databases;*
- (iii) *the means to populate the database are through AI tools for untargeted scraping; and (iv) the sources of the images are either from the internet or CCTV footage*¹⁶.

It defines database in this context and scraping and highlights that *the notion of 'untargeted' means without a specific focus on a given individual or group of individuals*¹⁷.

Finally, it is pointed up that *in the data protection context, the use of biometric data, in particular facial recognition technology, has been considered by the European Data Protection Board (EDPB) in its Guidelines 5/2022 on the use of facial recognition technology in the area of law enforcement and the European Data Protection Supervisor (EDPS) as affecting several fundamental rights and freedoms*¹⁸.

¹⁴ See: Communication from the Commission, Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), 29.7.2025 C (2025) 5052 final.

¹⁵ *Ibid.*, para. 359.

¹⁶ *Ibid.*, para. 224.

¹⁷ *Ibid.*, para. 226, 227, 228.

¹⁸ *Ibid.*, para. 396.

III Jurisprudence of the ECtHR

While the jurisprudence of the Court of Justice of the European Union primarily focuses on data protection compliance within the EU legal framework, the practice of the European Court of Human Rights (ECtHR) is uniquely relevant as it directly evaluates whether the use of facial recognition technology (FRT) by state authorities constitutes an interference with fundamental freedoms. In this context, the case of *Glukhin v. Russia*¹⁹ represents the current “gold standard” in ECtHR jurisprudence, as it provides the first and most comprehensive analysis of the compatibility of biometric surveillance with the European Convention on Human Rights (ECHR). Therefore, this case will be specifically analyzed in the following section.

The ECtHR reviewed the State Party’s use of FRT in *Glukhin v. Russia* for human rights compliance. In this case, the ECtHR examined how FRT impacted Article 8 privacy rights and Article 10 freedom of expression. The ECtHR found, using international standards, that the respondent state had breached the applicant’s ECHR rights.²⁰ The ECtHR recognizes that advanced technologies like FRT can improve law enforcement, but even highly intrusive technology must be thoroughly reviewed by the courts and be compatible with democratic values and the rule of law.²¹

In 2019, the applicant protested the detention and criminal charges brought against a political activist by traveling alone on the Moscow subway system and holding a banner. Screenshots of the protest were captured from a public Telegram channel and subsequently incorporated into a police database. The applicant was identified as the individual who had organized the protest by utilizing the images in conjunction with the FRT surveillance system. The applicant’s location was subsequently determined through the use of live FRT, which enabled the authorities to arrest him. Following the results of the police investigation, Glukhin was found guilty of not providing advance notification

¹⁹ ECtHR, *Glukhin v. Russia*, App no. 11519/20, 4 July 2023.

²⁰ The ECtHR decision regarding the right to privacy was influenced by the increasing number of international standards that govern the use of biometric technologies, including the Council of Europe Convention 108. Additionally, the ECtHR considered data privacy regulations, particularly those established by the European Union, such as the General Data Protection Regulation.

²¹ M. Mladenov, Implications pour les droits de l’homme de l’utilisation de la technologie de reconnaissance faciale du point de vue de la Cour européenne des droits de l’homme, 4e Conférence sur le Droit comparé et international qui s’est tenue le 14 juin 2024 à Bucarest, Société des sciences juridiques et administratives, 2024, 201.

before starting a public demonstration and was fined 20,000 Russian rubles. Despite the Russian government's refusal to admit to using FRT directly, the ECtHR acknowledged its use given the specific circumstances of the case.²² The ECtHR recognized the challenges faced by the applicant and determined that the use of FRT can be "reasonably assumed", given the lack of alternative explanations for the applicant's prompt identification and the implicit admission by the Government.²³

The applicant claimed in his submission to the ECtHR that the police had illegally obtained and used screenshots and recordings. He stated that Russia's interfering legislation didn't meet the "quality of law" standard since it was unclear and lacked judicial authority and control. The applicant further stated that his privacy invasion had no valid purpose and was not "essential in a democratic society" under Article 8(2). Given these conditions, the applicant argued that FRT and administrative conviction breached his rights under Articles 8 and 10 of the ECHR. He also complained about the unfairness of his proceedings under Article 6 of the ECHR.

