PWPM 2023, Vol. XXI
PROBLEMY WSPÓŁCZESNEGO PRAWA MIĘDZYNARODOWEGO, EUROPEJSKIEGO I PORÓWNAWCZEGO
REVIEW OF INTERNATIONAL, EUROPEAN AND COMPARATIVE LAW
ISSN 1730-4504

ARTYKUŁY / ARTICLES

DOI: 10.26106/q3ta-bv90

The use of 'real-time' remote biometric identification systems for law enforcement – comments in light of legislative work on the Artificial Intelligence Act

Aleksander Mitka
Candidate for LL.M. in International & European Law, University of Wrocław
https://orcid.org/0009-0008-5363-2542; e-mail: mitka.aleksander@gmail.com

Introduction

The proposal for the Artificial Intelligence Act (AIA)[1] was put forward by the European Commission (EC) in 2021. During the legislative process, one of the most controversial issues concerned the use of 'real-time' remote biometric identification systems (RTRBIS) in publicly accessible spaces for the purpose of law enforcement. There were many discrepancies between the positions of the EU institutions on this issue, but they came to an agreement on the final version of the AIA in December 2023. The legislative process itself was closely followed by the media and various stakeholders, including networks of organizations concerned with privacy protection. However, it is to be regretted that the process of negotiating the agreement on the final version of the AIA was not conducted in a transparent manner (at the time

[1] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final.

of submitting this article, neither the content of the agreement nor the final version of the AIA is publicly known). In light of the comparisons and discrepancies in the submitted amendments,[2] it can be expected that the use of RTRBIS in publicly accessible spaces for law enforcement purposes under the AIA will be subject to a relative prohibition. That is, while the default is to prohibit the use of RTRBIS in such circumstances, there will be limited grounds to override this prohibition.

The purpose of this article is therefore to analyze the legislative process concerning the use of RTRBIS, taking into account the EC's draft and the amendments tabled by the European Parliament (EP) and the Council of the European Union (EU Council). The article presents the controversies accompanying the legislative work on the general nature of the AIA and the specific wording of Article 5. The article asks the question of the consequences of adopting different regulatory solutions of RTRBIS for legal practice. To this aim, the article compares the original provisions of the EC's draft with the versions proposed by the EP and the EU Council in tabular form, which will help to clarify the divergences between these institutions on this matter. The discussion of the legislative process is placed in the context of broader debates on legal issues related to artificial intelligence, including the use of facial recognition technology (FRT), which includes RTRBIS.

Currently, no EU Member State has a law that regulates these issues comprehensively. Moreover, there are no such laws in the world.[3] The EC drew attention to the development of AI as early as May 2017, when it announced its intention to regulate AI at the European level.[4] In December 2018, an AI strategy issued by the EC was published, providing the necessary context and legislative direction. [5] In turn, in February 2020, the EC published a white paper on AI. [6] At the time,

[2] Interinstitutional File: 2021/0106(COD), Brussels, 25 November 2022, available at: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf, access date: 10.12.2023.

[3] D. Almeida, K. Shmarko, E. Lomas, *The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks*, "AI and Ethics" 2022, no. 2, p. 380.

[4] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the mid-term review on the implementation of the digital single market strategy. A connected digital single market for all, Brussels, 10 May 2017, COM(2017) 228 final, p. 11.

[5] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Coordinated plan on artificial intelligence, Brussels, 7 December 2018, COM(2018) 795 final.

[6] White paper on artificial intelligence – a European approach to excellence and trust, Brussels, 19 February 2020, COM(2020) 65 final.

the public debate pointed out that an EU regulatory act on AI would help the EU in the great race for supremacy in AI development with the US and China, given that, according to the World Intellectual Property Organization, about 85% of patents related to AI belonged to US and Chinese companies, while ensuring that EU citizens were duly protected from the dangers of AI development.[7] The European Council debated the development of artificial intelligence in October 2020. In its conclusion, it stressed its desire for the EU to become a world leader "in the development of safe, trustworthy and ethical artificial intelligence," encouraging the EC to continue its work in this area.[8]

The proposal of the AIA saw the light of day on 21 April 2021, when the EC published it along with a coordinated plan for Member States on AI.[9] The proposed AIA has taken the form of a horizontal EU regulation based on Article 16 (protection of personal data) and Article 114 (approximation of laws in the internal market) of the Treaty on the Functioning of the European Union (TFEU). It has been proceeded under the ordinary legislative procedure. The proposal aimed to regulate the development, use, and marketing of AI systems within the EU based on a risk-based approach.[10] It was intended to be the first legal act to comprehensively regulate AI globally. As such, is has the potential to become a model regulation for other countries around the world, especially given the impact of EU legislation on the international legal environment and related *Brussels effect*.[11]

Controversies over shape of AIA between EU institutions

No doubt, regulating the use of AI has become a necessity for Europe in the face of legally uncontrolled technological advances. From the outset, the purpose of

---

7 S. Amiel, *Artificial intelligence: how is the EU planning to make up ground on US and Chinese firms?*, "Euronews", 19 February 2020, https://www.euronews.com/2020/02/19/the-eu-s-new-ai-strategy-what-you-need-to-know, access date: 7.12.2023.

