UDC/УДК 342.738:004.8
ORIGINAL SCIENTIFIC ARTICLE / *ИЗВОРНИ НАУЧНИ РАД*

Balázs Gáti, LL.M., PhD student

Faculty of Law, University of Pécs, Hungarian
Criminology and Penal Execution Law Department

SOME DATA PROTECTION ISSUES OF THE EU REGULATION OF ARTIFICIAL INTELLIGENCE

The application of artificial intelligence in various forms is playing a significant role in an increasing number of areas of human activity. Due to its widespread application, a number of legal provisions regulate the conditions for the use of artificial intelligence, subject to more important data protection considerations. The aim of the study to present the main features of the data protection regulation on artificial intelligence. Current issues related to the challenges of artificial intelligence in relation of EU data protection regulation were searched and analyzed. The data protection package adopted in May 2016 - Regulation (Eu) 2016/679 of the European Parliament and of the Council – aims to prepare EU countries for the digital age, while providing general rules for the use of artificial intelligence by setting the conditions for automated data processing. Conclusion: The use of artificial intelligence carries number of risk elements with regard the rights and freedoms of natural persons, but regulation with appropriate guarantees and conditions can reduce these risks.

Key words: Artificial intelligence; Data protection; EU legislation.

1. INTRODUCTION

Artificial intelligence (AI) is a rapidly evolving family of technologies that can contribute to a wide range of economic and social benefits, as well as significant risks.[1]

The start of EU legislation can be traced back to 2017, referring to its resolution of 16 February 2017 addressed to the Commission with recommendations to the Commission on civil law rules on robotics.[2] By 2019, several pieces of legislation related to artificial intelligence were published, such as

Balázs Gáti, *gati.balazs@ajk.pte.hu.*

[1] Z. A. Nagy, *A mesterséges intelligencia és a jogi felelősség kérdése – 2010–2020 – as évek fordulóján de lege ferenda.* Ludovika Egyetem, Budapest 2020, 375.

[2] 2015/2103(INL).

the resolution of 1 June 2017 on the digitalization of European industry,[3] the resolution of 12 September 2018 on autonomous weapons systems,[4] and the 2018 resolution on linguistic equality in the digital age.[5] Resolution of 11 September 2018, Commission proposal of 6 June 2018 establishing the Digital Europe Program for the period 2021–2027,[6] establishing a European High Performance Computing Joint Undertaking Council Regulation 2018/1488.[7]

The socio-economic benefits as well as the risks are set out in the European Parliament's resolution of 12 February 2019 on a comprehensive European industrial policy for artificial intelligence and robotics.[8] Based on this, "*artificial intelligence and robotics offer an opportunity to enrich our lives and expand our capabilities, both as individuals and for the common good… Artificial intelligence is evolving rapidly and has played a role in our daily lives for years… Artificial intelligence and robotics are driving innovation, leading to new business models and playing a key role in transforming our societies and digitizing our economies in many sectors, such as industry, healthcare, construction and transport*."

With regard to risks, it draws attention to the fact that "*the malicious or negligent use of artificial intelligence could jeopardize digital, physical and public security, as large-scale, well-targeted and highly effective attacks on information society services and related machines and disinformation campaigns and generally restricts the right of individuals to self-determination. Stresses that the malicious or careless use of artificial intelligence can also pose a risk to democracy and fundamental rights*."

The definition of artificial intelligence as a legal concept can be found in resolutions and regulations. According to Auer,[9] "*there are positions in the legal literature and attempts at conceptualization, but we do not find a uniform and good answer on how to treat artificial intelligence, phenomena related to artificial intelligence (robots) in a legal sens*e". Gaszt[10] also states. Published in 2020, the White Paper[11] defines the concept of artificial intelligence as a set of technologies and automatisms, in addition to encouraging the diffusion of AI technologies and drawing attention to the compliance of these technologies with European ethical standards, legal requirements and social values.

[3] 2016/2271(INI).

[4] 2018/2752(RSP).

[5] 2018/2028(INI).

[6] 2021-2027COM/2018/434 final - 2018/0227 (COD).

[7] (EU) 2018/1488.

[8] 2018/2088 (INI).

[9] Á. Auer, "Gondolatok a mesterséges intelligencia egyes polgári jogi kérdéseiről", *Scientia et Securitas* 2/2021, 106.

[10] C. Gaszt, "A mesterséges intelligencia szabályozási kérdései, különös tekintettel a robotikára", *Infokommunikáció és Jog* 16/2019, 21.

[11] COM (2020) 65 final).

There is no uniform legal definition.[12] Most importantly, however, AI systems are not just sets of software components. AI systems also include the socio-technological system that surrounds them. On 21 April 2021, the European Commission presented a proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules for artificial intelligence[13] (hereinafter "the Proposal"), which also has important data protection implications.

