EUROPEAN DATA PROTECTION SUPERVISOR

WOJCIECH RAFAŁ WIEWIÓROWSKI
SUPERVISOR

Lucilla Sioli
Director
Artificial Intelligence Office
DG CNCT.A

Brussels,
WW/AP/nc/ D(2024) 4345 **C 2024-0279**
Please use AI-Act@edps.europa.eu for correspondence on this matter

EDPS comments to the AI Office's consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act launched by the European AI Office.

I. Introduction

On 13 November 2024, the European AI Office launched a multi-stakeholder consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act.[1]

The EDPS welcomes this consultation by the European AI Office. In this regard, the EDPS would like to highlight the following considerations, providing concrete examples where relevant, having also regard to the interplay of the provisions of the AI Act with EU data protection laws[2].

The EDPS notes that both the substantive data protection rules and principles[3] and the tasks and powers of data protection authorities[4] under data protection legislation are not affected by the AI Act.

[1] https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-ai-act-prohibitions-and-ai-system-definition
[2] Namely, Regulation (EU) 2016/679 ('GDPR'), Directive (EU) 2016/680 ('LED), and Regulation (EU) 2018/1725 ('EUDPR').
[3] Article 2(7) of the AI Act; see also recitals 137, recital 63, and recital 39 of the AI Act.
[4] Recital 10 of the AI Act.

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

With this contribution, the EDPS would like to highlight possible discrepancies of the processing of personal data in the context of the development and deployment of certain AI systems with data protection law (without prejudice to these being finally assessed by national Courts and by the CJEU). In this respect, we would like also to draw your attention to the most recent EDPB Opinion on certain data protection aspects related to the processing of personal data in the context of AI models adopted this week which further elaborates on the interplay of the AI Act and the GDPR.[5]

This contribution builds on the EDPB and EDPS Joint Opinion on the AI Act[6], as well as relevant EDPB guidelines[7].

For practical purposes, this contribution follows the structure of the questions included in the multi-stakeholder consultation.

II. Section 1: Definition of an AI System

1. EDPS comments on Question 1: Elements of the definition of an AI system

'designed to operate with varying levels of autonomy'

The EDPS considers that the concept of "autonomy" needs clarification, as to its definition and degree. In our view, all IT systems may be considered autonomous, as they do automate calculations and processes. For example: an IT system that includes a machine learning model that shows to a bank clerk a prediction on a loan application is autonomous. But in which sense is that IT system more autonomous that a simple rule based algorithm that will judge some attributes of the application?

'may exhibit adaptiveness after deployment'

The EDPS considers the notion of adaptiveness should be broadened to include a fundamental element, namely the adaptation and the learning procedure that occur **before the deployment**, which is a unique element to AI systems. The definition seems to obviate the fact that AI systems learn during their development. AI systems start their development with a set of unadjusted initial parameters. Then, they undergo a learning procedure in order to adjust/tune these parameters to improve their performance in a defined task. AI systems become 'intelligent' precisely because of their capability of learning and adapting.

[5] Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en
[6] EDPB-EDPS Joint Opinion 5/2021, paragraphs 27-35.
[7] See EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement.

2. EDPS Comments on Question 2: Simple software systems out of scope of the definition of an AI system

The EDPS considers unclear whether **Expert Systems or hybrid (neurosymbolic) AI systems** would fall under the AI system definition.

Expert Systems use a set of predefined rules and logic to solve problems based on expert knowledge. The decisions made by expert systems are typically deterministic, meaning they follow a specific rule for each input, with no randomness involved. Once the inputs and rules are defined, the output is always the same for the same inputs.

There are some systems that merge these expert systems with other types of AI systems, such as GenAI systems and it is unclear if the definition of AI system would apply to them or not.

III. Section 2: Prohibited AI Practices under the AI Act

1. Comments with regard to question 8 of the consultation on harmful subliminal, manipulative or deceptive practices (Articles 5(1)(a) and 5(1)(b) of the AI Act)

The EDPS notes that the AI Act prohibits the placing on the market, the putting into service or the use of, inter alia, AI system that:

- entails cognitive behavioural manipulation[8];
- exploits certain vulnerabilities of a person or a specific group of persons[9] to the extent that it appreciably impairs their ability to make an informed decision in a manner that causes significant harm.

