

The Legal Regulation of the Facial Recognition and Real-Time Remote Biometric Identification Systems in Ukraine and the Czech Republic

Olha Shpakovych* & Martin Škurek**

Summary: The presented article, created as the output of the project no. 23-PKV-V-UM-6 called CODE (COoperation and DEvelopment) supported within the grant program of the Ministry of Foreign Affairs of the Czech Republic, deals with the legal regulation of the facial recognition and real-time remote biometric identification systems usage in Ukraine and the Czech Republic. As for the situation in Ukraine, it should be noted that the adoption of the draft Law of Ukraine ‘On the Unified System of Video Monitoring of the State of Public Security’ poses risks of violating human rights and freedoms, and will significantly limit the fundamental right of every person to privacy. In order to ensure proper legal regulation of video monitoring of public security using facial recognition systems in Ukraine, the draft Law of Ukraine ‘On the Unified System of Video Monitoring of the State of Public Security’ needs to be finalized and brought into line with the above provisions of the relevant EU and Council of Europe legislation. As for the situation in the Czech Republic, the conclusion is that the AI Act does allow the use of real-time remote biometric identification systems, but under certain conditions. The main one is that the use of such a system to search for a specific person or persons must be authorized by a court or other independent authority. In real terms, this means that the decision to include a particular person in the reference database shall be made by a court. However, in relation to this very basic safeguard against abuse of the system, the Act no. 110/2019 Coll., on the Processing of Personal Data is to propose that this rule shall not be applied to certain relatively vaguely defined groups of persons. Thus, the Act shall negate this fundamental control mechanism in certain cases, in fact.

Key words: AI system, AI Act, the Directive (EU) 2016/679, the Directive (EU) 2016/680, the Convention no. 108, the Convention no. 108+, draft law

* Educational and Scientific Institute of International Relations, Taras Shevchenko National University of Kyiv, Ukraine. Contact email: olshpakovych@gmail.com.

** Faculty of Law, Palacky University in Olomouc, the Czech Republic. Contact email: martin.skurek@upol.cz.

no. 11031 ‘On the Unified System of Video Monitoring of the State of Public Security’, Act no. 110/2019 Coll., on the Processing of Personal Data

Citation: SHPAKOVYCH, O., ŠKUREK, M. The Legal Regulation of the Facial Recognition and Real-Time Remote Biometric Identification Systems in Ukraine and the Czech Republic. *European Studies – the Review of European law, Economics and Politics*. 2024, vol. 11, no. 2, pp. 115–140, DOI: 10.2478/eustu-2024-0019

1. Introduction

The presented article, created as the output of the project no. 23-PKVV-UM-6 called CODE (COoperation and DEvelopment) supported within the grant program of the Ministry of Foreign Affairs of the Czech Republic, deals with the legal regulation of the facial recognition and real-time remote biometric identification systems usage in Ukraine and the Czech Republic. The authors of the submitted article perceive that facial recognition systems draw the most criticism from human rights activists. Essentially, any video or camera system with a sufficiently high resolution may be used to collect data on citizens, including those who have never had any problems with the law, which may be considered indiscriminate mass surveillance. The intensive use of video or camera systems affects the behavior of individuals. These technologies may de facto limit the ability of individuals to move anonymously and use services anonymously. A person loses the fundamental right to privacy. Video or camera system surveillance by default is not necessary if there are other means to achieve the main objective. Otherwise, we are at risk of changing the norms of a person’s behavior, which can lead to a general acceptance of the lack of privacy in society and change the norms of a person’s behavior in society. The authors of the presented article are in absolute agreement on these premises. The above risks seem to be recognized by the decision-makers within the European Union institutions, and therefore the relevant European legislation, in particular the 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 (so-called the AI Act), the 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 (so-called

GDPR) and others, provide for instruments to prevent these risks. Thus, in the presented article, the authors discuss the question to what extent the national Ukrainian and Czech legislation in this area complies with EU law.¹

2. The legal regulation of the facial recognition systems in Ukraine

Video surveillance systems are gradually becoming a familiar attribute in Ukraine in the 21st century. Electronic devices record what is happening at stadiums, sports grounds, streets, parks, highways, airports, and train stations. Information technologies are used to protect public order, control road safety, protect property, etc.² In this regard, an important issue is the legal regulation of video monitoring of public security using facial recognition systems in Ukraine. As of today, the Verkhovna Rada of Ukraine has registered the draft law no. 11031 ‘On the Unified System of Video Monitoring of the State of Public Security’ on 20 February 2024.³ Pursuant to the explanatory note, the draft law ‘On the Unified System of Video Monitoring of the State of Public Security’ was developed to ensure national and state security, increase the overall level of public security and order, and ensure the safety of places of residence and stay of citizens by introducing a unified system of video monitoring of the state of public security on the basis of state authorities and local self-government bodies in accordance

¹ For more details see for instance JASSERAND, C. The Future AI Act and Facial Recognition Technologies in Public Spaces: Nice to Have or Strictly Necessary? *European Data Protection Law Review*. 2023, 9(4), pp. 430–443; Moreira, N. A., Freitas, P. M. Towards Transparent AI: How will the AI Act Shape the Future? *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14967 LNAI, pp. 296–307, 2024; Leucker, M. The AI Act and Some Implications for Developing AI-Based Systems. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 15240 LNCS, pp. 202–214, 2024; Hoffmeister, K. The Dawn of Regulated AI: Analyzing the European AI Act and its Global Impact. *Zeitschrift für Europarechtliche Studien*. 2024, 27(2), pp. 182–212; HERRERA, F., DIGNUM, V., PACHET, F. et al. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14967 LNAI, 23rd EPIA Conference on Artificial Intelligence, Viana do Castelo, 3–6 September 2024, code 323069 and others

² Guidelines for local self-government bodies ‘Video surveillance in public places’ [online]. Available at: http://labs.journ.univ.kiev.ua/hrj/wp-content/uploads/2021/07/Відеоспостереження-в-публічних-місцях_ПОСІБНИК.pdf

³ Draft Law of Ukraine ‘On the Unified System of Video Monitoring of the State of Public Security’ No. 11031 of 20 February 2024 [online]. Available at: <https://itd.rada.gov.ua/billInfo/Bills/Card/43733>

with uniform functional and technological standards. The aim is to monitor and facilitate the prevention and elimination of possible threats, as well as to control the elimination of the consequences of emergencies and offenses.

According to the Deputy Minister of Internal Affairs of Ukraine, ‘Today, there are more than 60 000 video surveillance cameras operating in more than 600 systems belonging to entities of various forms of ownership in Ukraine. The draft law provides for the introduction of standardized rules for the administration of such cameras and systems. Following the adoption of this legislative act, it will become clear which cameras will be used, what conditions will be provided for logging accesses, the procedure for storing information, and the data storage period.’⁴

One of the key aspects in the context of analysing the legal regulation of video monitoring of the state of public security using facial recognition systems in Ukraine is that the use of such modern facial recognition technologies might lead to mass monitoring of public places and collection of biometric data of citizens. The United Nations High Commissioner for Human Rights, Volker Türk, noted that such technologies could lead to ‘mass surveillance of our public spaces, destroying any concept of privacy’.⁵ The processing of biometric data using real-time facial recognition technologies in the absence of a proper legal basis and legitimate purpose may violate the right to privacy guaranteed by Article 32 of the Constitution of Ukraine, which protects every citizen from interference with private and family life.