This "*Artificial Intelligence Act*" Proposal defines an AI system as "*software that has been developed using one or more of the techniques and approaches listed in Annex I and that provides outputs, such as content, for a specific set of man-made objectives, is able to generate predictions, recommendations or decisions that affect the environment with which they interact".* These techniques and approaches include, a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programing, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; c) Statistical approaches, Bayesian estimation, search and optimization methods.

However, the Commission shall be empowered to adopt delegated acts in accordance with Article 73 of the Proposal in order to amend the list of techniques and approaches listed in Annex I in order to update the list in the light of market and technological developments. based on features similar to the techniques and approaches listed there. The Data Protection Package adopted in May 2016 - Regulation (EU) 2016/679,[14] and Directive (EU) 2016/680 "Law Enforcement Directive" (LED), and the Regulation (EU) 2018/1725 (EUDPR)[15] aims to prepare EU countries for the digital age, while setting general rules for the use of artificial intelligence by setting the conditions for automated data processing.

In my study, I would like to present the main features of the data protection regulation on artificial intelligence, taking into account the current issues related to the regulation of the Proposal.

2. ARTIFICIAL INTELLIGENCE ACT

At the end of April 2021, the European Commission published a draft regulation on the regulation of artificial intelligence,[16] which is part of the imple-

[12] COM (2020) 65 final). "2.8. It should also be noted that legal definitions (for the purpose of governance and regulation) differ from pure scientific definitions, whereas a number of different requirements must be met, such as inclusiveness, preciseness, permanence, comprehensiveness, and practicability. Some of these are legally binding requirements and some are considered good regulatory practice."

[13] COM (2021) 206 final.

[14] Regulation (EU) 2016/679.

[15] Regulation (EU) 2018/1725.

[16] COM (2021) 206 final.

mentation of the EU 2020 strategy White Paper, published in February 2020. The White Paper aims to build trust and transparency in AI systems by creating an environment based on excellence. In terms of building trust, the White Paper mentions the seven key elements identified in the Commission's Ethical Recommendation on AI[17] by an expert group set up by the Commission.[18] These are: human capacity and human oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, environmental and societal well-being and accountability.

Overall, the specific objectives of the Artificial Intelligence Proposal are to develop people-centered, sustainable, secure, inclusive and reliable artificial intelligence, as follows: a) ensuring that AI systems placed on the market and used in the EU are safe and respect existing legislation on fundamental rights and EU values; b) ensuring legal certainty to facilitate investment in AI and innovation in AI; c) improving governance and effective enforcement of existing legislation on fundamental rights and security requirements for AI systems; d) facilitate the completion of the single market for legitimate, secure and reliable AI applications and prevent market fragmentation.

The Proposal sets out harmonized rules for the market introduction, provision and use of AI systems, a ban on the use of AI systems, rules for operators and harmonized transparency rules for AI systems that interact with people. With regard to reliable artificial intelligence, the rules of the Proposal follow a risk-based approach. In addition to defining artificial intelligence, it is important to define *risk, high-risk, low-risk,* and *remote biometric identification systems*.

Prohibited AI practices – the category of unacceptable risk – includes AI systems that clearly endangered people's safety, livelihoods and rights – that is, their use is considered unacceptable because it violates EU values, such as a violation of fundamental rights. Prohibitions apply to practices that can unconsciously manipulate individuals to a large extent using subliminal techniques or exploit the vulnerability of certain vulnerable groups, such as children or people with disabilities, to distort their behavior in a way that is likely to harm them or others causes physical damage. These include AI systems or applications that manipulate human behavior to circumvent users' free will, such as voice-assisted games that encourage minors to engage in dangerous behavior. The Proposal also prohibits AI-based social scoring for general purposes done by public authorities, and the use of 'real time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement is also prohibited unless certain limited exceptions apply.

[17] European Commission, Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI, Publications Office, 2019, https://data.europa.eu/doi/10.2759/177365, last visited 2. 11. 2021

[18] „Key guidance derived from Chapter II: Ensure that the development, deployment and use of AI systems meets the seven key requirements for Trustworthy AI."

The Proposal identifies two main categories of high-risk AI systems:

- AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment,
- other stand-alone AI schemes, mainly related to fundamental rights, which are listed in Annex III. listed in Annex. These are:
    1. biometric identification and categorization of natural persons,
    2. critical infrastructures (e.g., transport) that could endanger the lives and health of citizens,
    3. educational or vocational training, which may determine someone's access to education and career throughout their lives (e.g., passing exams),
    4. employment, employee management and access to self-employment (e.g., use of CV selection software in recruitment procedures),
    5. basic private and public services (e.g., credit assessment of AI systems for assessing the creditworthiness or credit score of natural persons),
    6. law enforcement techniques[19] that may violate people's fundamental rights (e.g., assessing the reliability of evidence),
    7. handling migration, asylum and border control management (e.g., checking the authenticity of travel documents),
    8. administration of justice and democratic processes (e.g., AI systems designed to assist judicial authorities in researching and interpreting facts and law and in applying the law to specific facts).