8 EUCO 13/20, Brussels, 2 October 2020, https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf, access date: 7.12.2023.

9 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Fostering a European approach to Artificial Intelligence, Brussels, 21 April 2021, COM(2021) 205 final.

10 Artificial Intelligence Act, European Parliamentary Research Service, June 2023, p. 3, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf, access date: 7.12.2023.

11 S. Feldstein, *Evaluating Europe's push to enact AI regulations: how will this influence global norms?*, "Democratization", April 2023, p. 8–9.

this regulation has been to legally control AI and impose restrictions on its use with particular attention to its impact on fundamental rights. In light of these assumptions, it is expected that the AIA will have a positive impact on the protection of fundamental rights. The real subject of controversy was the scale of the restrictions that were to be imposed by this regulation on individuals, as well as on member states carrying out their law enforcement tasks.

This dispute among three EU institutions became apparent during the legislative process in which the EP adopted 771 amendments to the AIA.[12] The adoption of these amendments could have led to a substantial change in the direction of this regulation. The EP's position on the AIA was broadly in line with its non-binding resolution adopted at the July 2021 plenary session.[13] The amendments were adopted by an overwhelming majority (499 votes in favor, 28 against and 93 abstentions),[14] underscoring the EP's determination and unanimity on the issue. Substantial amendments were also proposed by the EU Council,[15] although its position was not so radically different from the EC's intentions.

The proposed amendments ranged from purely cosmetic and linguistic changes to requests to remove entire provisions and introduce new ones. This resulted in regular legislative deadlocks and heated discussions that even led to doubts about the possibility of reaching an agreement in the trilogue.[16]

The purpose of the proposed Regulation is found in recital 1 of the preamble to the AIA. The EU Council fully agreed with the EC's version. At the same time, the EP expected a fundamental recasting of its provision, leading, in fact, to a far-reaching modification of the objectives the AIA.

---

[12] Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html, access date: 10.12.2023.

[13] Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), Committee on Civil Liberties, Justice and Home Affairs, https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf, access date: 24.11.2023.

[14] https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1747977&t=d&l=en, access date: 24.11.2023.

[15] https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf, access date: 24.11.2023.

[16] L. Bertuzzi, *EU's AI Act negotiations hit the brakes over foundation models,* Euractiv, 10 November 2023, https://www.euractiv.com/section/artificial-intelligence/news/eus-ai-act-negotiations-hit-the-brakes-over-foundation-models/, access date: 24.11.2023.

Recital 1 to the AIA	
European Commission	European Parliament
(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with Union values. This Regulation pursues a number of overriding reasons of public interest, such as a high level of protection of health, safety and fundamental rights, and it ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.	**(1)** The purpose of this Regulation is to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law and the environment from harmful effects of artificial intelligence systems in the Union while supporting innovation and improving the functioning of the internal market. This Regulation lays down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence in conformity with Union values and ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of Artificial Intelligence systems (AI systems), unless explicitly authorised by this Regulation. Certain AI systems can also have an impact on democracy and rule of law and the environment. These concerns are specifically addressed in the critical sectors and use cases listed in the annexes to this Regulation.

In this juxtaposition, it can be seen that the EC put the internal market first, while emphasizing the importance of the AIA for safeguarding EU values and protecting fundamental rights. The EP's approach was quite different in that its amendments brought fundamental rights to the fore. Comments published by MEPs outline the rationale for the EP's position at the time. Eugen Tomac stressed that the vote on the amendments to the proposed AIA was a historic event, and looks forward to the creation of mechanisms to protect citizens to ensure that artificial intelligence, used by both state and private entities, will not be abused and undermine democracy. In contrast, Mick Wallace noted that without proper regulation, artificial intelligence will intensify "mass surveillance, structural discrimination, centralized Big Tech power and unaccountable public decision-making."[17]

[17] https://www.europarl.europa.eu/doceo/document/CRE-9-2023-06-14-ITM-020-01_EN.html, access date: 25.11.2023.