The EDPS highlights that the prohibition of harmful subliminal, manipulative or deceptive practices is also relevant from a **privacy and data protection perspective**. For instance, the use (or misuse) of personal data by AI systems could influence data subjects into making unintended, unwilling, and potentially harmful decisions as result of 'feedback loop' from input data such as AI companions. **The manner in which personal data are obtained and used by AI systems** are therefore relevant for the assessment of the manipulation of the individual.[10] Concrete examples may include AI chatbots and other human-imitating AI applications, including so-called AI voice replication technology that may cause significant financial, political or (mental) health harm.[11]

[8] Article 5(1)(a) of the AI Act; recital 29 of the AI Act.
[9] Article 5(1)(b) of the AI Act and recital 29 of the AI Act.
[10] Recital 28 of the AI Act also refers to the fundamental rights to data protection and to privacy as underpinning the prohibition of certain AI practices.
[11] See for instance from the press: https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice or https://www.law.kuleuven.be/ai-summer-school/open-brief/open-letter-manipulative-ai. In addition, possible dismorphopobic disorders as results of image alterations, beauty filters, etc should also be borne in

Even in the context of **marketing**, the criteria of impairment, decision and significant harm could be fulfilled. (e.g. financial harm through an impulsive purchase). In particular, the EDPS considers that **neuromarketing** - both with and without the use of brain-machine interfaces[12] - should be mentioned as a concrete example of practices that fall within the scope of the prohibition.[13] Such practices would also fulfil the criteria of significant harm and appreciably impair the ability of the concerned person to make an informed decision as laid down in Article 5(1)(a) of the AI Act[14], and should therefore be considered as falling under the scope of this prohibition.

The EDPS considers necessary to further clarify the notions of '**subliminal, purposefully manipulative or deceptive techniques'** of Article 5(1)(a) of the AI Act, as well as the criteria for '**material distortion**' involving a degree of coercion, manipulation or deception that goes beyond lawful persuasion. Moreover, we recommend to illustrate with examples what would be lawful persuasions, as well as '**significant harm**' and the requested **causal link** between them.

Particularly with regard to the notion of "significant harm", the EDPS submits that harm can manifest in many forms. In particular, it could be asked whether a recommender system could be considered to "harm" users by providing them content with more extreme political views (even if fit to their current inclination)? In the same line, it is also unclear when would an advertisement that is most often purposefully manipulative or deceptive be considered to be "harmful".
With regard to Question 5, the EDPS highlights that also recommender systems in social networks and news outlets could be examples of AI systems where the scope of the prohibition would require further clarification.

2. Comments with regard to Question 9 of the consultation on social scoring AI systems (Article 5(1)(c) of the AI Act)

The EDPS recommends recalling that evaluations, classifications or scores covered by Article 5(1)(c) include, but are not limited to, those relating to the person or group's access to education, employment, housing, public assistance benefits.[15]

---

mind.https://www.theguardian.com/technology/2024/nov/26/tiktok-to-block-teenagers-from-beauty-filters-over-mental-health-concerns

[12] See recital 29 of the AI Act, referring to brain-machine interfaces.

[13] Neuro-marketing is commonly defined as the use of neurodata to reveal and influence subconscious consumer decision-making processes. Neuro-marketers study and apply brain and biometric responses to understand and shape consumers feelings and actions In its TechDispatch 1/2024 on neurodata, the EDPS highlighted that the use of artificial intelligence ('AI') systems may also make technically possible exploitation of neurodata for purposes such as law enforcement, screening of migrants and asylum seekers, as well as by private entities for instance for workplace or commercial surveillance. In this context, the EDPS underlined that certain uses of neurodata pose unacceptable risks to fundamental rights and are likely unlawful under EU law See EDPS, TechDispatch 1/2024 on neurodata, 3 June 2024.

[14] Article 5(1)(a) states that : *"The following AI practices shall be prohibited:*
(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm."

[15] See recital (58) AI Act

With regard to the notion of "**unrelated** social contexts" included in Article 5(1)(c)(i) of the AI Act, the EDPS points out that otherwise legitimate activities, such as checking possible frauds or welfare allocations, should not be based on unrelated socio-economic factors, for instance the fact that an EU citizen has a migrant background.