Meanwhile, Michelle Bachelet, the former head of the Office of the United Nations High Commissioner for Human Rights, also warned about the dangers of unregulated AI tools and called for a moratorium on the sale and use of AI systems, particularly facial recognition and related technologies posing a threat to human rights.⁶ Amnesty International, a non-governmental organization uniting more than 7 million people around the world and dedicated to preventing serious human rights violations, has also launched a global campaign to ban the use of facial recognition systems for mass surveillance. In the view of the NGO, indiscriminate mass surveillance is never a proportionate interference with the human

⁴ Тимченко, Л. *Користувачі систем відеомоніторингу нестимуть відповідальність за незаконне розповсюдження даних* [online]. Available at: <https://mvs.gov.ua/news/leonid-timchenko-koristuvaci-informaciyi-z-kamer-videosposterezennia-nestimut-vidpovidalnist-za-nezakonne-rozpovsiudzennia-danix>

⁵ McCURDY, W. *UN High Commissioner says facial recognition could lead to destruction of privacy* [online]. Available at: <https://www.biometricupdate.com/202307/un-high-commissioner-says-facial-recognition-could-lead-to-destruction-of-privacy>

⁶ Войнов, М. *Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС* [online]. Available at: <https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/>

right to privacy, freedom of expression and freedom of association and peaceful assembly.⁷ According to the international non-governmental human rights organization Human Rights Watch, the government should publish statistics on the effectiveness of facial recognition systems and invite civil society experts to participate in the debate on the necessity, proportionality and lawfulness of using surveillance of such technologies.⁸

In line with Ukraine's international commitments, Title III of the EU-Ukraine Association Agreement provides for cooperation in the areas of justice, freedom and security. Under Article 15 of the Association Agreement, 'Ukraine and the European Union agree to cooperate in order to ensure an adequate level of protection of personal data in accordance with the highest European and international standards, including the relevant Council of Europe instruments.'⁹ Integration of Ukraine into the European Union's Digital Single Market requires the maximum approximation of the provisions of national legislation to the EU requirements in the field of personal data protection. Moreover, Ukraine is a party to The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter also referred to as the Convention no. 108). In May 2018, the Council of Europe adopted CETS Protocol no. 223 amending Convention no. 108. The Modernised Council of Europe Convention no. 108 (hereinafter also referred to as the Convention no. 108+) addresses most of the challenges posed by the development of information and communication technologies and strengthens the requirements for its implementation. Therefore, Ukraine is facing the issue of ratification of the aforesaid Protocol and bringing its legislation in compliance with the requirements of the Convention no. 108+.

Given the foregoing, one can argue that the adoption of any legislative act directly related to personal data protection should comply with the provisions of the relevant EU and Council of Europe legislation and be guided by the best practices of national legislation of EU Member States. As Ukraine seeks full integration and accession to the European Union, it must also consider European legislation in the field of human rights. As of 1 August 2024, the 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

⁷ Ibid

⁸ Авдєєва, Т. Чи легально встановлювати на міських вулицях камери із системою розпізнавання обличч? [online]. Available at: <https://cedem.org.ua/analytics/kamery-rozpiznavannya-vannya-oblych/>

⁹ *Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part* [online]. Available at: https://zakon.rada.gov.ua/laws/show/984_011

(EU) 2020/1828 (hereinafter also referred to as the AI Act) came into force in the EU, directly prohibiting the use of real-time biometric identification systems in publicly accessible spaces for the purpose of law enforcement. Exceptions are possible only in special cases, for example, to search for kidnapping victims or to prevent terrorist threats.¹⁰ The use of facial recognition technologies may also significantly affect people's behaviour by restricting their freedom of movement and ability to use public spaces anonymously. Such actions may jeopardize fundamental democratic values, as citizens may avoid participating in public events or protests for fear of being identified and prosecuted.

Another important aspect is the security of the array of digital data required for the implementation of a unified system of video monitoring of the state of public security, as well as the data that will be collected during the operation of this system. The draft law no. 11031 stipulates that the identification of the information object 'natural person' is carried out on the basis of a certain set of biometric data and the following information about the person: name, date of birth/death, place of birth, gender, information about the registered or declared place of residence or stay of the person, removal of the person from the place of residence registration or change of place of residence (stay) of the person, information about citizenship or lack thereof, digitized image of the person's face, tax payer identification number, series and number of a passport. The vast amount of personal data collected, including biometric data, will require an exceptional level of protection, as unauthorized access to or dissemination of this data can lead to significant privacy violations. Under such circumstances, personal data leakage may result not only in interference with the private life of citizens, but also in a threat to their personal safety and even life. Responsibility for the protection of such data should be clearly defined and regulated, with strict sanctions for violations, to avoid misuse and cybercrime.

The draft law 'On the Unified System of Video Monitoring of the State of Public Security' provides that the protection of personal data in video monitoring systems of the state of public security must comply with the Convention no. 108, the Additional Protocol to the Convention no. 108 regarding supervisory authorities and transborder data flows, the 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

¹⁰ *The 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 (the AI Act).* [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

(hereinafter also referred to as the Regulation (EU) 2016/679 or GDPR) adopted in the European Union, as well as legislation in the field of data protection.

In accordance with Article 8 of the European Convention on Human Rights¹¹: ‘Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’

Article 6 of the Council of Europe Convention no. 108¹² states that personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions. In accordance with Article 6 of the Convention no. 108+ of the Council of Europe,¹³ the processing of biometric data uniquely identifying a person shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. The Convention no. 108+ of the Council of Europe stipulates that the processing of categories of data such as biometric data is only possible on the basis of law, subject to appropriate and adequate safeguards against misuse.

On January 25, 2008, the Parliamentary Assembly of the Council of Europe adopted a Resolution entitled ‘Video surveillance of public areas’¹⁴. This Resolution provides that the Council of Europe member states should regulate the use of video surveillance systems in public places at the legislative level and, particularly, define mechanisms and concepts regarding¹⁵: (a) the collec-

¹¹ *The European Convention on Human Rights* [online]. Available at: https://zakon.rada.gov.ua/laws/show/995_004#Text

¹² *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [online]. Available at: https://zakon.rada.gov.ua/laws/show/994_326#Text

¹³ *The Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* [online]. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjecId=09000016807c65bf

¹⁴ *The Resolution of the Parliamentary Assembly of the Council of Europe on ‘Video surveillance of public areas’* [online]. Available at: http://w1.c1.rada.gov.ua/pls/mpz2/docs/769_1604.htm

¹⁵ SPILNO.ORG. *Україна ігнорує вимоги ЄС щодо систем відеоспостереження в публічних місцях* [online]. Available at: <https://spilno.org/article/ukraina-ihnoryue-vymohy-yes-schodo-system-videosposterezhennya-v-publichnykh-mistsyakh>

tion, treatment and conservation of data obtained through video surveillance; (b) strictly regulate the use of technical possibilities with certain far-reaching aspects of continuous surveillance; (c) determine limits for the installation of equipment and software with image zoom functions with respect to each specific place concerned; (d) ‘private zones’ should be defined by law and excluded from video observation by using specialized software; (e) practice of encoding video data; (f) the right of citizens to know about passing through an area under video surveillance and to gain access to all the images of him or herself.