The ECtHR stated that it had jurisdiction to consider the case because the incidents occurred before 16 September 2022, when the Russian Federation left the ECHR. The matter was examined under Articles 8 and 10 of the ECHR.

The ECtHR found that processing the applicant's data using FRT engaged Article 8 of the ECHR. Article 8 ensures respect for private and family life, home, and correspondence. Public authorities cannot interfere with this freedom unless it is prescribed by law, required in a democratic society, and achieves legitimate interests.²⁴ The fact that the applicants' protest was done in public does not prevent the relevance of Article 8. Following its case law, the ECtHR maintained that "private life" includes public behaviors, especially when they involve the systematic or persistent recording of identifiable persons' photographs.²⁵ According to the ECtHR, even though an individual's actions were publicly disclosed, the systematic processing and storage of their image through facial recognition technology fell within the category where that person had a reasonable expectation of privacy. One of the main elements of

²² F. Palmiotto, N. M. González, Facial recognition technology, democracy and human rights, *Computer Law & Security Review* 50(2023), 105857.

²³ ECtHR, *Glukhin v. Russia*, *op. cit.*, para 70.

²⁴ See: M. Mladenov, Protection of the Right to Privacy in the Practice of the European Court of Human Rights, *Zbornik radova Pravnog fakulteta u Novom Sadu* 47(2013)3, 575-593.

²⁵ ECtHR, *López Ribalda and Others v. Spain*, App No. 1874/13 and 8567/13, 17 October 2019.

a person's personality is their image, which sets them apart from their peers and exposes their distinctive qualities. Thus, a person's right to protect their photos and govern how they are utilized is crucial to personal autonomy.²⁶

ECtHR found the following actions represent the breach of the applicant's privacy: collecting and saving videos from underground station CCTV cameras and screenshots from a Telegram channel obtained through Internet monitoring; using live facial recognition on CCTV cameras to locate and arrest the applicant in real time; and using such material as evidence in administrative proceedings.²⁷

During the examination of Russia's interference in line with legal standards, the ECtHR found that police investigations followed domestic law. As demonstrated in its previous cases, the government must base its activities on domestic law and follow the rule of law to meet the ECHR's "quality of law" criterion. Specifically, national legislation should protect privacy rights from unreasonable interference. FRT-collected personal data must be regulated for duration, storage, use, and destruction to guarantee proper protection.²⁸

The ECtHR noted that the provisions in the national law were broadly stated. Biometric data processing, sometimes with FRT, is commonly used under the framework of "any judicial proceedings". The national legal system did not limit, restrict, or offer supervisory controls or remedies for data subjects. Despite police acting in conformity with national law, the ECtHR found that the national laws did not meet the "quality of law" threshold since FRT use was not regulated and protected.²⁹

The ECtHR also recognized the need to use contemporary technology to prevent crimes while determining the legitimate purposes and necessities of a democratic society. In this case, FRT should be considered in light of alleged criminal behavior. The "need" criterion in Article 8 requires government action to address an urgent social need and achieve a legitimate aim. The state must prove that the conducted intervention was necessary for society. The applicant faced prosecution for engaging in a solitary demonstration without

²⁶ *Glukhin v. Russia*, par. 64.

²⁷ F. Palmiotto, N. M. González, *op. cit.*, 3.

²⁸ A. Dadashov, Facial Recognition System is a Violation of Human Rights in the Context of the ECHR, *Human Rights Brief* 27(2023)1, Article 7, 47. <https://digitalcommons.wcl.american.edu/hrbrief/vol27/iss1/7>, last visited: 5. 12. 2025

²⁹ M. Mladenov (2024), 203–204.

prior notification to the appropriate authorities. He organized a non-violent protest without violence or harm. Therefore, the use of the FRT to identify an applicant cannot be deemed essential within a democratic society, and it constituted a breach of his right to privacy.³⁰

In addition, the ECtHR examined the alleged breach of Article 10's freedom of expression. ECHR describes this right as "including the freedom to express one's opinion, the freedom to communicate information, and the freedom to receive information".³¹

Public authorities may restrict freedom of expression under the three-part test. This test was previously mentioned in relation to Article 8 and concerns prescription by law, its necessity in a democratic society, and the achievement of certain legitimate interests.