Concerning Article 5(1)(c)(ii) of the AI Act, the EDPS highlights the need to clarify when a detrimental or unfavourable treatment of certain natural persons or groups of persons is "**unjustified or disproportionate** to their social behaviour or its gravity". In this regard, the EDPS proposes the following criteria to be taken into account:

a) **the impact of the treatment** on the person concerned, namely if the person is significantly affected by a decision as result of the scoring, possibly but not necessarily having a legal effect as such,
b) **the lack of proportionality** of the detrimental treatment having regard to the social behaviour (for instance, a minor road traffic infringement such as 'jaywalking', in the EDPS' view, would not justify, as unfavourable treatment, denied access to driving licence).

3. Comments with regard to Question 12 of the consultation on individual crime risk assessment and prediction (Article 5(1)(d) of the AI Act)

The EDPS recalls the clear commitment in Recital 42 of AI Act that "[n]atural persons should never be judged on AI-predicted behaviour based solely on their profiling, personality traits or characteristics". In this regard, we welcome the statement in the consultation that "*predictive crime and policing AI systems pose an 'unacceptable risk' since they infringe fundamental rights and freedoms in a democracy that is based on rule of law and requires a fair, equal and just criminal legal system*". In the same spirit, the EDPS considers that such practices, including 'crime prediction' based on personal data and profiling and inferences from 'big data', would not be compliant with the key legal principles of **presumption of innocence and of non-discrimination** and would also be incompatible with the **respect for human dignity**. This is notably the case of 'predictions' based on historical data and past behaviour, location, or any other such characteristics (such as debt, number of children, etc.).[16]

The EDPS also believes that it is essential for the future guidelines to clearly and unambiguously **explain the scope** of the prohibition, and especially of the **exclusion** of "AI **systems used to support the human assessment** of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity". The notion of this supporting role should be further clarified.

In this context, the EDPS considers that the guidelines should also address the risk of '**automation bias**', for example in cases of uncritical acceptance of the results of AI risk analytics, as well as the weight given to certain profiling techniques in practice when

[16] EDPB EDPS Joint Opinion 5/2021, paragraph 34.

establishing whether or not the risk assessment is based "solely" on profiling or the assessment of personality traits or characteristics.

In addition, the EDPS highlights the prohibition under **Article 11 LED of automated individual decision-making**, including profiling, which produces an adverse legal, or other significant, effect for the person subject to that decision. According to Article 11 LED, such decision-making can only be permitted by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, including the **right to obtain human intervention** from the controller.

Further clarification is also needed concerning **the exclusion from the scope** of the prohibition of individual predictions of **administrative offences**, even if these predictions are "*based solely on the profiling of a natural person or on assessing their personality traits and characteristics*". The argument that "these are not assessing the risk of individuals committing a criminal offence" does not seem, in the EDPS' opinion, convincing. In this context, the EDPS would like to recall the judgment of the CJEU (Grand Chamber) of 14 November 2013 (Proceedings concerning the enforcement of a financial penalty issued against Marián Baláž), which par. 35 states: "*It follows that, in order to ensure that the Framework Decision is effective, it is appropriate to rely on an interpretation of the words 'having jurisdiction in particular in criminal matters' in which the classification of offences by the Member States is not conclusive*".[17] The difficulty to draw a clear delineation between criminal and administrative offences has also been subject of a continuous discussion in the context of the scope of Directive (EU) 2016/680 (Law Enforcement Directive).

4. Comments with regard to Question 16 of the consultation on untargeted scraping of facial images (Article 5(1)(e) of the AI Act)

With regard to the placing on the market or putting into service of an AI system based on the 'untargeted' scraping of facial images from the internet or CCTV footage, prohibited under Article 5(1)(e) of the AI Act, the EDPS would like to draw the attention on EDPB Guidelines 05/2022[18], and in particular its Annex III, scenario 6, concerning a situation where a private entity provides an application where facial images are scraped off the internet to create a database.

Moreover, the EDPS considers that the untargeted 'scraping' of other types of biometric data, such as '**voice fingerprinting**', could also be covered by the prohibition under Article 5(1)(e) of the AI Act. Such interpretation would be in line with the principle of effectiveness ("effet utile") of EU law, due to the fact that the aim of the prohibition is to protect from the untargeted scraping of biometric data. As specified in recital 43 of the AI Act, "[untargeted scraping] should be prohibited because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy." This rationale applies to both facial images and voice fingerprinting.