The concerns expressed by MEPs are understandable and justified. Although the development of artificial intelligence and accompanying technologies is a relatively recent phenomenon, there are well-known examples of what the new technologies' potential is for restrictions and violations of human rights, as well as strengthening authoritarian regimes in countries such as China, Russia and India. The use of RTRBIS or related technologies has been crucial in this regard. In China, FRT has been used to detect misdemeanors and publicly harass petty criminals,[18] suppress protests[19] and persecute the Uighur minority.[20] In Russia, a dense network of cameras in Moscow with facial recognition was actively used to track political opponents of the regime[21] or evaders of military conscription in the context of the aggression against Ukraine.[22] Similar solutions are in place in India, where comprehensive surveillance systems using FRT, among other things, have been implemented at the local level. These systems have been criticized by NGOs[23] and have raised legitimate concerns among India's numerous minorities.[24]

With these examples in mind, the EU has taken steps to minimize the risk of similar threats in the future within its jurisdiction and to protect fundamental rights in the face of new challenges. For this reason, RTRBIS proved to be one of the sticking points in the negotiations between the EC, the EU Council and the EP under Article 5(1)(d) of the AIA. The impasse on this point and on the AIA as a whole was broken in the first half of December 2023, as confirmed in

[18] D. Davies, *Facial recognition and beyond: journalist ventures inside China's 'surveillance state',* NPR, 5 January 2021, https://www.npr.org/2021/01/05/953515627/facial-recognition-and-beyond-journalist-ventures-inside-chinas-surveillance-sta, access date: 9.12.2023.

[19] P. Mozur, C. Fu, A. Chien, *How China's police used phones and faces to track protesters*, "New York Times", 2 December 2022, https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html, access date: 1.12.2023.

[20] S. Feldstein, *China's high-tech surveillance drives oppression of Uyghurs*, "Bulletin of the Atomic Scientists", 27 October 2022, https://thebulletin.org/2022/10/chinas-high-tech-surveillance-drives-oppression-of-uyghurs/, access date: 1.12.2023.

[21] L. Masri, *How facial recognition is helping Putin curb dissent with the aid of U.S. tech,* Reuters, 28 March 2023, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/, access date: 9.11.2023.

[22] A. Kruope, *Russia uses facial recognition to hunt down draft evaders*, Human Rights Watch, 26 October 2022, https://www.hrw.org/news/2022/10/26/russia-uses-facial-recognition-hunt-down-draft-evaders, access date: 9.11.2023.

[23] *India: Hyderabad 'on the brink of becoming a total surveillance city'*, Amnesty International, 9 November 2021, https://www.amnesty.org/en/latest/news/2021/11/india-hyderabad-on-the-brink-of-becoming-a-total-surveillance-city/, access date: 9.11.2023.

[24] *Facial recognition taken to court in India's surveillance hotspot*, Al Jazeera, 20 January 2022, https://www.aljazeera.com/news/2022/1/20/india-surveillance-hotspot-telangana-facial-recognition-court-lawsuit-privacy, access date: 9.07.2023.

the December 9, 2023 press releases of the EU Council[25] and the EC, [26] resulting in an agreement on a common version of the AIA between the three institutions.

Definitions of 'biometric data,' 'remote biometric identification system' and 'real-time remote biometric identification system'

As a preliminary matter, it is worth noting that the definition of 'biometric data'[27] contained in Article 3(33) of the AIA is a slightly modified definition adopted in the General Data Protection Regulation[28] (GDPR), the Law Enforcement Directive[29] (LED) and the Regulation on the protection of natural persons with regard to the processing of personal data by the Union institutions.[30] Recital 7 of the Preamble to the AIA confirms that the definition of biometric data contained in the AIA is consistent with the definition of biometric data found in these three acts and should be interpreted uniformly. In this regard, the EP suggested referring directly to the definition contained in the GDPR. At this place, it also needs to be emphasized that the proposed AIA did not address the issue of the length of storage of biometric data. This issue will, therefore, be regulated by default by the LED.

---

[25] *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world*, Consilium Europa, 9 December 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/, access date: 10.12.2023.

[26] *Commission welcomes political agreement on Artificial Intelligence Act*, 9 December 2023, https://ec.europa.eu/commission/presscorner/detail/%20nl/ip_23_6473, access date: 10.12.2023.

[27] According to Article 3(33) of the AIA, 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

[28] 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, p. 1).

[29] 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, p. 89).

[30] 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 (OJ L 295, p. 39).

In order to understand what a '<real-time> remote biometric identification system' means, it is first necessary to look at the definition of 'remote biometric identification system' (RBIS) in Article 3(36) of the proposed AIA. Under this provision, drafted by the EC, RBIS is an AI system that serves to identify individuals remotely by comparing their biometric data with data contained in a reference database, whereby the user[31] of the system has no prior knowledge that the individual's data is in the database, nor does he or she know that he or she may be subject to identification. Already here, the first discrepancies appeared, as the EU Council wanted to remove the premise of the user's lack of awareness and to replace the term 'database' with 'data repository.'

