AK EUROPA

Position Paper
February 2025
Digital
Consumers

Regulation (EU) 2024/1689 on artificial intelligence (AI Act)

C(2025) 884 final
C(2025) 924 final

Guidelines on the definition of an AI system and on prohibited AI practices

Executive Summary

Content of the Draft

The Regulation on Artificial Intelligence (AI Regulation; Artificial Intelligence Act – AIA) entered into force on 1 August 2024, is to become fully applicable in two years and sets out the first rules on artificial intelligence in the world. The provisions of Chapter I (General Provisions) and II (Prohibited AI Practices) already apply since 2 February 2025.

The regulation divides AI systems into different risk classes. AI applications with the lowest risk shall remain unregulated, AI systems with limited risk are subject to transparency obligations and those with high risk, which make up the majority of the regulation, are comprehensively regulated. Finally, practices associated with unacceptable risks and that are therefore prohibited in the AI sector are also standardised.

In accordance with Article 96 of the AI Regulation, the European Commission developed guidelines for the implementation of the AI Regulation, including guidelines on the application of the definition of AI system contained in the AI Regulation and on prohibited practices. Those were published by the EU Commission in early February 2025 (C(2025) 884 final and C(2025) 924 final each with annex). The European Commission has carried out a targeted stakeholder consultation, the results of which are to be incorporated into the guidelines. AK (Austrian Federal Chamber of Labour) has contributed the following points.

Definition of AI system

The term "AI system" must be read in conjunction with other provisions of the AI Regulation (such as Article 6(3) of the AI Regulation), but also with other initiatives and draft regulations (such as the Digital Fairness Initiative and the draft directive on AI liability). The majority of the elements of the AI system require further explanation and clarification.

Prohibited AI practices

The prohibitions of AI practices standardised in Article 5 of the AI Regulation must be interpreted in favour of consumers:

- The intentionality or damage is to be assumed even in the case of the mere use of frowned upon and therefore prohibited AI techniques (Article 5(1)(a) and (b) of the AI Regulation).
- The group of persons particularly worthy of protection due to their social or economic situation is to be interpreted broadly (Article 5(1)(b) of the AI Regulation).
- A possible permissible range of applications of social scoring under Article 5(1)(c) of the AI Regulation must be kept to a minimum; if necessary, by clarification in the context of a first revision of the AI Regulation.
- With regard to the prohibition of assessing and predicting the individual risk of committing a criminal offence (Article 5(1)(d) of the AI Regulation), it should be clarified that this also applies to companies that profile consumers to assess the risk of them committing a criminal offence.
- The term "untargeted" in the prohibition of the untargeted scraping of facial images (Article 5(1)(e) of the AI Regulation) should be interpreted broadly, so scraping according to certain categories is still to be understood to be "untargeted".
- The exception to the prohibition of biometric categorisation (concerning the "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 Article 5(1)(g) of the AI Regulation must be explained in more detail.
- The prohibition of real-time biometric remote identification systems in publicly accessible spaces for the purposes of law enforcement pursuant to Article 5(1)(h) of the AI Regulation should be interpreted as broadly as possible.
- The prohibition of emotion recognition, which currently only applies to the workplace and in education institutions under Article 5(1)(f) of the AI Regulation, should be extended to all provider-consumer relationships as part of a future revision of the AI Regulation.
- The relationship of the prohibitions to other EU regulations affecting these areas (such as the AVMSD, DSA and GDPR) must be explained in more detail.

AK's position

Definition of AI system

Advantages and disadvantages:
The individual elements of the definition open up such broad scope for interpretation that, as a consequence of this lack of precision, both a very narrow and a broad scope of application are conceivable. At an AI expert level, there are various assessments of the advantages and disadvantages of the vague description of what AI should actually be within the meaning of the AI Regulation. The option of a narrow interpretation was seen as a locational advantage because only a few algorithmic systems would have to comply with the requirements of the AI Act. Likewise, the opposite thesis is put forward that a broad interpretation favours a surge in innovation because no company could easily bypass the AI Regulation through technological circumvention and thus research and development would not be slowed down.

Consumer perspective:

From the consumer's point of view, the consequences of a broad and narrow scope of application are difficult to predict. Simpler algorithmic systems outside the scope of the AI Regulation would therefore in principle be open to further elaboration by the EU or national legislator (unless the subject matter of the regulation falls within another fully harmonised area). Conversely, the fully harmonising nature of the AI Regulation also means that any application that meets the definition of AI is exempt from further regulatory powers.

This amounts to an ambivalent situation from the consumer's point of view. While a broad definition of AI means that more applications that affect consumers in their everyday lives are subject to the AI Regulation, not all – in fact, probably only a few – of these applications must comply with the product safety and transparency requirements of the AI Regulation or entail data subject rights. Due to the enormous restrictions and exceptions (e.g. as defined in Article 6 and Annex III of the AI Regulation), the broad inclusion of algorithmic systems may also have the undesirable consequence for consumer policy that AI applications are considered harmless, are not regulated by the AI Regulation and rules may not be introduced for reasons of consumer protection. This is because, depending on whether a specific application is classified as unacceptably risky or considered to be associated with high or low risks, its use is prohibited (better: restricted), is subject to the product safety and transparency provisions of the AI Regulation or, apart from voluntary commitments, may not be regulated in the vast majority of cases.

