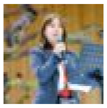
# Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights

VB verfassungsblog.de/shortcomings-of-the-ai-act/



Federica Paolucci

14 March 2024

## Shortcomings of the AI Act

After the much-awaited vote of the 13th March 2024 by the European Parliament, it is time to begin evaluating the state of fundamental rights in light of the AI Act (hereafter, also, the Regulation). In this blog post, three areas of potential inconsistencies and risks are examined: differentiation of provider and deployer, biometrics used in real-time and post-factum, and the standards of biometric recognition in the areas of immigration. I analyze these issues through the lens of the right to an effective remedy, as established by Article 47 of the EU Charter.

## Subjects and responsibilities: the boundary between provider and deployer

One key area requiring clarification in the AI Act pertains to the actors subject to compliance. Concretely, the Regulation differentiates between *deployers* and *providers*. The distribution of compliance obligations follows a "distributed responsibility" model: providers and deployers bear distinct responsibilities to prevent undue burden on a single party, at least in principle.

A *provider* is broadly defined as any entity developing an AI system and introducing it to the market or using it in service. The Regulation imposes stringent obligations on providers, particularly for high-risk AI systems, emphasizing compliance with European legal requirements and accountability principles. Conversely, a *deployer* refers to an actor utilizing an AI system under its authority, excluding non-professional personal activities. Deployers generally need to ensure CE conformity. Also, deployers assume greater responsibility when they are altering the foundational model of a generative AI system.

Accordingly, determining who qualifies as a provider or deployer poses a legal challenge since the differentiation depends on the interpretation of the legal standard, defined as "substantial modification" of the system, as determined in Article 3, paragraph 1, no. 23. The aim of the AI Act is to bear deployers' responsibility on generative AI only if they alter the foundation models, but the Regulation does not provide clearly which modifications suffice the threshold. Hence, it is not sufficiently evident when the provider would not be held liable for an intervention on the AI model committed only by the deployer.

The roles of providers and deployers under the AI Act need a particular observation with regard to the measures already established under existing European and national laws, as per Rec. 10. I specifically refer to the data protection laws. Under Article 35 of the GDPR, the Data Protection Impact Assessment (DPIA) is the measure of accountability to entrust the risks presented by the processing. Among the compliance measure, the AI Act creates a "fundamental rights impact assessment" whose aim is "to identify the specific risks to the rights of individuals or groups of individuals likely to be affected [and] identify measures to be taken in case of the materialization of [these] risks" (Rec. 96). The obligation to perform this ex ante evaluation refers to the deployers of high risky systems in the situations listed under Art. 27 of the AI Act. This Article (par. 4) establishes that, in case the deployer needs to perform a DPIA, the fundamental rights impact assessment referred to shall complement it. Hence, the two compliance measures will be mixed up.

Thus, if a deployer is classified as a "data controller", meaning the subject that determines the purpose and the meaning of the processing under data protection law, it is also responsible for conducting the DPIA under Article 26 par. 9 of the AI Act. Instead, the provider is regarded as a "data processor", being the subject who processes data on behalf of the controller.

Differently, if a provider is portrayed as having real control over an AI system, as with foundation models, data protection authorities would consider the provider as a data controller or potentially a joint controller with the entity deploying the AI system. However, if the provider is perceived as having significant control over the AI system, its classification under GDPR may be altered. Being labelled as a data controller or joint controller comes with additional responsibilities and obligations under data protection laws.

There is no cutting-edge answer as to what degree of control of the AI system the provider must have to be considered a data processor. This issue reflects future challenges of the compatibility of the AI Act with the existing laws and remedies under EU and national laws. This clarification is crucial to establish legal certainty and to understand the distribution of responsibilities among different entities involved in data processing. This clarity is seen as necessary not only to uphold the principle of legal certainty but also to specify the duties of the involved parties and to ensure the protection of individual rights (i.e., Articles 15-22 of the GDPR).

## Biometrics: real-time and ex-post

Regulating biometric recognition systems under Articles 5, 6, and 26 of the Regulation presents significant technical and interpretative challenges. The AI Act distinguishes between *real-time* and *ex-post* application of biometric data, referring to systems where face comparisons occur instantly and where recognition occurs later. Real-time applications of biometric recognition are generally prohibited, while post-uses are considered high-risk. Specifically, real-time biometric identification systems by law enforcement in publicly accessible spaces are prohibited, with exceptions listed in Article 5, paragraph 1, letter h).

Ex-post biometric identification systems are categorized as high-risk AI systems under Article 6, paragraph 2. This classification also includes biometric categorization and emotional recognition systems. Interpreting this rule alongside Article 26 of the AI Act and Annex III is crucial. Importantly, such usage is contingent upon authorization from a judicial or administrative authority but is limited to "targeted" cases. This implies that there is no authorization for widespread and indiscriminate use unless it is directly linked to a criminal threat, ongoing criminal proceedings, or the search for a missing person.