[17] Judgment of the Court (Grand Chamber) of 14 November 2013, Case C-60/12, ECLI:EU:C:2013:733, paragraph 35.
[18] Annex III 'Practical Examples', Scenario 6, of the EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, where the necessity and proportionality of such scraping is assessed in more details.

Furthermore the notion and scope of a "**facial recognition database**" could be clarified. In particular, the EDPS considers unclear whether it refers strictly to the reference database that is an integral part of the operational use of biometric identification, or whether this term additionally entail databases used for the validation and training of an AI-system for biometric identification other than the reference database. Finally, the EDPS submits that some clarification or use cases on **targeted** scraping vs. untargeted scraping could also be helpful.

5. Comments with regard to Question 18 of the consultation on Biometrics-based AI systems

The use of AI systems processing biometric data can have a significant impact and raise serious risks to several rights protected under the Charter. These risks concern in particular the interference with the rights to private and family life and the right to protection of personal data, as well as other fundamental rights.

In this regard, the EDPS recalls the paramount importance of the requirement of **lawfulness**, as applied by the Court of Justice of the European Union and by the European Court of Human Rights[19]. This requirement encompasses respect for the essence of the fundamental right at stake, necessity and proportionality of the interference with fundamental rights, and respect of human dignity. The principle of **necessity** requires an assessment of whether the purpose pursued cannot be achieved without using biometric data. The principle of **proportionality** requires strict consideration of the seriousness of the interference with the fundamental rights and freedoms. The **respect of human dignity** entails the need to respect freedom and fundamental rights of persons concerned having regard to particularly invasive data processing such as of biometric data. Defending persons from inferences from his or her body means defending not only personal freedom, integrity and dignity, but also the fundamental values of democratic systems.

6. Comments with regard to Question 19 and 21 of the consultation on AI emotion recognition (Article 5(1)(f) of the AI Act)

The EDPS stresses that processing of personal data entailed by emotion recognition AI systems, except for certain well-specified use-cases for health or research purposes (with appropriate safeguards in place and subject to all other data protection conditions and limits including purpose limitation) is highly likely to affect fundamental rights such as the right to mental integrity, freedom of thought and dignity.[20]

The EDPS notes that Article 5(1)(f) of the AI Act expressly prohibits both the use and the placing on the market, of AI systems to infer emotions of a natural person in the areas of workplace and education. In this regard, the EDPS recommends **a broader interpretation of the notion of "workplace"**, including teleworking and the recruitment phase.

---

[19] ECtHR, S and Marper v UK, App n. 30562/04 and 30566/04 [4 December 2008] GC; ECtHR Glukhin v Russia App n. 11519/20 [4 July 2023].

[20] See e.g. EDPB EDPS Joint Opinion 5/2021, paragraph 35, and International Working Group on Data Protection in Technology (IWGDPT), Working Paper on Facial Recognition Technology Discussed and adopted at the 70th Meeting on 29th-30th November 2022 and 71st Meeting on 7th-8th June 2023 Written Procedure after this meeting, at page 16 and 17.

In addition, the EDPS considers that the rationale for the prohibition of emotion recognition at workplace and at schools, namely the **imbalance of power**, is even more applicable and relevant to the law enforcement context. The same consideration applies also in the field of border control, migration and asylum.

The EDPS considers that the concept "identification" of emotions in Question 19 remains unclear. The introductory statement to that question seems to consider "identification" as the recognition of a previously recorded pair (biometric reference, emotion). The EDPS suggest that use cases for that scenario would be helpful to understand the notion in practice.

Furthermore a more detailed definition of "emotions" in contrast to "physical states" (such as pain or fatigue) and readily apparent expressions such as a smile could enhance clarity.