According to Article 3(37) of the proposed AIA, a RTRBIS is a sub-type of RBIS in which the collection and processing of biometric data takes place without significant delay. The definition also indicates that, in order to avoid circumvention, a system in which identification occurs immediately, but also with a slight delay, should also be considered an RTRBIS. This provision should be read in light of Recital 8 of the AIA, which states that the term RTRBIS should be defined functionally, irrespective of the specific technology, processes and types of biometrics used by the system. RTRBIS can therefore include FRT, as long as it operates remotely and without significant latency.

Leaving aside the differences between the definitions proposed by the three institutions, three main features of RTRBIS can be highlighted:

1) it is an artificial intelligence system for the remote biometric identification of persons;
2) the system is based on a reference database with previously entered biometric data of persons;
3) the system recognizes persons immediately or with a slight delay.

The EC proposed to include RTRBIS systems in the category of high-risk artificial intelligence systems. A list of such systems is provided in Annex III to the Regulation. According to Recital 33 of the AIA, the need to create a category of high-risk systems stems from their profound interference with fundamental rights, which is particularly related to the technical inadequacies of such systems. In practice, the inclusion of a system in the high-risk category will mean that

[31] Article 3(4) of the AIA proposal defines it as "any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity." In contrast, the EP suggested to change the term 'user' for 'deployer,' while Council of the EU described a user as "any natural or legal person, including a public authority, agency or other body, under whose authority the system is used."

such a system will be comprehensively regulated by the AIA under its Title III (High-risk AI systems).

In contrast, Article 3(38) of the AIA provides that a '<post> remote biometric identification system' is to be distinguished from an RTRBIS, which is any RBIS that is not an RTRBIS, so that the identification process is more deferred. The EP agreed with this definition, while the EU Council wanted to drop the introduction of this definition in the AIA.[32]

(Relative) ban of RTRBIS in publicly accessible spaces for the purpose of law enforcement

The key provision on the use of RTRBIS is Article 5(1) of the AIA. The EC's 2021 draft reflected its compromise approach to balancing the protection of fundamental rights with technological progress, emphasizing the principle of proportionality in the use of RTRBIS. The EC's concerns are expressed in the Preamble, which recognizes the profound interference of the RTRBIS with the freedoms and rights of the persons concerned.[33] It was therefore the Commission's intention to impose a rigid restriction on the use of RTRBIS in publicly accessible spaces[34] for law enforcement purposes. To this end, the proposal provided for only three instances of permissible use of this technology listed in Article 5(1)(d).[35] Article 5(1)(d) of the AIA should, according to recital 23 of the Preamble, be treated as *lex specialis* with regard to Article 10 of the LED, which regulates the processing of special categories of personal data, including biometric data.

The EU Council primarily agreed with the EC's proposal on this matter, but made a number of amendments, both of a technical and purely formal nature. A completely different view of the use of RTRBIS was taken by the EP, which decided to strongly oppose any use of RTRBIS in the public space, and to significantly expand the catalogue of prohibited practices in Article 5(1). The result of the divergence of vision between the EC and the EU Council on the one hand, and the EP on the other, was the proposed provisions of Article 5(1)(d) indicated below:

---

32 Article 3(38) was deleted from the EU Council document of 25 November 2023.

33 Recital 18 to the AIA.

34 According to recital 9 to the AIA, the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned.

35 Recital 19 to the AIA.

Article 5(1)(d) of AIA		
European Commission	EU Council	European Parliament
1. The following artificial intelligence practices shall be prohibited: [...] **(d)** the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives: **(i)** the targeted search for specific potential victims of crime, including missing children; **(ii)** the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack; **(iii)** the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, as determined by the law of that Member State.	**1.** The following artificial intelligence practices shall be prohibited: [...] **(d)** the use of 'real-time' remote biometric identification systems in publicly accessible spaces by law enforcement authorities or on their behalf for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives: **(i)** the targeted search for specific potential victims of crime; **(ii)** the prevention of a specific and substantial threat to the critical infrastructure, life, health or physical safety of natural persons or the prevention of terrorist attacks; **(iii)** the localisation or identification of a natural person for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for offences, referred to in Article 2(2) of Council Framework Decision 2002/584/JHA and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years, or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years, as determined by the law of that Member State.	**1.** The following artificial intelligence practices shall be prohibited: [...] **(d)** the use of 'real-time' remote biometric identification systems in publicly accessible spaces. **(i)** *deleted* **(ii)** *deleted* **(iii)** *deleted*

The provisions proposed by the EC and the EU Council formulate a relative prohibition which allows an exemption to the prohibition of the use of RTRBIS

for law enforcement purposes in certain cases. Article 5(1)(d)(iii) contains a closed catalogue of offences for which RTRBIS may be used, referring to Article 2(2) of Council Framework Decision 2002/584/JHA.[36] This provision states that the listed offences may form the basis of a European Arrest Warrant provided they are punishable in the issuing State by a custodial sentence or a detention order for a minimum period of three years. This provision has caused a great deal of controversy because the right to issue a European Arrest Warrant has been abused on the basis of this provision and has led, for example, to the prosecution of bicycle or car tires thieves[37] and possessors of negligible amounts of cannabis.[38] It can therefore be assumed that similar offences will be able to form the basis for the lawful application of the RTRBIS under this provision of the AIA.