I would like to highlight the position on Remote Biometric Identification Systems (RBIS) from the proposal. An RBIS is an AI system that remotely identifies natural persons by comparing a person's biometric data with the biometric data in the reference database and without the AI system user's prior knowledge that the person is present will be and identifiable. The definition of biometrics used in this Regulation is in line with the definition of biometrics in Article 35 (4) (14) GDPR and Article 36 (3) (18) EUDPR and with the biometric data in Article 37 (3) (13) of the LED. All remote biometric identification systems are considered high risk under the Proposal and are subject to strict requirements. The Proposal distinguishes between "real-time" and "non-real-time" RBIS. „*In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-in-*

[19] Z. A. Nagy, *Mesterséges intelligencia a bűnügyi munkában* ,Nemzeti Közszolgálati Egyetem, Budapest 2021, 9.

stantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-'live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned."[20]

The possible use of real-time RBIS in places accessible to the public for law enforcement purposes shall be considered prohibited unless such use is strictly necessary for one of the following purposes:

- targeted, specific searches for victims of crime, including missing children,[21]
- the prevention of a specific, significant and imminent threat to the life or physical security of natural persons or to a terrorist attack[22],[23]
- the detection, tracing, identification or prosecution of the perpetrators or suspects of the offenses referred to in Article 2 (2) of Council Framework Decision 2002/584 / JHA,[24] if these offenses are punishable by a term of imprisonment of at least three years under that law or a measure involving deprivation of liberty.

The Proposal sets out several conditions for the use of high-risk systems, such as data collection criteria, technical documentation, registration requirements, transparency, which are also relevant from a data protection point of view. The Proposal also contains detailed rules on product liability and the conformity of AI systems. It seeks to develop mechanisms to facilitate standardization, compliance testing, and the introduction of certification in the application of AI systems.

Data is a key component of AI applications. Within the GDPR, a number of specific provisions concern artificial intelligence-based decisions for individuals, particularly those related to automated decision-making and profiling.[25]

[20] „Artificial Intelligence Act" (23).

[21] I. L. Gál, M. Nagy, D. Ripszám, *Gyermekkereskedelem a terrorizmus tükrében*, Pannon Egyetem, Nagykanizsa 2021, 9.

[22] L. Kőhalmi, „Gondolatok a vallási indíttatású terrorizmus ürügyén" *Belügyi Szemle* 63/2015, 52.

[23] D. Tóth, *A terrorizmus típusai és a kiberterrorizmus*, Grastyán Endre Szakkollégium, Pécs 2014, 286.

[24] 2002/584/JHA.

[25] EU 2016/679 Art. 4. (4).

3. PRIVACY CONSIDERATIONS

The Digital Europe program has been able to prepare for the challenges of the fourth industrial revolution, including the use of artificial intelligence systems. The existing EU data protection legislation,[26] such as the GDPR, the LED and, the EUDPR also applies to the processing of any personal data covered by the draft regulation on artificial intelligence. When discussing artificial intelligence (AI) policies, it's hard not to talk about the General Data Protection Regulation (GDPR) at the same time. That's because the GDPR has had the most impact of any law globally in terms of creating a more regulated data market – while data is the key ingredient for AI applications. Article 22 of the GDPR is a general restriction on automated decision-making and profiling. However, this only applies if the decision is based solely on automated processing – including profiling. In addition, the stricter GDPR requirements in Article 15 relate specifically to automated, individual decision-making and profiling, which are also covered by Article 22. Article 22 only applies when a "*decision*" is based "*solely*" on automated processing – including profiling – which "*produces legal effects* or *similarly significantly affects the data subject*". Moreover, the stricter GDPR requirements of Article 15 are specifically linked to automated, individual decision making and profiling that fall within the narrow scope of Article 22. These include:

- The "*existence*" of automated decision making, including profiling,
- "*Meaningful information about the logic involved*",
- "*The significance and the envisaged consequences of such processing*" for the individual.

The bottom line: If Article 22 does not apply, these additional obligations do not apply, either.