7. Comments with regard to Question 21 of the consultation: polygraphs (Annex III, point 6(b) and point 7(a) to the AI Act)

The EDPS submits that the AI Act seems to allow for the use of polygraphs (by considering them as high-risk, but not prohibited) at least in following cases included in Annex III of the AI Act:

a) "AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;"
b) "AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies as polygraphs or similar tools;"

In this regard, the EDPS considers that:

a) the **AI Act does not create a presumption of legality** of polygraphs and similar tools, also in the light of the specification "in so far as their use is permitted under relevant Union or national law" in the 'chapeau" in point 6 and 7 of Annex III;
b) the use of polygraphs is only allowed on the basis of national/EU law (where, and insofar as, such 'enabling law' have been enacted); and
c) the use of polygraphs is already prohibited in some Member States[21].

As general observation, the EDPS considers that the processing of personal data related to the use of polygraphs is highly likely to be **disproportionate**, if not breaching the essence

[21] In this sense, having regard to national case law, the decision by the German Federal Constitutional Court, according to which the use of polygraph during criminal proceedings is prohibited (see BVerfG, 1982 NEUE]URISTISCHE WOCHENSCHRIFT, 375; https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5Cnjw%5C1982%5Ccont%5Cnjw.1982.375.1.htm) because these tests invade the individual's intimate sphere, also when the accused person provides consent to the use of the lie detector.

of fundamental rights, and eventually breaching the presumption of innocence and the right not to self-incriminate, thus resulting in direct conflict with essential values of the EU[22].

8. Comments with regard to Question 23, 24 and 25 of the consultation on biometric categorization (Article 5(1)(g) of the AI Act)

The AI Act prohibits the use and the placing on the market of AI systems that categorise natural persons according to 'sensitive characteristics', namely, to infer from biometrics (e.g. face, voice or gait) their race, political opinions, trade union membership, religious or philosophical belief, sex life or sexual orientation.[23] The EDPS considers that the prohibition of the deployment of AI systems using biometrics to categorize individuals into clusters should be interpreted in a broad sense and thus should also cover possible categorisation according to **ethnicity, or other possible grounds for discrimination**[24] [25] prohibited under Article 21 of the Charter. Moreover, the notion of "categorise(ing) individually natural persons" should not be limited to personal data of an individual but also a group of individuals.

According to Article 5(1)(g) of AI Act, the prohibition does not cover any "labelling" or "filtering" of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement. In this regard, the EDPS considers that this part of the legal provision **should not be interpreted as a general derogation for the law enforcement authorities** from the above-mentioned prohibition but as a clarification that there are other types of biometric categorisation for different legitimate purposes, such as age or gender estimation, e.g. in CSAM photos and videos, or "sorting of images according to hair colour or eye colour" (Recital 30 AI Act). Therefore, it essential for the guidelines to unambiguously clarify the scope of such legitimate processing of biometric data by law enforcement authorities and to clearly distinguish it from the prohibited practice of biometric categorization based on sensitive characteristics.

It should also be borne in mind that the use of the biometric categorization systems to infer sensitive characteristics, as specified above and including for law enforcement, would not be compliant with data protection principles (notably in light of the principle of lawfulness and

[22] See EDPB EDPS Joint Opinion 5/2021, paragraph 33; on 'tests' considered by the Court of Justice in breach of Article 1 and Article 7 of the Charter, see Judgment of the Court of 2 December 2014, A, Joined Cases C-148/13 to C-150/13, ECLI:EU:C:2014:2406, paragraph 53.
See also Judgment of the Court (Third Chamber) of 25 January 2018, F, C-473/16, ECLI:EU:C:2018:36, paragraph 35.
[23] Article 5(1)(g) of the AI Act.
[24] In this regard, see Study "Biometric Recognition and Behavioural Detection, Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces", August 2021, p. 54: "Grouping persons into (even uncontroversial) categories based solely on the decision of biometric recognition systems raises further ethical concerns, as the personal identifiers are only alleged. For example, a person's ethnicity, gender or disabilities, or sexuality cannot be inferred exclusively from external appearance because they are much more complex phenomena."
[25] See also International Working Group on Data Protection in Technology (IWGDPT), Working Paper on Facial Recognition Technology Discussed and adopted at the 70th Meeting on 29th-30th November 2022 and 71st Meeting on 7th-8th June 2023 Written Procedure after this meeting, at page 17 and 18: "Biometric categorization systems similarly assume that certain biometric traits are linked to specific tendencies, inclinations, or characteristics – a premise virtually indistinguishable from phrenology or physiognomy. Companies have claimed that these systems can identify a range of traits, including sexuality, autism, likelihood of criminality, and more. However, these technologies rely on historical data containing its own biases, assumptions, and prejudices, frequently exacerbating historic and societal harms towards marginalized groups. We are yet to see evidence that these systems successfully identify anything but existing bias."