During his solo demonstration, the applicant intended to share his thoughts on a topic of public concern. Article 10 provided limited grounds for restricting this right. The applicant's right to freedom of expression had been interfered with by his escort to the police station, administrative arrest, and conviction for an administrative offense.³² There was reason to doubt that the manner of application of the contested legal provisions had been sufficiently foreseeable to meet the case's quality requirement, given the nature of the applicant's solo demonstration and the lack of any additional clarifications from higher Russian courts regarding the scope and method of application of the relevant provisions or any thorough analysis by the domestic courts in the applicant's case. Nevertheless, even if we assume that the interference was in accordance with the law and aimed at meeting the legitimate aims of "prevention of disorder" and "protection of the rights of others", it wasn't considered "essential in a democratic society".³³ Furthermore, the national authorities and courts did not justify their interference, despite the demonstration being completely peaceful and non-disruptive. In light of the previous facts, the ECtHR concluded that the applicant's right to freedom of expression, as outlined in Article 10 of the ECHR, had been violated.³⁴

³⁰ A. Dadashov, *op. cit.*, 47.

³¹ J. Flauss, The European Court of Human Rights and the Freedom of Expression, *Indiana Law Journal* 84(2009)3, 809.

³² *Glukhin v. Russia*, par. 52.

³³ *Ibid.*, par. 56.

³⁴ M. Mladenov (2024), 205–206.

Glukhin v. Russia clarifies some key aspects of FRT and human rights, but it also raises major questions. The ECtHR did not assess whether FRT violates Article 8, notably proportionality. The ECtHR examined whether Article 8(2) justified data processing. Thus, the ECtHR analysis was quite restricted.

The ECtHR further stressed that, regarding the “quality of law” requirement in accordance with Article 8, domestic legislation must clearly state, among other things, the specific groups of individuals that may be subject to targeting. Although this measure may be sufficient for FRT used after the fact, it is not suitable for real-time facial recognition. Live FRT requires continuous video surveillance of individuals in specific places. Thus, a technology that impacts everyone without discrimination cannot be defined by its goal.³⁵

Finally, the ECtHR acknowledged FRT’s potential benefits for criminal investigation but stressed the need for law enforcement safeguards. The ECtHR emphasized that when evaluating the infringement on the right to privacy, it considered the characteristics and seriousness of the crime, and whether such interference was necessary in a democratic society. However, the ECtHR refrained from specifying the criteria for determining the types of offenses that could warrant the use of FRT. Can FRT be used for apprehending individuals suspected of property crimes, or is it exclusively employed in cases where illegal activity poses a threat to human life or physical well-being? The ruling does not effectively implement additional unresolved concerns that are still under the jurisdiction of national laws.³⁶

IV Face recognition: Serbian legal approach

In the Republic of Serbia, the issue of legal regulation of the use of face recognition in publicly accessible space has been very topical for some time. Although there have been attempts to regulate this area, this has not been done so far. In this regard, it is important to note that both the Draft Law on Internal Affairs from 2021 and the Draft Law on Internal Affairs from 2022 have been withdrawn from the legislative procedure, as well as the Assessment of the Impact of Personal Data Processing Activities Using Biometric Data Processing Software in the Video Surveillance System of the Ministry of Internal Affairs on the Protection of Personal Data³⁷. It was pointed out

³⁵ F. Palmiotto, N. M. González, *op. cit.*, 5.

³⁶ M. Mladenov (2024), 207.