The Council of Europe’s Committee on Artificial Intelligence in its studies emphasizes that facial recognition systems can seriously threaten the rights to privacy, freedom of expression and prohibition of discriminatory treatment. The Regulation (EU) 2016/679¹⁶ prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. The exception to this Article is Article 9(g): processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Before introducing certain new technologies or processing methods that may pose a ‘significant threat’ to the rights and freedoms of individuals, the Regulation (EU) 2016/679 requires the controller to carry out the data protection impact assessment. Pursuant to Article 35(1) of the Regulation (EU) 2016/679, where the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Article 35(3) of the Regulation (EU) 2016/679 provides that a data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing

¹⁶ *The 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 (the General Data Protection Regulation)*. [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale. In pursuance of Article 35(7) of the Regulation (EU) 2016/679, a data protection impact assessment shall contain at least the following: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Article 32 of the Regulation (EU) 2016/679 requires the controller and the processor to ‘implement appropriate technical and organizational measures’. The Regulation (EU) 2016/679 contains provisions on the types of safeguards that may be considered ‘based on the risks involved’, including: (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The analysis of the above-mentioned provisions of the EU and Council of Europe legislation has demonstrated that both legislations are extremely cautious about the use of video surveillance systems and real-time biometric identification in public places and try to apply appropriate safeguards, set appropriate restrictions or bans at the legislative level with respect to the use of facial recognition systems. Where facial recognition technology is introduced, detailed rules governing the scope and use of the technology and safeguards to prevent abuse and arbitrariness are required. The need for safeguards is greater when it comes to the use of real-time facial recognition technology.

Article 13 of the draft law ‘On the Unified System of Video Monitoring of the State of Public Security’ also provides that personal data (information about a natural person, vehicle owner, etc.) shall be collected and processed in the systems of video monitoring of the state of public security for the period necessary to achieve the purposes of processing such data as defined by law, but no longer than fifteen years. Personal data is subject to depersonalization upon expiry of the storage period or in cases provided for by law. Data on the digitized image

of a person's face, brand, model, color, license plate, etc. of a vehicle is stored only in the central-level video monitoring system of public security.

It should be noted that when facial recognition cameras are used on a regular basis, it is hardly possible to define specific purposes and restrictions on the further use of images. Therefore, the legitimate goal of 'preventing crime and protecting public order' does not allow for the establishment of a time period for which information will be stored, nor for the justification of the grounds for collecting data on an unlimited number of individuals.

While developing the provisions of this draft law in relation to the remote biometric identification system, it is essential to adhere to the principles of personal data processing pursuant to Article 5 of the Regulation (EU) 2016/679: (1) principle one: lawfulness, fairness and transparency, (2) principle two: purpose limitation, (3) principle three: data minimisation, (4) principle four: storage limitation, (5) principle five: integrity and confidentiality, (6) principle six: accuracy, (7) principle seven: accountability. For example, in accordance with the principle of personal data storage limitation, personal data should not be stored for longer than is necessary for the purposes for which the data is processed ('storage limitation'). Once the purpose has been achieved, personal data shall be destroyed or depersonalized. Depersonalized personal data is data from which all information has been removed and which no longer allows for the identification of a specific person in any way – the subject of personal data. Personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to appropriate technical and organizational measures provided for by law to guarantee the rights and freedoms of the data subject. To ensure that personal data is not stored for longer than necessary, the controller shall set time limits after which it is deleted or reviewed.

In our opinion, the fifteen-year data retention period provided for in the draft law 'On the Unified System of Video Monitoring of the State of Public Security' is excessive and cannot be considered necessary in a democratic society. The use of facial recognition technology requires a high level of justification in order to be considered 'necessary in a democratic society'. The highest level of justification is required for the use of real-time facial recognition technology. Among the problematic issues of the draft law 'On a Unified System of Video Monitoring of the State of Public Security' is the fact that the purpose of the draft law is defined too broadly and vaguely: 'in order to ensure national security, increase the overall level of public safety and order, ensure the security of places of residence and stay of citizens, prevent and eliminate possible threats, as well as control the elimination of the consequences of emergencies and offences in the interests of the population of the state or certain administrative and territorial

units', while ensuring the security of places of residence and stay of citizens is already a direct interference with the right to respect for private and family life.

One more problem not mentioned in the draft law 'On the Unified System of Video Monitoring of the State of Public Security' is the use of technical devices (means) prohibited in some countries due to security breaches already detected, which in aggregate can lead to much greater problems for national security. Since hacking such a system and access to it by persons interested in monitoring a particular object, such as critical infrastructure or a government authority, may lead to serious consequences.¹⁷

3. The legal regulation of the real-time remote biometric identification systems in the Czech Republic

This part of the presented article deals with the legal regulation of the real-time remote biometric identification systems in the Czech Republic. Regarding a national practice, for several years now, the Police of the Czech Republic has been using a smart camera system at the Václav Havel Airport in Prague (hereinafter also referred to as the Airport), that can identify the perpetrators of certain crimes or the faces of kidnapped and missing persons in crowds of passengers. This artificial intelligence (hereinafter also referred to as AI) system is capable of biometric identification of people remotely in real time. It must be noted that the real-time biometric identification system located at the Airport is the only one of its kind in the Czech Republic so far. According to a press report of the Ministry of the Interior, 145 cameras in total were deployed in the public area of the Airport in places with a high concentration of passengers. The system was put into operation on 15 June 2018.^{18,19}

¹⁷ CSPa. *Проект Закону про єдину систему відеомоніторингу стану публічної безпеки* [online]. Available at: <https://cspa.digital/video-surveillance/>

¹⁸ HANDREJCHOVÁ, M. *Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů* [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-aneb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju>

¹⁹ For more details on the real-time biometric identification system located at the Airport see for instance Digitálně-právní organizace luRe. *Kamery rozpoznávající tváře na letišti v Praze jsou v souladu se zákonem* [online]. Available at: <https://digitalnisvobody.cz/blog/2021/11/30/kamery-rozpoznavajici-tvare-na-letisti-v-praze-jsou-v-souladu-se-zakonem/>; MACH, V., VOBOŘIL, J. *Účel biometrie při sledování veřejného prostoru v České republice* [online]. Available at: <https://digitalnisvobody.cz/uploads/2021/02/FUJÁČEK, J. „Nejde o velkého bratra,“ říká policie o identifikaci obličejů. Úřad po ní žádá vysvětlení> [online]. Available at: <https://www.echo>