The GDPR already clearly names profiling as data management,[27] and treats IP address, browser cookies, and location data as personal information, as well as log files, insofar as they can be used in conjunction with other information to create a natural person's profile and identify that person.[28] „*Ensuring data quality, addressing algorithmic biases, and applying and improving methods around code interpretability that help reconstruct the algorithm can all play a key role in fair and ethical use of AI*."[29]

[26] G. L. Szőke, *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén ,* HVG-ORAC, Budapest 2015, 188.

27 EU 2016/679, Art. 4. (4).

[28] EU 2016/679 Preamble 30.

[29] SAS, GDPR and AI: Friends, foes or something in between? Kalliopi Spyridaki, by Chief Privacy Strategist, SAS Europe,*https://www.sas.com/en_in/insights/articles/data-management/gdpr-and-ai--friends--foes-or-something-in-between-.html*, last visited 2. 12. 2021.

Despite the narrow applicability of Article 22, the GDPR includes a handful of provisions that apply to all profiling and automated decision making (such as those related to the right to access and the right to object). Finally, to the extent that profiling and automated decision making include the processing of personal data, all GDPR provisions apply – including, for instance, the principles of fair and transparent processing.

According to the GDPR, regardless of the purpose of the monitoring, a legitimate interest can only be established if the data subject can reasonably expect that the data will be processed for that purpose at the time and in connection with the collection of personal data.

The data subject has the right to information in connection with profiling. If the result of the profiling is based on a decision that significantly affects the situation of the data subject, it is mandatory to conduct a data protection impact assessment before starting the activity.[30] However, the Regulation contains a number of data security requirements[31] and recommends the use of pseudonymisation (pseudo-anonymisation), which should not lead to the conclusion that the data will no longer be considered personal data.

The Law Enforcement Directive sets uniform rules for all EU law enforcement agencies.

With regard to profiling, it states that a decision based solely on automated data processing, including profiling, which has a legal effect that is detrimental to or significantly affects the data subject is prohibited. Unless permitted by Union or Member State law which also provides for adequate guarantees of the rights and freedoms of data subjects, including at least the right of the data subject to request human intervention from the controller.[32]

The application of AI requires a significant amount of personal data or deprivation of their personal character, the so-called anonymized data. This can apply either to data required for machine learning methods or even to input data used in the operation of applications. Sikolya analyzed the impact of GDPR on solutions based on artificial intelligence.[33] According to Sikolya, "*that most of the grounds for data processing allowed by Article 6 (1) of the GDPR are not, or are difficult to apply, to the use of personal data for artificial intelligence reasons in principle or in practice*". These are: a) difficulties in applying a legitimate interest – especially in machine learning, b) the revocability of the consent and the difficulty of obtaining it, c) regulations on automated decision-making,

[30] EU 2016/679, Art. 35.

[31] EU 2016/679, Art. 32.

[32] EU 2016/680, Art. 11. (1)

[33] Zs. Sikolya, "Kormányzati Adatpolitika a Mesterséges Intelligencia korában. Áttekintés a mesterséges intelligenciában rejlő lehetőségek kiaknázásához szükséges kormányzati adatpolitikai feladatokról", *Új Magyar Közigazgatás* 12/2019, 50.

profiling and stakeholder information; strong limitations of the related guidelines, d) uncertainties in the regulation of data processing for statistical purposes – for example, for which data controllers data processing can be interpreted and, if it can be interpreted outside official statistics, what regulates its conditions.

According to the cited study, the application of rules for data processing for purposes other than the purpose of data collection is a problem. The conditions for data processing are even stricter for special data, such as health data. With regard to the issue of anonymizations, he points out that originally personal data which have been anonymized, ie whose data subjects are no longer identifiable, are no longer covered by the GDPR, but also points out that in some cases there is a risk the relationship of the data considered anonymized to the original data subjects may be revealed.

With regard to the data management of AI systems, the following shall be defined in accordance with the GDPR:

- Assessing the need for data management,
- Definition of personal data and data subject matter,
- Purpose of data management,
- Legal basis for data management:
    1. Stakeholder input,
    2. The contract with the data subject,
    3. Fulfillment of a legal obligation,
    4. Data management in the public interest (e.g., law enforcement systems and certain government services),
    5. Data management based on legitimate interests (e.g., property protection, law enforcement systems).
- Determining the duration of data management.

The data protection rights also apply to the data subject in relation to AI systems, which are the right of access, the right to rectification, the right to delete (right to forget), the right to data and the right to restrict data processing, the right to data portability.