³⁷ N. Ružić, *op. cit.*

that “[t]he adoption of the proposed regulations in practice would mean an indiscriminate encroachment on the right to privacy and the protection of personal data of all citizens and anyone who is on the territory of the Republic of Serbia, without previously establishing that such action is proportionate and necessary in a democratic society, which is a standard established by international conventions that are incorporated into the legal system of the Republic of Serbia”³⁸. In addition, in the Republic of Serbia, there are no regulations that systematically regulate the use of video surveillance, which is very significant due to the application technology that enables facial recognition.³⁹

We will refer to other documents of the Republic of Serbia that are important for this issue. In the Constitution of the Republic of Serbia, in article 42, it is prescribed that the protection of personal data is guaranteed and that the collection, keeping, processing and use of personal data are regulated by law. In addition, the Constitution provides that the use of this data outside the purpose for which they were collected is prohibited and punishable, except for the purposes of conducting criminal proceedings or protecting safety of the Republic of Serbia, in the manner stipulated by the law. Finally, everyone has the right to be informed about the collected data about him/her, in accordance with the law, and the right to judicial protection against their misuse⁴⁰. Furthermore, the most important law in the Republic of Serbia in this regard is the Law on Personal Data Protection⁴¹. Since the application of face recognition technology involves biometric data, the Law defines them as *personal data obtained through special technical processing in connection with physical features, physiological features or behavioral features of a natural person, which enables or confirms the unique identification of that person, such as a picture of his face or his dactyloscopic data*. In every processing of data, whether biometric or not, the Law stipulates the obligation to respect the

³⁸ Biometrijski nadzor na javnim površinama u Srbiji, pozicija Share fondacije nakon predloženih nacrti zakona, Share foundation, 2, https://www.sharefoundation.info/wp-content/uploads/SHARE_Pozicija_Biometrijski_Nadzor.pdf, last visited: 20. 12. 2025.

³⁹ Strategija zaštite podataka o ličnosti za period od 2023. do 2030. godine, *Sl. glasnik RS*, br. 72/2023 [Personal data protection strategy for the period 2023 to 2030, *Official Gazette of RS*, No. 72/2023].

⁴⁰ Ustav Republike Srbije, *Sl. glasnik RS*, br. 98/2006 i 115/2021 [Constitution of the Republic of Serbia, *Official Gazette of RS*, no. 98/2006 and 115/2021].

⁴¹ Zakon o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br. 87/2018 [Law on Personal Data Protection, *Official Gazette of RS*, No. 87/2018].

principles of lawfulness, fairness and transparency; limitation in relation to the purpose of processing; data minimization; accuracy principles; storage limitation; the principle of integrity and data confidentiality (Article 5). The law prohibits the processing of biometric data for the purpose of unique identification of a person (Article 17, paragraph 1), except in exceptional cases (Article 17, paragraph 2).

In addition, the Law specifically stipulates that the processing of biometric data for the purpose of unique identification of a natural person by the competent authorities for special purposes is allowed only if it is necessary, with the application of appropriate measures to protect the rights of the persons to whom the data refer, in one of the following cases: 1) the competent authority is authorized by law to process special types of personal data; 2) the processing of special types of personal data is carried out in order to protect vital interests of the person to whom the data refer or another natural person; 3) processing refers to special types of personal data that the person to whom they relate to has apparently made them available to the public (Article 18). Finally, in these cases, an assessment of the impact on the protection of personal data is mandatory (Article 54), as well as the previous opinion of the Commissioner for Information of Public Importance and Protection of Personal Data, which has to be requested by the operator if the assessment of the impact on the protection of personal data indicates that the intended processing operations will produce a high risk if no measures are taken to reduce the risk. Under Article 55, if the processing is carried out by the competent authority for special purposes, the operator, i.e. the processor, must request the Commissioner's opinion before starting the processing operations that will lead to the creation of a new collection of data in the event that: protection of personal data, indicates that the intended processing actions will produce a high risk if no measures are taken to reduce the risk; or, the type of processing, especially if new technologies, protection mechanisms or procedures are used, represent a high risk for the rights and freedoms of the persons to whom the data refer.