The contractors of the system at the Airport agreed in the contract for the implementation of that project that the system would be adapted ‘to search for matches of captured faces with persons of interest and to evaluate saved face detection records with ex post searches of embedded photographs of persons.’ In detail, the system works by matching the biometric facial profiles extracted from the images captured by the camera system with the Police of the Czech Republic biometric facial profiles database of persons-of-interest, into which the data are being drawn from the information system called PATROS, i. e. the Persons-of-Interest Searching System. This information system processes data on wanted and missing persons. The system allows both real-time matching and retrospective matching by saving biometric profiles of faces recorded by the camera system in the last 30 days. According to a statement from the Police of the Czech Republic, NEC’s NeoFace Watch and NeoFace Archiver software technologies are being used in the camera system to capture the biometric facial profiles. The entire camera system is also linked to other Airport security systems and operational databases.^{20,21}

As for the legal regulation, at EU level, the issue of AI and the setting of comprehensive legal rules for the use of real-time remote biometric identification systems is regulated by the AI Act. The legal basis for the AI Act is Article 16 of the Treaty on the Functioning of the EU, enshrining the protection of personal data, to the extent that Article 5 restricts the use of AI systems for a real-time biometric identification in publicly accessible areas for law enforcement purposes, and Article 114 of the Treaty on the Functioning of the EU, regulating the functioning of the internal market, to the remaining extent. Recital 38 of the AI Act provides that, to the extent that Article 16 of the Treaty on the Functioning of the European Union is the legal basis for the provisions of the AI Act, the AI Act constitutes a special regulation of the biometric data processing in relation to Article 10 of the Directive (EU) 2016/680 of the

24.cz/a/HJrg8/zpravy-domaci-kamery-system-rozpoznavani-obliceju-policie-tvare-velky-bratr-dpo-prezident

²⁰ HANDREJCHOVÁ, M. *Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů* [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-aneb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju>

²¹ For more details on the real-time biometric identification system located at the Airport see for instance MACH, V., VOBORIL, J. *Český Minority Report – Využití umělé inteligence Policií České republiky* [online]. Available at: <https://digitalnisvobody.cz/uploads/2024/01> and Policie České republiky, úřad služby kriminální policie a vyšetřování Policejního prezidia České republiky. *Posouzení vlivu na ochranu osobních údajů k informačnímu systému Digitálních podob osob v souladu s § 37 zákona č. 110/2019 Sb., o zpracování osobních údajů* [online]. Available at: <https://uoou.gov.cz/media/poskytnute-informace/2023/2092023/4-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia-dokument-c-4.pdf>

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 (hereinafter also referred to as the Directive (EU) 2016/680), covering the personal data processing for police and criminal justice purposes. At this point, it should be noted that the real-time remote biometric identification of natural persons in public areas may only be used, from the AI Act's entrance into force, under the conditions set out therein. In other words, the biometric data processing in connection with such use is thus regulated in the AI Act exhaustively.^{22,23}

In view of the above, it is necessary a brief explanation of the terms as defined by the AI Act. Under Article 3 of the AI Act, biometric data are personal data resulting from specific technical processing, relating to physical or physiological features or behavioural characteristics of a natural person, such as facial or fingerprint data. Biometric identification is the automated recognition of physical, physiological, behavioural or psychological human characteristics in order to establish the identity of a natural person by comparing that person's biometric data with the biometric data of individuals recorded in a database. This may include, for example, automated recognition of facial shape, eye movement, body shape, voice, gait, posture or heart rate. A remote biometric identification system is an AI system for the purpose of identifying natural persons remotely by matching the biometric data of a person with biometric data recorded in a reference database where the user of the AI system does not know in advance whether the person will be present and identifiable. Typically, these systems are used to capture multiple persons or their behaviour simultaneously without the active involvement of those persons. A real-time remote biometric identification system is a system where the capture of biometric data, matching, and identification are performed without delay and involve not only instantaneous identification but also limited short delays to prevent circumvention. A publicly accessible area is any physical place on public or private property accessible to an unspecified

²² HANDREJCHOVÁ, M. *Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů* [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-aneb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju>

²³ For more details, see *The 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 (the AI Act)*. [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

number of individuals, regardless of whether certain access conditions may apply and regardless of possible capacity constraints, e. g. airports, shops, streets, restaurants, banks, bus stops, theatres, squares etc.^{24,25}

As mentioned above, AI Act lists, among other things, prohibited practices in the field of AI use. In principle, under Article 5(1) of the AI Act, the prohibited practices also include the use of real-time remote biometric identification systems in publicly accessible areas. The reason is that the use of such a system particularly interferes with the rights and freedoms of the persons concerned as it may affect the private life of a large part of the population. Moreover, a real-time remote biometric identification system may make people feel constantly monitored and discourage them from exercising their freedom of peaceful assembly and other fundamental rights indirectly. However, the prohibition expressed above is not absolute, as Article 5(1)(d) of the AI Act permits the use of real-time remote biometric identification systems in certain, precisely specified, exceptional situations. Such an exception is where the system is used for law enforcement purposes, if and to the extent strictly necessary for one of those purposes: (a) targeted searching for victims of kidnapping, human trafficking or sexual exploitation, as well as searching for missing persons; (b) the prevention of a specific, serious and imminent threat to the life or physical safety of persons or an actual, imminent or foreseeable terrorist attack; (c) the location and identification of a person, suspected of having committed a criminal offence, for the purpose of criminal investigation, prosecution or punishment for criminal offences listed in Annex II to the AI Act. Moreover, when using real-time remote biometric identification systems, it is always important to take into account the nature of the situation and also the consequences of the use of these systems for the rights and freedoms of all persons concerned and the guarantees and conditions ensured by such use. Such systems should only be used to confirm

²⁴ HANDREJCHOVÁ, M. *Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů* [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-aneb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju> and Article 3 of the AI Act.