4. EDPB-EDPS JOINT OPINION 5/2021 ON THE PROPOSAL

On 21 June 2021, the European Data Protection Board and the European Data Protection Supervisor adopted a joint opinion on the proposal for a Regulation of the European Commission laying down harmonized rules on artificial intelligence.[34]Among the issues raised by the EDPB and the EDPS were concerns about the scope of the Proposal, the risk-based approach, the ban, remote biometric identification and the compliance system. The reso-

[34] EDPB-EDPS Joint Opinion 5/2021.

lution also addresses the classification of AI systems, the "*social scoring*", the designation of the European Data Protection Supervisor as the competent authority and market surveillance authority for the supervision of EU institutions, agencies and bodies, the European Artificial Intelligence Body, harmonized enforcement, artificial intelligence regulatory test environments with detailed data protection regulations for codes of conduct.

With regard to the scope of the Proposal, the resolution agrees with the aim of addressing the use of AI systems in the European Union, including the use of AI systems by EU institutions, bodies or agencies. However, the exclusion of international law enforcement cooperation from the scope of the Proposal raises concerns, as such exclusion poses a significant risk of circumvention, for example in third countries or international organizations operating high-risk applications on which the EU authorities rely.

The opinion agrees with the risk-based approach underlying the Proposal but considers that the concept of "*fundamental rights risk*" should be brought into line with the EU data protection framework. The EDPB and the EDPS recommend that the social risks to groups of individuals should also be assessed and mitigated. Furthermore, they agree with the Proposal that the classification of an AI system as high risk does not necessarily mean that it is legitimate and as such applicable by the user. It is considered necessary that compliance with legal obligations under EU law, including legislation on the protection of personal data, should be a precondition for access to the European market as a product bearing the CE marking.

The EDPB and the EDPBS take note of the high-risk artificial intelligence systems in Annex II of the Proposal and III in accordance with the Annex. It lacks a list of certain types of use that carry significant risks, such as the use of AI for insurance premiums or for the evaluation of medical treatments or health research. It is therefore considered important that these annexes be regularly updated to ensure that they have appropriate effect.[35]

The Proposal requires AI system providers to carry out a risk assessment, however, in most cases (data) managers are users of AI systems rather than providers, e.g. the user of a facial recognition system is a "*data controller*" and is therefore not bound by the requirement for high-risk AI providers.[36] In addition, the service provider will not always be able to assess in advance all subsequent uses of the AI. Thus, the initial risk assessment will be more general than the actual use of the AI system. Even if the initial risk assessment of the service provider does not indicate that the AI system is "*high risk*" under the Proposal, this should not preclude a subsequent assessment - a Data Protection Impact Assessment (DPIA) – under Article 35 of the GDPR and Article 39 of the EUDPR or Article 27 of the LED.[37]

[35] *Ibid.*, 19.

[36] *Ibid.*, 2.2 20.

[37] *Ibid.*, 2.3 21.

According to the EDPB resolution on cases of illicit use of artificial intelligence, forms of AI systems that violate human dignity should be considered as prohibited AI systems under Article 5 of the Proposal, rather than simply being classified as "*high risk*". This applies in particular to data comparisons involving persons who have given no or little reason to police surveillance or its processing, all of which violate the purpose limitations principle under data protection law. The use of AI in public places by police and law enforcement should be based on precise, predictable and proportionate rules that take into account the interests of the persons concerned and their impact on the functioning of a democratic society.[38]

According to Article 5 (1) (c) of the Proposal, the use of AI may lead to "*social scoring*", discrimination and is contrary to the fundamental values of the EU. Private companies, especially social media, cloud and other providers can process huge amounts of personal data and perform community scoring. Consequently, the Proposal should prohibit all forms of social scoring. It should be noted that in the context of law enforcement, Article 4 already significantly restricts, if not prohibits, this type of activity under the LED.[39]

According to the resolution, the biometric remote identification of individuals in publicly accessible places poses a high risk of intrusion into individuals' privacy. Identification systems also raise transparency issues and legal issues based on data processing under EU law. In addition, the way in which individuals are properly informed and the processing involved remain unresolved, nor is the effective and timely exercise of the rights of individuals resolved.[40] It is therefore proposed to apply a general ban in the following cases:

- any use of artificial intelligence to automatically recognize human features, such as faces, but gait, fingerprints, DNA, voice, keystrokes, and other biometric or behavioral signs, in places accessible to the public, in any context,[41]
- artificial intelligence systems, which group individuals on the basis of biometric data such as ethnicity, gender, political or sexual orientation or other grounds of discrimination under Article 21 of the Charter,
- the use of artificial intelligence to infer the emotions of a natural person,[42] except for certain well-defined uses, namely for health or research purposes, always with appropriate safeguards, including purpose limitations.

[38] *Ibid.*, 2.3 27

[39] *Ibid.*, 2.3 29.

[40] *Ibid.*, 2.3. 30.

[41] *Ibid.*, 2.3. 32.

[42] *Ibid.*, 2.3. 35.