In addition to cosmetic or clarifying changes, the EU Council expected letter (d) to be modified by supplementing the exemption clause of the RTRBIS prohibition with a provision on the prevention of a specific and serious threat to critical infrastructure and health. Critical infrastructure was to be defined by the point added by the EU Council to Article 3 of the AIA as "an infrastructure component, system, or part thereof that is necessary to provide a critical service for the maintenance of essential societal functions or economic activity within the meaning of Articles 2(4) and 2(5) of Critical Entities Resilience Directive."[39] In this regard, Article 2(5) of the said Directive defines a 'essential service,' a feature of critical infrastructure, as one that is essential for the maintenance of essential societal functions, economic activity, public health and safety or the environment. The inclusion of the critical infrastructure provision in the AIA by the EU Council seems a reasonable and proportionate addition to the rationale for exempting the default prohibition in Article 5(1)(d) of the AIA,. At the same time, it should be emphasized that this addition introduces another broad category of situations exempting the default prohibition.

Moreover, the EU Council intended to broaden the scope of Article 5(1)(d)(iii) to include not only the offenses contained in the catalog of Framework Decision 2002/584/JHA, but also other offences which are punishable by a custodial

[36] Notably, this catalogue counts 32 types of offences.

[37] O. Bowcott, *Trivial cases undermining European arrest warrants, warns Brussels*, "Guardian", 10 April 2011, https://www.theguardian.com/law/2011/apr/10/trivial-undermine-european-arrest-warrants, access date: 25.11.2023.

[38] https://data.consilium.europa.eu/doc/document/ST-10975-2007-INIT/en/pdf, access date: 25.11.2023.

[39] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, p. 164).

sentence or a detention order for more than 5 years under national law. The EU Council therefore expected more enforcement powers for state authorities in this respect.

As shown above, adopting the AIA in the original EC version would have allowed for a quite broad and uncountable catalog of exemptions to the Article 5(1)(d) prohibition and the adoption of the EU Council amendments would only compound this problem.

The EP remained reluctant to allow the use of RTRBIS for a long time. However, minor concessions leading to a limited authorization of the use of RTRBIS in public spaces for law enforcement purposes were considered in the negotiations, in return for which the EP expected to recognize its amendments. In the EP's amendments, the proposed wording of Article 5(1)(d) would not only prohibit the use of RTRBIS in front of public entities for law enforcement purposes, but would also prevent private entities from implementing such systems in public spaces for their own purposes. In practice, for example, it would not be possible for a private organizer of a mass event to use RTRBIS to prevent selected individuals from entering the event premises.[40] This is a radical solution that, while it would be most beneficial from the point of view of protecting fundamental rights, would prevent the use of a highly effective technology for law enforcement. At the same time, it is doubtful that the world would willingly replicate this solution within its legal framework. Nevertheless, according to recent reports, an absolute ban was not envisaged as part of the agreement between the three EU institutions,[41] which ended up with only a relative ban.

Finally, it should be noted that with respect to the definition of RTRBIS, according to the joint position of the European Data Protection Board and the European Data Protection Supervisor, [42] the lack of clarification of what

[40] One example of such a scenario is using FRT by Madison Square Garden to keep enemy lawyers out of its venues. See: I. Ivanova, *Madison Square Garden uses face recognition to keep out enemy lawyers. That may be illegal*, CBS News, 26 January 2023, https://www.cbsnews.com/news/madison-square-garden-face-recognition-illegal-new-york-attorney-general-letitia-james/, access date: 2.12.2023.

[41] *EU: Bloc's decision not to ban public mass surveillance in AI Act sets a devastating global precedent*, Amnesty International, 9 December 2023, https://www.amnesty.org/en/latest/news/2023/12/eu-blocs-decision-to-not-ban-public-mass-surveillance-in-ai-act-sets-a-devastating-global-precedent/, access date: 10.12.2023.

[42] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf, access date: 25.11.2023.

constitutes 'a significant delay' may create room for circumvention of the prohibition under Article 5(1)(d). The potential loophole would allow to categorise a system as 'post' RBIS instead of RTRBIS. Such an interpretation would make the relative prohibition in Article 5(1)(d) inapplicable, and since the EC's AIA proposal does not provide for similar prohibitions for RBIS "post", public entities would not be limited in its use.[43] The EU Council's amendments did not took this issue into account. However, such a prohibition stems from EP Amendment no. 227, under which the use and commissioning of AI systems to analyze footage from public spaces via 'post' RBIS systems would be relatively prohibited, except in cases where such systems are subject to pre-judicial approval under Union law and are absolutely necessary for a targeted search related to a specific serious crime as defined in Article 83(1) TFEU that has already taken place, for law enforcement purposes. This is a reasonable alternative to the use of RTRBIS in public spaces for law enforcement purposes. In addition, it is worth noting that RBIS 'post' is to be classified, according to the EC version, in the same way as RTRBIS in the high risk category (Annex III to the AIA).