²⁵ For more details see for instance Xiaohan, Y. A face authentication-based searchable encryption scheme for mobile device. *Journal of Supercomputing*. 2024, 81(1); MOHD, A. et al. ECG Biometric Verification Incorporating Different Physiological Conditions. *Journal of Advanced Research in Applied Sciences and Engineering Technology*. 2024, 51(2), pp. 97110; MILOSI, M. *ECG Remote biometric identification systems and ethical challenges: The case of facial recognition*. 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference, SEEDA-CECNSM, Preveza, 24–26 September 2021; KIESLICH, K., LŮNICH, M. *ECG Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations*. 2024 ACM Conference on Fairness, Accountability, and Transparency, FAccT 2024, Rio de Janeiro, 3–6 June 2024 and others.

the identity of a specifically targeted person, taking into account time, place and personal limitations.^{26,27}

Given its high-risk nature, if a law enforcement agency (the Police of the Czech Republic, for instance) decides to use a real-time remote biometric identification system, Article 6 and 51 of the AI Act states that the law enforcement agency should conduct an assessment of such a system's impact on fundamental rights and register such a system in the EU Database for High-Risk AI Systems. Any use of such a system should also be subject to explicit and specific authorization by a judicial authority or an independent EU Member State administrative authority whose decision is binding. In principle, the authorization for the use of such a system should be obtained prior to its use (an exception may arise in a duly substantiated case of urgency) on the basis of a reasoned request submitted by a law enforcement authority. At the same time, the national data protection authority (in the case of the Czech Republic, the Office for Personal Data Protection) should be informed of any use of such a system. This national data protection authority then submits a regular report on this matter to the European Commission. EU Member States may, in accordance with the arrangements set out in the AI Act, lay down more detailed rules for the use of such a system in their country. The processing of biometric data through such a system for law enforcement purposes must also comply with all the requirements set out in the Directive (EU) 2016/680. Due to the possibility of technical errors in AI systems, the AI Act also regulates situations where a person who is not in the reference database is identified wrongly. For these cases, the AI Act states that only on the basis of the use of a real-time remote biometric identification system a decision that has adverse legal effects for a particular person cannot be issued.²⁸

At the national level, in response to the AI Act coming into force, the use of AI real-time remote biometric identification systems shall be regulated by the Amendment of the Act no. 273/2008 Coll., on the Police of the Czech Republic,

²⁶ For more details on prohibited practices in the field of AI use see HANDREJCHOVÁ, M. *Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů* [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-aneb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju> and Article 5 of the AI Act.

²⁷ For more details on prohibited practices in the field of AI use see for instance NEUWIRTH, R. J. Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). *Computer Law and Security Review*. 2023, 48; Guridi, E., Francisco, J. THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS FOR REMOTE BIOMETRIC IDENTIFICATION IN PUBLICLY ACCESSIBLE SPACES IN THE EUROPEAN AI LAW. *Actualidad Jurídica Iberoamericana*. 2024, 21, pp. 528–565.

²⁸ HANDREJCHOVÁ, M. *Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů* [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-aneb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju>

and some other acts, including the Act no. 110/2019 Coll., on the Processing of Personal Data (hereinafter also referred to as the Amendment draft), newly. The Amendment draft was approved by the Government of the Czech Republic on 30 September 2024 and is in the legislative process at the level of the Chamber of Deputies, i. e. in the first reading of the Amendment draft, at the moment. In relation to the above, the following text of the presented article will be focused on the question to what extent the Amendment draft complies with the AI Act.²⁹

As to the reasons for the submission of the Amendment draft, it is, as the legislators clearly intended, strongly linked to the system operating at the Airport. In detail, point 1.D of the general part of the Explanatory Memorandum to the Amendment draft states that the Police of the Czech Republic operates the relevant system, i. e. the system at the Airport, as an isolated system for the purpose of security ensuring and crime prevention. In order to avoid unnecessary interruption of the relevant parts of this system, the Amendment draft shall transpose, to the necessary extent, the conditions required for a real-time remote biometric identification in a specific scope by amending the Act no. 110/2019 Coll., on the Processing of Personal Data (hereinafter also referred to as the Act), which has already transposed most of the provisions of the Directive (EU) 2016/680. As the Czech government foresees, for reasons of internal security protection, the extension of this relevant system to other Czech international airports, the Amendment draft shall allow for the deployment of an isolated system at more Czech international airports, but nowhere else, although the AI Act allows for that. Under the Explanatory Memorandum to the Amendment draft, this case-by-case legislation shall meet the current pressing needs of internal security in the context of the prohibition of AI systems for a real-time remote biometric identification, but shall not represent an exhaustion of the possibilities allowed by the AI Act *de lege ferenda*.³⁰

In parallel with the powers of the administering authority to operate an isolated system, the Amendment draft shall also introduce new minor offences for breaches of the authority's obligations (although most of the minor offences shall be punishable under other rules regulating the personal data processing), that should be dealt with under the standard sanction regime. On the contrary, the vast majority of the rules of the AI Act shall not be adapted by the Amendment draft because: (a) they are not related to the special regulation of biometric data use for real-time remote identification in public areas during the activities of law enforcement authorities and (b) they exceed the competence of the Ministry of

²⁹ *Amendment draft to the Act no. 110/2019 Coll., on the Processing of Personal Data* [online]. Available at: <https://odok.cz/portal/veklep/material/KORND34KYGTD/>

³⁰ *Amendment draft to the Act no. 110/2019 Coll., on the Processing of Personal Data* [online]. Available at: <https://odok.cz/portal/veklep/material/KORND34KYGTD/>

Interior as a promoter. Nor are the various hypothetical systems for a real-time remote biometric identification in public areas (i. e. systems deployed in areas with a large number of people passing through or randomly appearing in other ways, systems with a variable geographical scope, etc.) subject to adaptation. In the case of other biometric identification systems, i. e. those that do not operate in real time in publicly accessible areas, the biometric and personal data processing related to their use will still fall under Article 10 of the Directive (EU) 2016/680 mentioned above. Where purposes other than law enforcement are involved, Article 9 of the Regulation (EU) 2016/679 and Article 10 of the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) no. 45/2001 and Decision no. 1247/2002/EC, covering personal data processing by EU institutions and bodies, will still be applied. As regards the specific impacts of the Amendment draft, it is intended to add new provisions to the Act, namely Sections 39a, 39b and 39c.³¹

With regard to its content, significant comments can be made on the Amendment draft. In general, concerns can be expressed as to whether the proposal as presented, in some aspects going beyond the minimum required by EU law, will not lead to the “Chinese model”, i. e. to the massive deployment of camera systems with facial recognition and their subsequent mass exploitation. The second general comment related to the above is the risk that the elastic provisions of the Amendment draft, without ensuring sufficient control, will in practice allow the hypertrophy of the use of the designed systems and thus highly increase the risk of excessive interference with the rights of suspected and potentially suspected persons in the sense of so-called “phishing”. Where it would have been easy to proceed by way of the criminal procedure, which guarantees the protection of the persons, against whom certain repressive measures are to be used, it will be possible to proceed in a de facto non-procedural manner, thus eliminating the possibility of the persons, against whom these measures are to be used, having their constitutional rights guaranteed.³²

The above harsh criticism arises mainly from the fact that the legal regulation under the Act is intended to divide the inclusion of persons in the reference database. Specifically, in cases under Section 39(a)(3) of the Act, where persons suspected or accused of certain offences or persons under investigation

³¹ Ibid.