In addition, anonymous appearance in public places is a legitimate expectation – its restriction has a direct negative effect on the freedom of expression, the exercise of freedom of assembly and association, and freedom of movement.

It is a question, however, of the implications for law enforcement. Article 5 (1) (d) of the Proposal contains an extensive list of exceptions that allow real-time remote biometric identification in publicly accessible places for law enforcement purposes.

The EDPB and the EDPS raise several objections to this approach. It is not clear "*what should be understood a significant delay*"[43] in the Proposal and how this can be considered as a Mitigating factor given that a mass identification system can identify thousands of individuals in a matter of hours. In addition, processing is intrusive its nature does not always depend on whether the identification takes place in real time or not. RBIS, for example, in the event of political protest, is likely to have a significant impact on people's fundamental rights and freedoms, such as freedom of assembly and association, and the principles of democracy in general. The intrusive nature of data management does not necessarily depend on its purpose. The use of this system for other purposes, such as private security, poses the same threat to respect for private and family life and to the fundamental rights to the protection of personal data. Finally, even with the planned restrictions, the potential number of suspects or perpetrators of crime will almost always be "*high enough*" to justify the continued use of artificial intelligence systems to detect a suspect, despite the fact that the conditions set out in Article 5 (2) to (4) of the Proposal have been laid down. "*The reasoning behind the Proposal seems to omit that when monitoring open areas, the obligations under EU data protection law need to be met for not just suspects, but for all those that in practice are monitored*."[44] For these reasons, the EDPB and the EDPS call for a general ban on the use of AI systems for the automated recognition of human characteristics in publicly accessible locations.

Human dignity is also affected if the computer determines or categorizes the future. Artificial intelligence systems used by public authorities assess the risk of a natural person committing repeated responsibilities when carrying out an individual risk assessment of natural persons.[45]

[43] Proposal COM(2021) 206 final (8) "In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems in question by providing for minor delays. (…)" In the case of 'post' systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned."

[44] EDPB-EDPS Joint Opinion 5/2021, 2.3. 31.

[45] The Proposal Annex III.6.a).

It is used to predict the occurrence or recurrence of an actual or potential criminal offense based on the profiling of a natural person or the assessment of personality traits and past criminal behavior.[46] This goal leads to a crucial subordination of police and court decision-making and objectifies the human being concerned. Such AI systems violate the essence of the right to human dignity and should therefore be prohibited under Article 5 of the resolution.[47]

Regarding the conformity assessment procedure, the EDPB and the EDPS propose to adjust these assessments in accordance with Article 43 of the Proposal and considers it necessary to carry out a preliminary third-party compliance assessment for high-risk AI.[48] According to the Proposal,[49] the new conformity assessment procedure for high-risk artificial intelligence systems should be applied in the event of a significant change, for example, in the case of AI systems that were placed on the market and developed before the Proposal. It is important that AI systems meet the requirements of the AI Regulation throughout their life cycle.[50]

The certification scheme outlined in the Proposal lacks a clear link to EU data protection law, and other areas of high-risk artificial intelligence systems with other Community legislation.

The Proposal should be amended to clarify the relationship between certificates and data protection certificates, seals and markings issued under that Regulation.

The EDPB and the EDPS recall that data protection authorities already enforce the GDPR and the LED for AI and personal data in order to ensure the protection of fundamental rights, in particular the right to data protection. As a result, the designation of data protection authorities as national supervisory authorities would ensure a more harmonized regulatory approach and contribute to a more consistent interpretation of data management provisions across the EU, [51] proposes their designation as a national supervisory authority.[52] In any case, restrictions on the use of AI systems for "real-time" remote biometric identification for law enforcement purposes in places accessible to the public must be verified by independent authorities.[53]

[46] The Proposal Annex III.6.e).

[47] EDPB-EDPS Joint Opinion 5/2021, 2.3 34.

[48] *Ibid.*, 2.4.1. 37.

[49] The Proposal Art. 43 (4).

[50] EDPB-EDPS Joint Opinion 5/2021, 2.4.1. 38.

[51] The Proposal Art. 59.

[52] EDPB-EDPS Joint Opinion 5/2021, 2.5.1 48.

[53] *Ibid*.

Regarding the rights of the individual, it is essential that data subjects are always informed when their data are used by means of an artificial intelligence system, the forecast of the legal basis for processing, the general explanation of the procedure and the scope of the AI system.