Proportionality assessment of RTRBIS use

Article 5(2) of the AIA is addressed to persons intending to use RTRBIS and to control authorities and embodies the principle of proportionality in the use of this technology. The essence of Article 5(2) sets out the elements that, when analyzed on a case-by-case basis, are necessary to enable the use of RTRBIS in public spaces for law enforcement purposes. The EU Council accepted Article 5(2) in its entirety, as proposed by the EC. However, given its irrelevance in view of the EP's rejection of the grounds permitting for the use of RTRBIS prohibition imposed by Article 5(1)(d), the EP rejected Article 5(2) in its entirety. At his point, it is certain that this provision will appear in the final version of the AIA in a form similar to the EC's version due to the fact that the relative prohibition associated with the use of RTRBIS was retained under the agreement negotiated in December 2023. The EC's proposal reads as follows:

[43] European Commission adoption consultation: Artificial Intelligence Act, European Digits Rights, Brussels, 3 August 2021, p. 12, https://edri.org/wp-content/uploads/2021/08/European-Digital-Rights-EDRi-submission-to-European-Commission-adoption-consultation-on-the-Artificial-Intelligence-Act-August-2021.pdf, access date: 9.12.2023.

Article 5(2) of AIA
European Commission
2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall take into account the following elements: **(a)** the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system; **(b)** the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use, in particular as regards the temporal, geographic and personal limitations.

In the potential use of the RTRBIS, one needs to analyze the potential consequences of two equally important aspects. On the one hand, reference is made to the need for enforcement and prevention, and on the other hand, to respect individual rights and freedoms. Thus, under Article 5(2)(a), it is necessary to assess how serious the harm to the public interest that could be avoided by applying RTRBIS might be. For this purpose, the nature of the situation intended to give rise to the application of RTRBIS shall be taken into account, the seriousness of the situation shall be assessed, the likelihood of the adverse effects of the situation and the magnitude of the potential harm shall be estimated. On the other hand, according to Article 5(2)(b), the judicial or independent administrative authority must take into account the dimension of the rights and freedoms that may be violated against the person or persons who are to be subjected to RTRBIS. Here, too, the severity, likelihood, and magnitude of the consequences if the system is applied must be assessed. In assessing both aspects, the authority further considers the necessary and proportionate safeguards and conditions for using RTRBIS, taking into account temporal, geographical, and personal limitations.

A deeper reflection on Article 5(2)(a) leads to the conclusion that this provision is preventive in nature, as it refers to the estimation of potential damage as a result of the non-application of the system and, therefore, its potential occurrence and an attempt to prevent it.

Article 5(2) of the AIA must be read in the light of Article 52 of the Charter of Fundamental Rights (CFR), which, inter alia, imposes general principles according to which rights under the CFR, with the exception of rights considered

absolute, may be limited.[44] In this case, the principle of proportionality (Article 52(1) of the CFR) plays a key role. Furthermore, in order to be considered lawful, a limitation of fundamental rights must be based on a law, respect the essence of the rights, serve a general interest recognized by the Union or the need to protect the rights and freedoms of others.[45]

The EU legislator rightly points out in the Explanatory Memorandum of the draft AIA and the Preamble[46] that RTRBIS used for law enforcement purposes restricts rights and freedoms belonging to both the public and the individual, which derive, inter alia, precisely from the CFR. The principle of proportionality therefore requires that the use of RTRBIS be proportionate to the purpose it serves. Thus, in recognizing that the technology constitutes an intrusion into the sphere of private life of individuals, it is to be expected not only that its use is precisely regulated by law, but also that it is appropriate and necessary for a legitimate law enforcement purpose. In particular, the question of the necessity of the measure relates to the assessment of the effectiveness of other alternatives (technologies) that constitute a lesser intrusion into the sphere of private life of individuals. In turn, proportionality stricto sensu requires that the marginal benefits of its application outweigh the marginal costs to the individual. These requirements are reflected in Article 5(2) of the AIA.

According to the impact assessment of the AIA,[47] the RTRBIS used for law enforcement can, in various circumstances of its application, lead in particular to violations of Article 1 (human dignity), Article 7 (respect for private and family life), Article 8 (protection of personal data), Article 11 (freedom of expression), and Article 12 (freedom of assembly and association) of the CFR. On the other hand, it should be mentioned that, due to technological limitations, there is also a risk of violating Article 21 (non-discrimination); according to a 2018 study by researchers at the Massachusetts Institute of Technology and Standford University on the effectiveness of FTR systems, the systems tested showed error-rates of no more than 0.8 percent for white men, however, error-rates for black women

---

44 K. Lenaerts, *Limits on limitations: the essence of Fundamental Rights in the EU*, "German Law Journal" 2019, vol. 20, is. 6, p. 792.