This legal framework presents a few issues that need to be unpacked. In particular, as already pointed out by the Joint Opinion of the EDPB and EDPS (5/2021), the distinction between the real-time and ex-post application of biometric recognition is futile from a fundamental rights perspective. The intrusiveness of the processing does not always depend on *when* the identification or the recognition is performed. The difference is purely technical and consists of two different moments of the identification process, but it entails the same consequences for the surveillance of citizens. Particularly, the biometric system is mostly the same, trained with a biometric data set, that it is used in two modalities: e.g., live while the crime is happening, or after, ex-post.

The second and main concern on biometric recognition relates to the broad freedom granted to Member States to define the modalities of using biometric systems, especially concerning the authorization procedure, as stipulated in Article 5, paragraph 2. While the Regulation identifies the margins within which the use of these systems must occur, it also contains several grey areas. For example, Member States are left to determine which entity should authorize the use of biometric recognition: judicial or independent administrative authority.

There are several reasons why the Member States should move the needle towards a judicial authority. The main reason is to be found in granting judicial independence and transparency of a decision that has high impacts on the individual's rights, as it has been clarified by the European Court of Justice in *Corbiau*, C-24/92 (i.e. par. 15). In this decision, the Court placed significant importance on the idea of independence in defining whether a body constitutes a court or tribunal. This emphasis is not surprising given that the core principle of the rule of law hinges on the reviewability of decisions made by public authorities through independent courts. Thus, the criterion of independence is widely regarded as the most crucial factor distinguishing national courts from administrative authorities.

Moreover, the European Court of Human Rights, in the case of *Glukhin v. Russia* (Application no. 11519/20), pointed out that the procedure for authorizing the use of face recognition in public spaces was deficient. Among other things, it lacked adequate safeguards since “a high level of justification is therefore required in order for them to be considered necessary in a democratic society, […]” (par. 86). In essence, the assurance of judicial independence can be considered to suffice the highest level of justification criterion. Hence, without prejudice to the principle of procedural independence, it is essential for the Member States to determine that judicial authority is going to be the only one in charge of such an authorization in order not to undermine rights and grant procedural fairness.

## Emotion recognition and immigration are subject to high-risk standards

Making sure that judges oversee the authorization process also impacts the utilization of emotion recognition systems. These are extremely controversial uses of AI that, unlike previous versions of the Regulation, have been categorized as high-risk (Annex III, par. 1 lett. c). The use of emotion recognition is not allowed in workplaces and educational settings. However, it is permitted in other cases as long as it adheres to obligations for high-risk systems. Article 52, which deals with transparency obligations, is somewhat unclear. It excludes the requirement to inform individuals undergoing emotional or biometric analysis when the AI systems identify, prevent, and investigate crimes.

Similar issues are raised by the use of AI in the context of migration, where individuals subjected to the collection of their (biometric) data find themselves in a particularly vulnerable situation. In this regard, the Regulation classifies polygraphs and systems used to assess security risks, irregular migration, or health risks as high-risk systems (Annex III, paragraph 7). This applies to an individual entering or having entered the territory of a Member State, for evaluating asylum or visa applications or in the context of border management and control.

The scope of use, as evident, is significantly broad, encompassing numerous and varied scenarios that seem similar in terms of risk level to those designated as prohibited. This aspect has consequences in terms of authorizing the use of biometric and emotion systems in policing, border control, immigration, and asylum. Notably, Recital 59 states:

> “In addition, this Regulation should preserve the ability for law enforcement, border control, immigration, or asylum authorities to carry out identity checks in the presence of the person that is concerned […]. In particular, law enforcement, border control, immigration, or asylum authorities should be able to use information systems in accordance with Union or national law to identify a person who, during an identity check, either refuses to be identified or is unable to state or prove his or her identity, without being required by this Regulation to obtain prior authorization.”

In other words, in specific cases, facial recognition can be used without approval by a judicial or any other authority. This raises serious concerns about the regulation's compatibility with legal certainty and ensuring effective remedies. There is a risk of distorted applications, particularly in sensitive areas like migration, where invasive practices are already prevalent. In cases of irregular migration, where verifying identity upon entry is often difficult due to a lack of documentation, biometric recognition could be extensively used, even beyond the criminal offences listed in Annex II of the Regulation.

## The challenges ahead

This commentary is not meant to cast a negative glance at the AI Act. On the contrary, the AI Act introduces remarkable achievements with respect to the inclusion of the Fundamental Rights Impact Assessment framework for high-risk systems and the exercise of procedural rights in front of the Market Surveillance Authority (Articles 27 and 70). However, concerns remain, including inconsistencies in biometric surveillance and potential inefficiencies of mechanisms of fundamental rights protection. Finally, the imbalance of power between the public authority and the individual, along with the inherent risk of collecting data on vulnerable individuals, are all reasons why judicial authority oversight must be required. In the realm of AI, it is essential for the judiciary to maintain the authority as a protector of rights, particularly in authorizing and monitoring AI's practical implementation.

EXPORT METADATA
Marc21 XMLMODSDublin CoreOAI PMH 2.0

SUGGESTED CITATION  Paolucci, Federica: *Shortcomings of the AI Act: Evaluating the New Standards to Ensure the Effective Protection of Fundamental Rights, VerfBlog,* 2024/3/14, https://verfassungsblog.de/shortcomings-of-the-ai-act/, DOI: 10.59704/363991b7c0205f64.

Explore posts related to this:

Other posts about this region:
Europa