³² *Objections to the Amendment draft made during law-making process* [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>

are to be concerned, it shall not be necessary, contrary to the AI Act, to issue a judicial authorization. The problem is that almost anyone could be included in the database in this way. The decision as to who is a suspect shall not be made by anyone authoritatively, it shall be a factual belief of the administering authority, i. e. the belief of a police officer generally, that someone may have committed the act under investigation. Only then it shall be examined whether there is any reason to initiate a criminal prosecution against such a person. Thus, according to the Act, anyone can become a suspect without knowing about it in fact and without having the opportunity to defend themselves. The legal regulation under Section 39(3) of the Act thus creates a wide scope for the system to be abused. It also seems to be very serious that Article 5(1)(d) of the AI Act provides the exception to the general prohibition on AI practices, while Section 39a(3) of the Act relates only to the inclusion of persons' biometric data in a reference database, not to the use of a real-time remote biometric identification system as a whole. In particular, there is no consideration and regulation, in terms of the GDPR principles that should apply subsidiarily, of the biometric data processing outside the reference database. At the same time, it is absolutely impossible to agree with the statement in the Explanatory Memorandum to the Amendment draft that the impact on the human rights and freedoms of non-classified persons is comparable to that of camera systems not using biometric identification.³³

Under Section 39a(1)(b) of the Act, the space in which an isolated system, thus a real-time biometric identification system, is to be used shall be defined by "facilities and areas that are parts of an international airport", but there is no precise definition of "facilities and areas that are parts of an international airport". Specifically, under the Explanatory Memorandum to the Amendment draft, the system is to be used at the Airport only in the publicly accessible parts of the Airport complex, i. e. the departure and arrival halls and adjacent public areas. Under the Explanatory Memorandum to the Amendment draft, the parts of the Airport where only authorized personnel and screened passengers may move after security screening cannot be considered publicly accessible. While it can be agreed that some areas accessible only to authorized personnel should not be public areas, this argument cannot be accepted for areas which, even after security screening, are accessible to all passengers. This is commented on in Article 3(39) of the AI Act, according to which even a publicly accessible area may be subject to certain conditions of access.³⁴

³³ Ibid.

³⁴ *Objections to the Amendment draft made during law-making process* [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>

It is also necessary to mention that, under Section 39a(2) of the Act, the isolated system may include multiple geographically separated components. From the Explanatory Memorandum to the Amendment draft, it is therefore clear that the legislator intends to extend the system to other airports in the Czech Republic, while it shall be one isolated system as a whole. In essence, the proposed wording allows to link all areas and objects that will meet the conditions of Section 39a(1)(a) and (b) of the Act into one system. However, as a result of the merging of sub-areas of different character, duties that should be carried out separately for each such system, i. e. assessment of the impact of high-risk system on fundamental rights, approval, registration, reporting on the use of this system and others, shall not be carried out.³⁵

It appears to be quite crucial that Article 5(1)(d) of the AI Act, regulation the use of real-time remote biometric identification systems, i. e. in the words of the Amendment draft, an isolated system, quite restrictively states that the practices of using such systems in publicly accessible places for law enforcement purposes are prohibited, unless it is strictly necessary for one of the purposes defined in the AI Act, and only to the extent strictly necessary. However, the legislator transposed this negative condition of the AI Act in reverse, by making it positive. This can be deduced from Section 39(a)(3) of the Act, which is to specify the data that shall be capable of being included in the database of the isolated system, and also from both Section 39(b)(1) and Section 39(c)(1) of the Act, which shall deal with the cases where the system may be used. Following on from this, the Act is to lack the general requirement of necessity and the necessary extent as required by the AI Act for the use of systems in public spaces. While the wording of Section 39(a)(3) of the Act is intended to provide for the inclusion of data only for the necessary purposes set out here, the wording of the AI Act is more restrictive.³⁶

Furthermore, the Amendment draft distinguishes between the inclusion of a natural person in the reference database of an isolated system under Section 39b and 39c of the Act. The differentiation in the Amendment draft indicates that the use or use of an isolated system, consisting in entering the biometric data of a natural person into the reference database of the isolated system, has different levels of assessment and control depending on the person or the objective being pursued. However, it cannot be inferred from the content of the AI Act that it contains two levels of authorization relating to the isolated real-time remote biometric identification systems. Specifically, difference is that while in other cases under Section 39c of the Act the judge shall issue a written usage authorization

³⁵ Ibid.

³⁶ *Objections to the Amendment draft made during law-making process* [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>

for a specific individual, in the case of pre-determined categories of persons under Section 39b of the Act the judge shall only authorize the commencement of the system, but not its use in relation to specific persons. This is problematic for several reasons.³⁷

First of all, in many cases it may not be entirely clear on what basis the competent judge is supposed to make a decision in granting permission if he does not know how the system will be used. The benefit of the system is the ability to identify a specific person at a specific time in a specific place. From this, the competent judge can make a satisfactory assessment of the specific location, but the temporal and personal scope of the use of the system is at the later discretion of the system operator, which at the very least conflicts with the principle of predictability and also the requirement of lawfulness of the interference with the right to respect for private life under Article 8 of the European Convention on Human Rights. It should also be noted that the proposed legal regulation does not comply with the AI Act. According to Article 5(3) of the AI Act, each use of the system is subject to prior authorization by a court or an independent administrative authority. In contrast, the proposed legal regulation of the Act provides for the authorization of an unlimited number of uses under conditions predefined only in outline.³⁸

It can be said that certain supervisory mechanism shall be the notification of the inclusion of persons in the database to the commissioner. As regards the position of the commissioner, their authorization under Section 39b(9) of the Act, according to which they are supposed to assess the inclusion of biometric data of each specific person and to express their consent or disagreement with this inclusion, is highly doubtful. The reason for this conclusion is that in the case of the isolated system operated by the Police of the Czech Republic at the Airport, this would certainly create a conflict of interest if the inclusion of a particular person should be decided by a commissioner on duty at the Presidium of the Police of the Czech Republic. This is further related to the delegation of the commissioner to supervise the reference database under Section 39b(3)(d) of the Act. Article 14 of the AI Act, regulating the human supervision of high-risk AI systems, implies the measures by which human supervision is ensured. However, the content of Article 14(4) of the AI Act suggests the position of a person fulfilling more the role of an administrator with continuous access, so it is a matter for consideration whether the commissioner in the sense of the Act is a person who can fulfil these measures. Related to this is the fact that this is not compatible with the status of the commissioner as defined in Article 39 of the Regulation (EU) 2016/679. By

³⁷ Ibid.