45 *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit*, European Data Protection Supervisor, 11 April 2017, p. 4.

46 Recital 18 to the AIA.

47 Impact assessment accompaying the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts, Brussels 21 April 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0084, access date: 5.12.2023.

exceeded 20 percent.[48] Many similar studies have been conducted, and the results were similar. Arrests made on the basis of incorrect identification by the system, which in particular relate to persons of non-white complexion, undoubtedly constitute racial discrimination.[49]

Authorization of RTRBIS use

The provision of Article 5(3) is an extension of Article 5(2) and is mainly addressed to the judicial or competent administrative authority whose task is to control and authorize the use of RTRBIS (controlling authority) at the request of the authority intending to use the system in each individual case. There was a slight divergence between the EC and the EU Council with regard to Article 5(3). In contrast, Article 5(3) did not apply in the EP proposal.

Article 5(3) of AIA		
European Commission	EU Council	European Parliament
3. As regards paragraphs 1, point (d) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation and the authorisation may be requested only during or after the use.	**3.** As regards paragraphs 1, point (d) and 2, each use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 4. However, in a duly justified situation of urgency, the use of the system may be commenced without an authorisation provided that, such authorisation shall be requested without undue delay during use of the AI system, and if such authorisation is rejected, its use shall be stopped with immediate effect.	**3.** *deleted*

[48] L. Hardesty, *Study finds gender and skin-type bias in commercial artificial-intelligence systems*, "MIT News", 11 February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212, access date: 5.12.2018.

[49] M. Gentzel, *Biased face recognition technology used by government: a problem for liberal democracy*, "Philosophy & Technology" 2021, vol. 34, p. 1643–1648.

Article 5(3) of AIA		
European Commission	EU Council	European Parliament
The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.	The competent judicial or administrative authority shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request. In deciding on the request, the competent judicial or administrative authority shall take into account the elements referred to in paragraph 2.	

In this case, the EU Council requested increased protection of the rights and freedoms of the persons concerned. Its main demand on this issue of Article 5(3) is to add an additional condition to the option provided by the EC, which allows the use of RTRBIS without the consent of the controlling authority. The EC's proposal implies that the option to use RTRBIS without the prior consent of the controlling authority is only possible in well-founded emergencies. However, the provision does not provide clear guidance on the assessment of such a situation. An emergency situation under the EC proposal does not exempt an entity intending to use RTRBIS from the obligation to notify the controlling authority. In this case, the request may be made during or after the use of RTRBIS.

In the EU Council amendment, Article 5(3) states that the use of RTRBIS without the approval of the controlling authority can only take place if, during the already ongoing use of RTRBIS, the user applies for an authorization without undue delay. Applying for a permit after the use of RTRBIS has ended may therefore constitute a breach. Importantly, if the controlling authority rejects this emergency request, the use of RTRBIS must be discontinued with immediate effect.

The authorization for the use of RTRBIS shall be granted if the controlling authority is satisfied, on the basis of objective evidence and clear reasons provided by the authority requesting the use of RTRBIS, that such use is necessary and proportionate under Article 5(2) to achieve the objectives that allow an exception to the relative prohibition under Article 5(1)(d). At this point, it is important to note

the vagueness of the term 'individual use.' It raises doubts as to whether the case of each individual should be considered, or whether it would be possible to take into account only the individual purpose, such as the search for missing children on a long list of.[50]

Competence of the Member States in detailing the rules on RTRBIS use

Article 5(4) expresses respect for the principle of subsidiarity and procedural autonomy and confers competence on Member States to determine their own detailed rules for the use of RTRBIS in public spaces for enforcement purposes within the limits imposed by Article 5(1)(d) and Article 5(2) and (3). It is the responsibility of the Member State to establish detailed rules governing the use, issuance, execution and supervision of RTRBIS authorizations.

There is a relative consensus between the EC and the EU Council in the case of Article 5(4). It presents itself as follows:

Article 5(4) of AIA
European Commission
4. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (d), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (d), including which of the criminal offences referred to in point (iii) thereof, the competent authorities may be authorised to use those systems for the purpose of law enforcement.

Under this provision, it will be up to the Member State to decide whether the use of RTRBIS for law enforcement purposes will be possible in its jurisdiction to the full extent provided for in the AIA or to a limited extent. There is nothing to prevent a Member State from prohibiting the use of RTRBIS for law enforcement purposes in its entirety, as proposed by the EP in the 2023 amendments. The EU Council amendment additionally provides for the competence of the Member State to regulate the reporting of the use of RTRBIS, which is the only change advocated by the EU Council in Article 5(4). This provision also provides that the Member

[50] M. Veale, F. Borgesius, *Demystifying the draft EU Artificial Intelligence Act*, "Computer Law Review International" 2021, vol. 4, p. 102.