A working group has been formed in the Republic of Serbia to draft a law on artificial intelligence, and it is expected that, following the example of the AI Act, it will include provisions related to the application of face recognition technologies. So far, only the Strategy for the Development of Artificial Intelligence in the Republic of Serbia for the period 2025-2030 has highlighted that one of the risks of applying artificial intelligence is that face recognition has been improved by using special artificial intelligence

tools, so that the need for data has led to data processing that is often not legally regulated⁴².

In the European Commission Serbia 2025 Report is mentioned that *the legal framework for the protection of personal data (PDP) needs to be further aligned with the EU acquis; the PDP law is mostly aligned with the EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), but its implementation is difficult as it includes provisions from both the GDPR and the LED, while the process of harmonising all other laws with the PDP law is significantly delayed. Furthermore, in the report it is stated that following the Commissioner's previous negative opinions on the Ministry of the Interior's impact assessment on street video surveillance, a legal basis has not yet been developed*⁴³.

Bearing in mind this very fact – that in the Republic of Serbia there is currently no legal basis for the processing of personal data through video surveillance with the option of face recognition – the jurisprudence of the European Court of Human Rights also represents a useful and mandatory guide in the future legislative regulation of this area⁴⁴.

V Conclusion

Facial recognition technology, like all other modern technologies that are evolving and improving rapidly, poses a challenge for legal regulation. In the European Union, the regulation regarding the use of face recognition technology is set in a way that protects human rights, and above all the right to privacy and protection of personal data. There are three key legal documents in this area – General Data Protection Regulation (GDPR), Law Enforcement Directive (LED) and the AI Act. Unlike the GDPR and AI Act, which are directly applicable in EU member states as such, the Directive leaves them to regulate the subject area in their national legislations, but in a way that achieves the goals set in the directive. On the other hand, the use of face recognition

⁴² Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025-2030. godine [Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2025-2030], 21-22.

⁴³ Commission Staff Working Document Serbia 2025 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2025 Communication on EU Enlargement Policy, Brussels, 4.11.2025 SWD(2025) 755 final, p. 39.

⁴⁴ D. Golubović, M. Galetin, Pregled prakse Evropskog suda za ljudska prava od značaja za obradu podataka o ličnosti putem video-nadzora, *Strani pravni život* LXVIII (2024)1, 76.

technology in the Republic of Serbia is not legally regulated, although there have been some attempts. Serbian *legal framework* concerning protection of personal data *is generally aligned with the EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED)*, but its implementation is difficult as *it includes provisions from both the GDPR and the LED*. The Law on Artificial Intelligence of the Republic of Serbia is currently being drafted, and it remains to be seen how our legislator will respond to this challenge. As the Republic of Serbia is a candidate for full membership in the European Union, it is expected that steps undertaken in the European legislation will be followed. In addition, for the Republic of Serbia as a member of the Council of Europe, jurisprudence of the European Court of Human Rights (ECtHR) is valuable, and it should represent another guideline for the actions of Serbian legislator.

Vladimir Medović*

Marijana Mladenov**

Milena Galetin***

Primena tehnologije prepoznavanja lica: pravni pristup EU i pravni pristup Srbije

Sažetak

Upotreba tehnologije prepoznavanja lica je veoma aktuelna tema koja nameće pitanja zaštite ljudskih prava u ovom procesu. U radu, nakon uvoda, autori analiziraju pravni okvir u Evropskoj uniji u vezi sa upotrebom ove tehnologije, koja je usko povezana sa zaštitom podataka o ličnosti, zaštitom prava na privatnost i veštačkom inteligencijom, a zatim i praksu Evropskog suda za ljudska prava. Pristup Republike Srbije u vezi sa ovim pitanjem je predstavljen u posebnoj poglavlju. Konačno, s obzirom na to da upotreba tehnologije prepoznavanja lica u Srbiji nema pravni osnov, u zaključnim napomenama autori ukazuju u kom pravcu bi srpski zakonodavac trebalo da deluje, kako bi ispunio utvrđene standarde zaštite ljudskih prava. U radu se koriste metode karakteristične za društvene nauke: normativni, pozitivnopravni, uporednopravni i analiza sudske prakse.

* Redovni profesor, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Srbija.