³⁸ Ibid.

its very nature, a delegation of the reference database supervision would give a responsibility to the commissioner, but in the Czech Republic that responsibility belongs to the managing authority in fact. Under the relevant national legal regulation, the commissioner cannot be held personally liable for compliance with data protection requirements. The last objection is the fact that the legal regulation under the Act is not to make it clear on the basis of what information the commissioner shall assess the eligibility of the persons' inclusion in the database, or what information shall be submitted to them for this purpose. Therefore, it can be concluded that the activities of the commissioner under the Act do not meet the quality requirements of the authorization scheme set out in the AI Act and the commissioner is not always an independent body.³⁹

Article 5(4) of the AI Act states that each EU Member State shall lay down in its national law the necessary detailed rules after the adoption of the isolated system, i. e. the relevant rules regulating the isolated system authorization request, issuance and exercise of authorization, as well as the supervision and reporting on them. These rules shall also determine in relation to which of the objectives referred to in Article 5(1)(d) of the AI Act, and in relation to which of the offences referred to in Article 5(1)(d)(iii) of AI Act, the competent authorities may be authorized to use such systems for law enforcement purposes. However, neither the Amendment draft nor the Explanatory Memorandum to the Amendment draft sets out these obligations in a comprehensive way. At the same time, among the mandatory particulars of the system authorization request in Section 39(b)(3) of the Act, there is no indication of what purpose referred to in Section 39(a)(3) of the Act (and hence in Article 5(1)(d) of the AI Act) the request is to be submitted for.⁴⁰

As to the intended legal regulation under Section 39(b) and Section 39(c) of the Act, it should also be noted that while Section 39(a)(3)(a) to (d) of the Act, i. e. the legal regulation which is intended to identify the persons whose biometric data may be included in the system, complies with the cases listed in Article 5(1)(d)(i) to (iii) of the AI Act, in the case of Section 39(b)(1) of the Act, the proper implementation of the AI Act may be questioned. Regarding their categories, it is not clear what is intended to be the basis for the scope of persons under section 39b(1)(a)(2.) of the Act, as the AI Act does not permit its application to persons suspected of committing an offence other than an offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the EU Member State concerned by a custodial sentence or a detention order

³⁹ *Objections to the Amendment draft made during law-making process* [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>

⁴⁰ *Ibid.*

for a maximum period of at least three years, as determined by the law of that EU Member State. The legislator, in the special part of the Explanatory Memorandum to this provision of the Act, mentions the condition of ‘restriction of personal liberty in combination with the condition of a specific threat to life or health’ in the sense of Article 5(1)(d)(ii) of the AI Act, but it is not possible to agree with this conclusion. The condition of the system’s use for the prevention of a specific, serious and imminent threat to the life or physical safety of natural persons should be interpreted restrictively and not applied to persons suspected, accused or charged of any crime essentially.⁴¹

Related to the above, there is similar doubt about the group defined in the following Section 39b(1) (b)(2), which shall include persons who are wanted and whose personal liberty may be restricted. However, according to the conclusion of the legislator, in such a case, the reason for the restriction of personal liberty must not be related to criminal activity, so that the restriction set out for criminal offences in Article 5(1)(d)(iii) of the AI Act would not be circumvented. In the context of the intended legal regulation under Section 39(b)(1)(a) of the Act, this conclusion of the legislator is not understandable.⁴²

Finally, Section 39c(2) of the Act implies that data and records shall not be destroyed if it is necessary to document acts already performed in connection with the use of an isolated system. This is completely inconsistent with Point no. 35 of the Position of the European Parliament, adopted with a view to the adoption of the AI Act, which without more calls for the immediate, within 24 hours, discarding and deletion of the results and outputs of the system’s use. Moreover, it is not entirely clear whether and how the legislator assessed the necessity, proportionality and riskiness of the personal data processing. The Explanatory Memorandum refers to the fact that the Amendment draft introduces rules for the existing use of urgent remote biometrics. However, the fact that such systems are already in use does not guarantee their compliance with data protection and there is no reason not to assess their necessity, proportionality and risk-taking. The tightening of the conditions for the use of such technologies by the AI Act applies to both the existing systems and the future ones.⁴³

In the context above, the application of the isolated system to persons referred to in Section 39(b)(1)(a)(2) and (b)(2) of the Act under Article 5(1)(d)(i) to (iii) of the AI Act needs to be clarified, or the text of the Act needs to be modified to be consistent with the restrictive concept of the AI Act, and to ensure that biometric data of persons, not anticipated by the AI Act, are not included in the

⁴¹ *Objections to the Amendment draft made during law-making process* [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>

⁴² Ibid.

⁴³ Ibid.

reference database. The same goes for Section 39c(1) of the Act, which lacks the ‘indispensable necessity’ and ‘necessary extent’ conditions as a guarantee of the limits set out in Article 5(1)(d) of the AI Act.⁴⁴

4. Conclusions

As for the situation in Ukraine, it should be noted that the adoption of the draft Law of Ukraine ‘On the Unified System of Video Monitoring of the State of Public Security’ poses risks of violating human rights and freedoms, and will significantly limit the fundamental right of every person to privacy. In order to ensure proper legal regulation of video monitoring of public security using facial recognition systems in Ukraine, the draft Law of Ukraine ‘On the Unified System of Video Monitoring of the State of Public Security’ needs to be finalized and brought into line with the above provisions of the relevant EU and Council of Europe legislation.

As for the situation in the Czech Republic, the conclusion is that the AI Act does allow the use of real-time remote biometric identification systems, but under certain conditions. The main one is that the use of such a system to search for a specific person or persons must be authorized by a court or other independent authority. In real terms, this means that the decision to include a particular person in the reference database shall be made by a court. However, in relation to this very basic safeguard against abuse of the system, the Act no. 110/2019 Coll., on the Processing of Personal Data is to propose that this rule shall not be applied to certain relatively vaguely defined groups of persons. Thus, the Act shall negate this fundamental control mechanism in certain cases, in fact.

At first glance, it may seem that the aim of the regulation set up this way is to try to keep the system at the Airport running continuously and essentially in the same mode as it has been operating there since 2018. The Ministry of the Interior is certainly right that the system at the Airport does not identify anyone who is not in the database, but on the other hand, almost anyone can be included in the database without sufficient control. The Ministry of the Interior also fails to add the important fact that the biometric identifications of anyone who is captured and not identified by the system at the Airport shall be retained for an additional three months for possible future use. Originally, the Ministry of the Interior did not envisage limiting the scope of the regulation under the Act only to international airports. However, when a number of comments were made

⁴⁴ *Objections to the Amendment draft made during law-making process* [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>

on the Act, the Ministry of the Interior relented and, apparently in an effort to push the Act through the legislative process, limited the possibility of using the systems to international airports only. However, the Explanatory Memorandum to the Amendment draft makes it quite clear that there is an intention to use the systems elsewhere in the future.⁴⁵