State is obliged to define by law a catalogue of offences (permitted under Article 5(1)(d)(iii) of the AIA) for the commission of which the competent authorities may require the use of RTRBIS in public spaces for law enforcement purposes.

The wording of this provision suggests that the law adopted by the MS in this regard will implement EU law and thus subject to assessment of compliance with the CFR. It follows from Article 51 of the CFR which defines its scope of application, as limited to and bodies of the EU with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law.[51]

In closing, it should be however noted that an important limitation on the operation of the relative ban on use would be the exclusion from these provisions of the activities of the secret services and their cooperation as falling under the public security exception, as requested by some Member States[52].

Conclusions

The development of artificial intelligence raises legitimate concerns for the protection of fundamental rights and freedoms. The AIA should be considered as a necessary attempt to control the use of RTRBIS for the purpose of law enforcement and its adoption as a matter of urgency. The Act will not regulate all issues related to RTRBIS, so in accordance with the principle of subsidiarity, it will be supported by complementary legislation from Member States (if they choose to use RTRBIS for law enforcement purposes) and other EU laws, in particular LED. Furthermore, respect for fundamental rights in relation to the potential use of RTRBIS will be protected by the CFR. According to many organizations and human rights experts, the lack of a rigid prohibition on the use of RTRBIS by the apparatus of power is worrying. However, it is important to note that the AIA does not mandate its use, but merely limits the ability of Member States to do so and tidies up its potential use under the law. At the draft stage of the AIA, however, there were some inaccuracies and imprecisions that could lead to circumvention of the law, which will hopefully be corrected in the final version of the regulation.

The analysis of legislative progress presented in this article has shown that the relative ban related to the use of RTRBIS in publicly accessible spaces for the purpose of law enforcement has been a vital axis of contention between the EC and the

[51] T. Lock, *Commentary of Article 51* [in:] M. Kellerbauer, M. Klamert, J. Tomkin (ed.), *Commentary on the EU Treaties and the Charter of Fundamental Rights*, Oxford 2019, p. 2243.

[52] *CSOs fear the final EU AI Act will fall short of effectively protecting people from harmful effects of AI*, European Center for Not-for-Profit Law, 13 December 2023, https://ecnl.org/news/eu-reaches-agreement-artificial-intelligence-act, access date: 23.01.2024.

EU Council, on the one hand, which presented a relatively similar position, and the EP, which sought an absolute ban on RTRBIS. The reading of the EP's amendments suggests the possibility of minor concessions on this issue in exchange for the recognition of other essential restrictions not foreseen by the proposed AIA. The relative ban has been maintained as part of the agreement between the institutions involved in the legislative process, as the press reports. However, the content of this agreement is not yet known.

Abstract

The Artificial Intelligence Act is set to become the world's first piece of legislation comprehensively regulating artificial intelligence. However, its adoption has been delayed by disputes between the European Commission, the Council of the European Union and the European Parliament, who have been negotiating intensively in trialogues over the final form of the regulation. One of the contentious issues was the restriction of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes. This article analyses the proposed legislation related to this technology as proposed by the European Commission, taking into account the amendments of the Council of the European Union and the European Parliament, and the potential consequences of its application.

Key words: Artificial Intelligence, EU law, Artificial Intelligence Act, 'real-time' remote biometric identification systems, law enforcement

Wykorzystanie systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym do celów egzekwowania prawa – uwagi w świetle prac legislacyjnych nad aktem w sprawie sztucznej inteligencji

Streszczenie

Akt w sprawie sztucznej inteligencji ma stać się pierwszym na świecie aktem prawnym kompleksowo regulującym sztuczną inteligencję. Jego przyjęcie zostało jednak opóźnione przez spory pomiędzy Komisją Europejską, Radą Unii Europejskiej i Parlamentem Europejskim, które prowadziły intensywne negocjacje trójstronne nad ostatecznym kształtem rozporządzenia. Jedną ze spornych kwestii było ograniczenie stosowania systemów zdalnej identyfikacji biometrycznej „w czasie rzeczywistym" w przestrzeni publicznej do celów egzekwowania prawa. Niniejszy artykuł analizuje proponowane przez Komisję Europejską przepisy dotyczące tej technologii, z uwzględnieniem poprawek Rady Unii Europejskiej i Parlamentu Europejskiego, oraz potencjalne konsekwencje ich stosowania.

Słowa kluczowe: sztuczna inteligencja, prawo UE, akt w sprawie sztucznej inteligencji, systemy zdalnej identyfikacji biometrycznej „w czasie rzeczywistym", egzekwowanie prawa