In this regard, the individual has the right to restrict data processing[54] and to delete data.[55]

The controller must make an explicit commitment to inform the data subject of the relevant periods. The AI system must be able to meet all of these conditions.[56]

5. SUMMARY

The use of artificial intelligence carries a number of risk elements with regard to the rights and freedoms of natural persons, but regulation with appropriate guarantees and conditions can reduce these risks. The proposal on the regulation of artificial intelligence, published at the end of April 2021, is a significant step forward in European Union legislation in this area, its topicality is necessary in the light of technical progress and is based on the strategic approach of the White Paper. Consistency is also ensured with the Charter of Fundamental Rights of the European Union and with existing secondary EU legislation on data protection, consumer protection, non-discrimination and gender equality. The proposal was preceded by the General Data Protection Regulation (Regulation (EU) 2016/679), the Directive on data protection in law enforcement (Directive (EU) 2016/680) and Regulation (EU) 2018/1725 on the protection of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies. Critical areas for compliance with the data protection package are harmonized rules for the design, development and use of high-risk AI systems and restrictions on certain uses of remote biometric identification systems. In May 2021, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) commented on the Proposal for such legislation, with regard to the Charter of Fundamental Rights, and on compliance rules. The Proposal is based on a risk-based approach. According to this, while "unacceptable risk" significant artificial intelligence systems are banned, "high risk" AI systems can be marketed with strict obligations. Most of the provisions of the legislation deal with high-risk systems, imposing obligations on service providers, users and other actors in the AI value chain. It pays particular attention to the conformity assessment procedures to be followed for all types of high-risk AI systems. Although the risk-based

[54] (EU) 2016/679 Art. 18 and (EU) 2018/1725 Art.20

[55] *Ibid.*, 1725 Art. 19.

[56] EDPB-EDPS Joint Opinion 5/2021, 3.1 60.

approach is fundamentally good, the EDPB and the EDPBS set stricter criteria for interpreting the concepts from a data protection point of view.

Further coordination is needed in these areas, including a clearer definition of restrictions, a reinterpretation of the further wider use of periodic AI systems, supervision by "national authorities", including national regulation, to ensure the development of innovation while protecting fundamental rights. The definition of exceptions for certain applications and the definition of targets are key areas, for example with regard to the purpose of law enforcement, as it is clear that the security of individuals is as much a value to be protected as the protection of personal data.

According to a study by Ebers,[57] who has already criticized compliance with certification schemes, the proposal focuses on the idea of co-regulation based on standardization under the New Legal Framework. According to the Proposal, "standardization should play a key role" in ensuring that appropriate technical solutions are available to service providers to ensure compliance with this Regulation. Providers may demonstrate compliance with the requirements of this Regulation by complying with the harmonized standards laid down in Regulation (EU) No 1025/2012 of the European Parliament and of the Council.[58]

Therefore, the development of standards through co-regulation is an essential element of future regulation. However, fundamental ethical and legal decisions should not be delegated to private standardization organizations. Accordingly, the draft legislation should set out legally required obligations for essential requirements for high-risk AI systems. So there is a need for further wide-ranging consultation on consumer protection and NGOs on standardization. Concerning the protection of personal data, the EDPB and the EDPS agree on the Commission's proposal and consider that such legislation is necessary to guarantee the fundamental rights of EU citizens and residents. In their view, however, the proposal needs to be amended on a number of issues in order to comply with EU principles.

LIST OF REFERENCES

Scientific works

1. Auer, Adam, "Gondolatok a mesterséges intelligencia egyes polgári jogi kérdéseiről", *Scientia et Securitas* 2/2021;
2. Ebers, Martin, *Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act*, Cambridge 2022;

[57] M. Ebers, *Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act,* Cambridge 2022, 22.

[58] The Proposal Preamble (61).

3. Gál, László, Nagy, Melánia, Ripszám, Dóra, *Gyermekkereskedelem a terrorizmus tükrében, Pannon Egyetem*, Nagykanizsa 2021;
4. Gaszt, Csaba, "A mesterséges intelligencia szabályozási kérdései, különös tekintettel a robotikára", *Infokommunikáció és Jog* 16/2019;
5. Kőhalmi, László, „Gondolatok a vallási indíttatású terrorizmus ürügyén", *Belügyi Szemle* 63/2015;
6. Nagy, Zoltán András, *A mesterséges intelligencia és a jogi felelősség kérdése – 2010–2020 – as évek fordulóján de lege ferenda*, Ludovika Egyetem, Budapest 2020;
7. Nagy, Zoltán András, *Mesterséges intelligencia a bűnügyi munkában*, Nemzeti Közszolgálati Egyetem, Budapest 2021;
8. Sikolya, Zsolt, "Kormányzati Adatpolitika a Mesterséges Intelligencia korában. Áttekintés a mesterséges intelligenciában rejlő lehetőségek kiaknázásához szükséges kormányzati adatpolitikai feladatokról", *Új Magyar Közigazgatás* 12/2019;
9. Szőke, Gergely László, *Az európai adatvédelmi jog megújítása. Tendenciák és lehetőségek az önszabályozás területén*, HVG-ORAC, Budapest 2015;
10. Tóth, David, *A terrorizmus típusai és a kiberterrorizmus*, Grastyán Endre Szakkollégium, Pécs 2014.