** Vanredni profesor, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Srbija.

*** Vanredni profesor, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Srbija.

Ključne reči: prepoznavanje lica, biometrijski podaci, Opšta uredba o zaštiti podataka o ličnosti (GDPR), Uredba EU o veštačkoj inteligenciji (AI Act), praksa Evropskog suda za ljudska prava.

References

Biometrijski nadzor na javnim površinama u Srbiji, pozicija Share fondacije nakon predloženih nacрта zakona, Share foundation, https://www.share-foundation.info/wp-content/uploads/SHARE_Pozicija_Biometrijski_Nadzor.pdf, last visited: 20. 12. 2025.

Dadashov A. Facial Recognition System is a Violation of Human Rights in the Context of the ECHR, *Human Rights Brief* 27(2023)1, Article 7, 47–48, <https://digitalcommons.wcl.american.edu/hrbrief/vol27/iss1/7>, last visited: 5. 12. 2025.

Flauss, J. The European Court of Human Rights and the Freedom of Expression, *Indiana Law Journal* 84(2009)3, 809–849.

Golubović, D., Galetin, M. Pregled prakse Evropskog suda za ljudska prava od značaja za obradu podataka o ličnosti putem video-nadzora, *Strani pravni život* LXVIII (2024)1, 61–81. https://doi.org/10.56461/SPZ_24104KJ

Madiega T., Mildebrath H. *Regulating facial recognition in the EU*, European Parliament, Brussels 2021.

Mladenov M. Implications pour les droits de l’homme de l’utilisation de la technologie de reconnaissance faciale du point de vue de la Cour européenne des droits de l’homme, *4e Conférence sur le Droit comparé et international qui s’est tenue le 14 juin 2024 à Bucarest*, Société des sciences juridiques et administratives, 2024, 195–210.

Mladenov M. Protection of the Right to Privacy in the Practice of the European Court of Human Rights, *Zbornik radova Pravnog fakulteta u Novom Sadu* 47(2013)3, 575–593. <https://doi.org/10.5937/zrpfns47-4909>

Palmiotto F., González N. M. Facial recognition technology, democracy and human rights, *Computer Law & Security Review* 50(2023), 105857, <https://doi.org/10.1016/j.clsr.2023.105857>

Ružić, N. Tehnologija prepoznavanja lica i prava i slobode lica — slučaj Republike Srbije, *Savremene studije bezbednosti* (2024)1, 83–101. <https://doi.org/10.5937/ssb2401083R>

Legal sources

Charter of Fundamental Rights of the European Union, *Official Journal of the European Communities* C 346, 18.12.2000.

Commission Staff Working Document Serbia 2025 Report Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2025 Communication on Eu Enlargement Policy, Brussels, 4.11.2025 SWD(2025) 755 Final.

Communication from the Commission, Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), 29.7.2025 C(2025) 5052 final.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L* 119, 4.5.2016.

European Declaration on Digital Rights and Principles for the Digital Decade, *Official Journal of the European Union*, C23/1, 23.1.2023.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), *OJ L*, 2024/1689, 12.7.2024.

Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2025-2030. godine [Strategy for the development of artificial intelligence in the Republic of Serbia for the period 2025-2030].

Strategija zaštite podataka o ličnosti za period od 2023. do 2030. godine, *Sl. glasnik RS*, br. 72/2023 [Personal data protection strategy for the period 2023 to 2030, *Official Gazette of RS*, No. 72/2023)].

Ustav Republike Srbije, *Sl. glasnik RS*, br. 98/2006 i 115/2021 [Constitution of the Republic of Serbia, *Official Gazette of RS*, No. 98/2006 and 115/2021].

Zakon o zaštiti podataka o ličnosti, *Sl. glasnik RS*, br. 87/2018) [Law on Personal Data Protection, *Official Gazette of RS*, No. 87/2018)].

Case law

ECtHR, *Glukhin v. Russia*, App no 11519/20, 4 July 2023.

ECtHR, *López Ribalda and Others v. Spain*, App No. 1874/13 and 8567/13, 17 October 2019.

Received: 26 February 2026

Accepted: 28 April 2026