fairness of the data processing) and human dignity. Moreover, considerations related to the **societal impact of such AI practices** may also reinforce a finding of non-compliance with GDPR and LED principles by these biometrics-based inferences (which are also object of concern under the accuracy and scientific validity viewpoint and often labelled as 'new phrenology'[26]).

9. Comments with regard to Question 27 and 28 of the consultation on real-time remote biometric identification in publicly accessible spaces (Article 5(1)(h) of the AI Act)

The EDPS notes that, concerning real-time remote biometric identification systems for law enforcement purposes, the AI Act provides a general prohibition, set forth in Article 5(1)(h), subject to some exceptions, exhaustively listed in the same provisions. In this respect, in relation to the **notion of "real-time", the meaning of no "significant delay"** in recital 17 should be clarified. In particular, the EDPS would find it useful to clarify whether the distinction is purely temporal or whether it is rather/also a functional or technical one (for instance the type of system generating the data or the way that data is stored or processed). As the devices used for real-time or post-remote identification are increasingly one and the same with different functionalities, further clarification on this point would be helpful.

With regard to the exemptions, further elaborations on the notions of "**imminent threat to life**" and "**foreseeable threat of a terrorist attack**" would also increase clarity.

Furthermore, the AI Act provides, as safeguards, a set of rules to be complied with if such systems are deployed[27]. It is important to highlight that the AI Act **does not provide a legal basis for this processing under Article 8 LED**[28]. As a result, Member State law would still need to provide the legal basis for processing of personal data under Article 8 LED. Such a law must be sufficiently clear in its terms to give adequate indications of conditions and circumstances, so that its application is foreseeable for those persons who are subject to it.[29]

Taking into account the LED and GDPR, the EDPS has concerns about how large-scale remote identification systems in public spaces would meet the **necessity and proportionality requirements**, and could therefore, be considered acceptable interferences of fundamental rights. In this regard, the Member State law would not only have to comply with the minimum requirements laid down in the AI Act[30], but also comply with all requirements in Article 52 of the Charter as applied by the CJEU.

---

[26] See The reanimation of pseudoscience in machine learning and its ethical repercussions, Andrews, Mel et al., Patterns, Volume 5, Issue 9, 101027.
[27] Recital 38 of the AI Act specifies that: "such use and processing should be possible only in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680".
[28] Ibid.
[29] Article 8, 10, recital 33 LED.
[30] Under Article 5(1)(h), 5(2)-(8) of the AI Act.

The same considerations apply to ***ex post*** remote biometric identification systems[31]. In such cases, the AI Act also provides minimum safeguards. The EDPS notes that **the safeguards** required for such post-remote processing in the AI Act as high-risk AI systems pursuant to Article 26(10) **are slightly lower than for real-time** biometric identification in public spaces, despite the fact that the serious interference with the fundamental rights to privacy and to the protection of personal data, including the so-called 'chilling effect' on the freedoms of movement, association and of expression, can occur regardless of whether the remote biometric identification is performed in real-time or after 'a significant delay'[32]. Moreover, the 48h in-advance-deadline for prior authorisation of a post-remote system by a judicial authorisation does not apply when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence.

Finally, with regard to the minimum requirement to request a judicial authorisation ex ante, the EDPS suggest that the Guidelines should also clarify how to proceed if the authority does not decide within a reasonable timeframe. We note that Article 5(3) - as well as 26(10) of the AI Act - provide for the stopping of the use and the ex-post deletion of data, results and outputs deleted in case the authorisation is rejected. Bearing this in mind, the EDPS would seek clarification as to whether this should be interpreted as a possibility to start the use of the remote biometric identification system if such authorisation is not granted timely.

Brussels, 19 December 2024

(e-signed)
Wojciech Rafał WIEWIÓROWSKI

[31] See Article 26(10) of the AI Act.
[32] EDPB EDPS Joint Opinion 5/2021, paragraph 31.