Legal documents and internet sources

1. Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA), *Official Journal of the European Union*, L190/1, No. 63/2020;
2. Council Regulation (EU) 2018/1488 of 28 September 2018 establishing the European High Performance Computing Joint Undertaking, *Official Journal of the European Union*, L 252, 8, No. 54/2011;
3. 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) 18 June 2021, *https://edps.europa.eu/system/files/2021-06/2021-06-18-edpb-edps joint opinion ai regulation en.pdf*;
4. European Commission, Directorate-General for Communications Networks, Content and Technology, Ethics guidelines for trustworthy AI, Publications Office, 2019, *https://data.europa.eu/doi/10.2759/177365*, last visited 1. 10. 2021;
5. European Parliament resolution of 1 June 2017 on digitizing European industry (2016/2271(INI)), *Official Journal of the European Union*, C307, 26. No. 61/2018;
6. European Parliament resolution of 11 September 2018 on language equality in the digital age, (2018/2028(INI)), *Official Journal of the European Union*, C433, 23. No. 62/2019;

7. European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)), *Official Journal of the European Union*, C 449, 23. No. 63/2020;
8. European Parliament resolution of 12 September 2018 on autonomous weapon systems (2018/2752(RSP)), *Official Journal of the European Union*, C 433, 23. No. 62/2019;
9. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), *Official Journal of the European Union*, C 252, 18. No. 61/2018;
10. Opinion of the European Economic and Social Committee on 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 — 2021/106 (COD)) , *Official Journal of the European Union*, C 517, 22. No. 64/2021;
11. Opinion of the European Economic and Social Committee on 'White paper on Artificial Intelligence — A European approach to excellence and trust' (COM(2020) 65 final), *Official Journal of the European Union*, C 364, 28. No. 63/2020;
12. Proposal for a regulation of the European Parliament and of the Council establishing the Digital Europe Programme for the period 2021-2027com/2018/434 final – 2018/0227 (cod), document 52018pc0434;
13. 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. 4. 2021 com (2021) 206 final, 2021/0106 (cod);
14. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending council directives 89/686/eec and 93/15/eec and directives 94/9/ec, 94/25/ec, 95/16/ec, 97/23/ec, 98/34/ec, 2004/22/ec, 2007/23/ec, 2009/23/ec and 2009/105/ec of the European Parliament and of the Council and repealing council decision 87/95/eec and decision no 1673/2006/ec of the European Parliament and of the Council. *Official Journal of the European Union* l 312, 12. No. 55/2012;
15. 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), *Official Journal of the European Union*, L 119, 1. No. 59/2016;
16. 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, *Official Journal of the European Union*, L 295, 39. No. 61/2018;

17. SAS, GDPR and AI: Friends, foes or something in between? Kalliopi Spyridaki, by Chief Privacy Strategist, SAS Europe, *https://www.sas.com/en_in/insights/articles/data-management/gdpr-and-ai--friends--foes-or-something-in-between-.html*.

Балаш Гати, ма

Докторанд Правног факултета Универзитета у Печују, Мађарска
Катедра за криминологију и пенологију

НЕКА ПИТАЊА ЗАШТИТЕ ЛИЧНИХ ПОДАТАКА У ОДРЕДБАМА ЕВРОПСКЕ УНИЈЕ О ВЈЕШТАЧКОЈ ИНТЕЛИГЕНЦИЈИ

Сажетак

Примјена вјештачке интелигенције игра значајну улогу у све већем броју области људског дјеловања. Због широке примјене вјештачке интелигенције велики број правних одредби регулише услове за њену употребу. Циљ ове студије је да представи главне карактеристике правних одредби заштите личних података у области вјештачке интелигенције. У раду се анализирају актуелна питања везана за изазове које вјештачка интелигенција поставља у контексту одредаба Европске уније у области заштите личних података. Пакет о заштити личних података усвојен у мају 2016. године – Уредба Европске уније 2016/679 Европског парламента и Вијећа има за циљ да припреми земље ЕУ за дигитално доба а истовремено поставља општа правила за употребу вјештачке интелигенције успостављајући услове за аутоматску обраду података. Закључак: Употреба вјештачке интелигенције носи одређене елементе ризика у смислу права и слобода појединаца, али правна регулатива која обезбјеђује одговарајуће гаранције и поставља услове за њену употребу ове ризике може значајно смањити.

Кључне ријечи: *Вјештачка интелигенција; Заштита података, Законодавство ЕУ*.