List of references

- АВДЄЄВА, Т. Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? [online]. Available at: <https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/>
- FUJÁČEK, J. „Nejde o velkého bratra,“ říká policie o identifikaci obličejů. Úřad po ní žádá vysvětlení [online]. Available at: <https://www.echo24.cz/a/HJrg8/zpravy-domaci-kamery-system-rozpoznavani-obliceju-policie-tvare-velky-bratr-dpo-prezident>
- GURIDI, E., FRANCISCO, J. THE USE OF ARTIFICIAL INTELLIGENCE (AI) SYSTEMS FOR REMOTE BIOMETRIC IDENTIFICATION IN PUBLICLY ACCESSIBLE SPACES IN THE EUROPEAN AI LAW. *Actualidad Jurídica Iberoamericana*. 2024, 21, pp. 528–565.
- HANDREJCHOVÁ, M. Úsměv! Sleduje vás AI aneb co přinese novela zákona o zpracování osobních údajů [online]. Available at: <https://www.tx.cz/blog/usmev-sleduje-vas-ai-an-eb-co-prinese-novela-zakona-o-zpracovani-osobnich-udaju>
- HERRERA, F., DIGNUM, V., PACHET, F. et al. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14967 LNAI, 23rd EPIA Conference on Artificial Intelligence, Viana do Castelo, 3–6 September 2024, code 323069.
- HOFFMEISTER, K. The Dawn of Regulated AI: Analyzing the European AI Act and its Global Impact. *Zeitschrift für Europarechtliche Studien*. 2024, 27(2), pp. 182–212.
- JASSERAND, C. The Future AI Act and Facial Recognition Technologies in Public Spaces: Nice to Have or Strictly Necessary? *European Data Protection Law Review*. 2023, 9(4), pp. 430–443.
- KIESLICH, K., LÜNICH, M. ECG Regulating AI-Based Remote Biometric Identification. Investigating the Public Demand for Bans, Audits, and Public Database Registrations. *2024 ACM Conference on Fairness, Accountability, and Transparency, FAccT 2024*, Rio de Janeiro, 3–6 June 2024.
- LEUCKER, M. The AI Act and Some Implications for Developing AI-Based Systems. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 15240 LNCS, pp. 202–214, 2024.
- MACH, V., VOBORIL, J. Český Minority Report – Využití umělé inteligence Policií České republiky [online]. Available at: <https://digitalnisvobody.cz/uploads/2024/01>

⁴⁵ Digitálně-právní organizace IuRe. *Co jste nechtěli vědět o biometrickém dohledu v Česku a bálí jste se zeptat* [online]. Available at: <https://digitalnisvobody.cz/blog/2024/09/24/co-jste-nechteli-vedet-o-biometrickem-dohledu-v-cesku-a-bali-jste-se-zeptat/>

- MACH, V., VOBOŘIL, J. *Využití biometrie při sledování veřejného prostoru v České republice* [online]. Available at: <https://digitalnisvobody.cz/uploads/2021/02>
- McCURDY, W. *UN High Commissioner says facial recognition could lead to destruction of privacy* [online]. Available at: <https://www.biometricupdate.com/202307/un-high-commissioner-says-facial-recognition-could-lead-to-destruction-of-privacy>
- MILOSSI, M. ECG Remote biometric identification systems and ethical challenges: The case of facial recognition. *6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference, SEEDA-CECNSM*, Preveza, 24–26 September 2021.
- MOHD, A. et al. ECG Biometric Verification Incorporating Different Physiological Conditions. *Journal of Advanced Research in Applied Sciences and Engineering Technology*. 2024, 51(2), pp. 97–110.
- MOREIRA, N. A., FREITAS, P. M. Towards Transparent AI: How will the AI Act Shape the Future? *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 14967 LNAI, pp. 296–307, 2024.
- NEUWIRTH, R. J. Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). *Computer Law and Security Review*. 2023, 48.
- ВОЙНОВ, М. Система розпізнавання обличчя: правові аспекти використання в Україні та в ЄС [online]. Available at: <https://www.helsinki.org.ua/articles/systema-rozpiznavannia-oblychchia-pravovi-aspekty-vykorystannia-v-ukraini-ta-v-yes/>
- ТИМЧЕНКО, Л. Користувачі систем відеомоніторингу нестинуть відповідальність за незаконне розповсюдження даних [online]. Available at: <https://mvs.gov.ua/news/leonid-timchenko-koristuvaci-informaciyi-z-kamer-videosposterezennia-nestimut-vid-povidalnist-za-nezakonne-rozpovsiudzhennia-danix>
- XIAOHAN, Y. A face authentication-based searchable encryption scheme for mobile device. *Journal of Supercomputing*. 2024, 81(1).
- CSPA. *Проект Закону про єдину систему відеомоніторингу стану публічної безпеки* [online]. Available at: <https://cspa.digital/video-surveillance/>
- DIGITÁLNĚ-PRÁVNÍ ORGANIZACE IuRe. *Co jste nechtěli vědět o biometrickém dohledu v Česku a báli jste se zeptat* [online]. Available at: <https://digitalnisvobody.cz/blog/2024/09/24/co-jste-nechteli-vedet-o-biometrickem-dohledu-v-cesku-a-bali-jste-se-zeptat/>
- DIGITÁLNĚ-PRÁVNÍ ORGANIZACE IuRe. *Kamery rozpoznávající tváře na letišti v Praze jsou v souladu se zákonem* [online]. Available at: <https://digitalnisvobody.cz/blog/2021/11/30/kamery-rozpoznajaci-tvare-na-letisti-v-praze-jsou-v-souladu-se-zakonom/>
- POLICIE ČESKÉ REPUBLIKY ÚŘAD SLUŽBY KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ POLICEJNÍHO PREZIDIA ČESKÉ REPUBLIKY. *Posouzení vlivu na ochranu osobních údajů k informačnímu systému Digitálních podob osob v souladu s § 37 zákona č. 110/2019 Sb., o zpracování osobních údajů* [online]. Available at: <https://uouo.gov.cz/media/poskytnute-informace/2023/2092023/4-posouzeni-vlivu-na-ochranu-osobnich-udaju-dpia-dokument-c-4.pdf>
- SPIILNO.ORG. *Україна ігнорує вимоги ЄС щодо систем відеоспостереження в публічних місцях* [online]. Available at: <https://spilno.org/article/ukraina-ihnoryue-vy-mohy-yes-schodo-system-videosposterezhennya-v-publicnykh-mistsyakh>

- Amendment draft to the Act no. 110/2019 Coll., on the Processing of Personal Data* [online]. Available at: <https://odok.cz/portal/veklep/material/KORND34KYGTD/>
- Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part* [online]. Available at: https://zakon.rada.gov.ua/laws/show/984_011
- Draft Law of Ukraine ‘*On the Unified System of Video Monitoring of the State of Public Security*’. No. 11031 of 20 February 2024 [online]. Available at: <https://itd.rada.gov.ua/billInfo/Bills/Card/43733>
- Guidelines for local self-government bodies ‘*Video surveillance in public places*’ [online]. Available at: http://labs.journ.univ.kiev.ua/hrj/wp-content/uploads/2021/07/Відеоспостереження-в-публічних-місцях_ПОСІБНИК.pdf
- Objections to the Amendment draft made during law-making process [online]. Available at: <https://odok.cz/portal/veklep/material/pripominky/KORND34KYGTD/>
- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [online]. Available at: https://zakon.rada.gov.ua/laws/show/994_326#Text
- The European Convention on Human Rights* [online]. Available at: https://zakon.rada.gov.ua/laws/show/995_004#Text
- The Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* [online]. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
- The 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 (the General Data Protection Regulation)*. [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- The 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 (the AI Act)*. [online]. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- The Resolution of the Parliamentary Assembly of the Council of Europe on ‘Video surveillance of public areas’* [online]. Available at: http://w1.c1.rada.gov.ua/pls/mpz2/docs/769_1604.htm