"Digital Fairness Initiative":

Against this backdrop, the European Commission should also place consumer protection in relation to algorithmic systems more clearly and systematically at the heart of its regulation within the framework of its ongoing "Digital Fairness Initiative". For example, the automated fraud prevention and detection processes used by many industries have a high risk of violating the fundamental rights of consumers (privacy, discrimination) or putting them at a financial disadvantage (withholding of contracts, unjustified accusations of abuse or termination). Nevertheless, the AI Regulation expressly declares this area to be a low-risk area (Annex III, point 5(b) of the AI Regulation). With a broad definition of AI, this area would have to be included by the Commission in Annex III of the AI Regulation as soon as the number of consumer complaints increases, or regulated separately within the context of closing the loophole in digital consumer legislation.

Unfavourable schedule:

According to Article 6(5) of the AI Regulation, the European Commission had to provide guidelines on the practical implementation of the exemptions for high-risk systems under Article 6 of the AI Regulation and a "comprehensive" list of practical examples of cases of application for AI systems that are high-risk or not high-risk by 2 February 2026. However, from a consumer perspective, the discussion about the definition of AI cannot be conducted independently of the question of which applications the safety and transparency rules should be applied to at all. If, for example, the European Commission were to come to the conclusion that the automated credit ratings of consumers, which are already widespread on the market, are generally not considered high-risk despite their inclusion in the list of high-risk applications in Annex III pursuant to Article 6(3) of the AI Regulation, consumer protection does not need to comment further on the question of a narrow or broad definition of AI. Rather, the much more salient point is the interpretation of Article 6(3) of the AI Regulation as to whether the AI Regulation provides any levers at all for the interests and protection needs of consumers.

AI definition and consequences for AI liability:

It should be noted that the AI definition is also of crucial importance for the envisaged AI liability. The draft directive adapting the rules on non-contractual civil liability to artificial intelligence (AI Liability Directive) is based on the terminology of the AI Regulation. As it is currently impossible to assess whether the final version of this draft will contain any useful instruments to facilitate legal enforcement for consumers who have suffered harm, the consequences of a broad or narrow interpretation of the definition of AI cannot be reliably assessed.

Almost all elements of the definition of an AI system require further explanation:

Recital 12, which explains the term "AI system", contains far too little interpretation guidance. The original Commission draft of the AI Regulation highlighted examples of AI techniques in its Annex I; in particular, point (c) in Annex I to the Commission draft ("statistical approaches, Bayesian estimation, search and optimization methods") is missing from the list in Recital 12.

It is also unclear whether the descriptive references in the recital are an illustrative or exhaustive list. There are also no provisions in the event of doubt. If there are arguments both for and against a specific application being subject to the AI definition, it should fall within the scope of application in the event of doubt.

Recital 12 emphasises that the definition should "distinguish it from simpler traditional software systems or programming approaches" and should not cover systems "based on the rules defined solely by natural persons to automatically execute operations." The time period of the automated process to which this restriction refers remains unclear. It is not uncommon for self-learning systems to be marketed without learning algorithms or to be further developed or corrected on the basis of rules. Conversely, initially rule-based applications can also achieve a certain degree of autonomy in the subsequent application stage.

The further explanations in Recital 12 essentially reproduce the text of the standard and do not contribute to clarification: "The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use." This leaves the meaning of the standard text, according to which an AI system "may exhibit adaptiveness", completely undefined. It is essential for a system to be able to adapt, or is this optional?

If this characteristic had to be present throughout, the processes described above (such as adaptive training and placing "trained" AI on the market) would be excluded.

According to Recital 12, the techniques that enable differentiation during the design of an AI system include "machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling. "The term "infer" provides too much room for interpretation and must be clearly defined, especially with regard to the mere understanding in the technical sense.

Recital 12 also emphasises that "AI systems are designed to operate with varying levels of autonomy", which means "that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention. "The boundary between this gradual independence and systems dependent on human influence is more than unclear.

Neither the text of the standard nor this explanation define with legal certainty when there is a "different" or "certain level of autonomy". Every algorithmic system operates to a certain extent independently of human intervention. In any case, a definition that only covers complex systems whose decision-making processes cannot be traced and which therefore have a black box nature cannot be a suitable differentiation criterion. This is because explainability remains a mandatory requirement for the manufacturer or user; if this were not the case, they would not be able to comply with the transparency obligations under the AI Regulation or the requirements under Article 22 of the General Data Protection Regulation (GDPR) or the future AI Liability Directive and would immediately become liable as the controller in the event of damage.

The term "machine-based" refers to the fact that AI systems are operated by machines. This is initially trivial and undisputed, but does not go into more detail about which human (e.g. corrective) interventions in the process are (not) detrimental to this concept. This is because AI systems are always socio-technical systems that must be subject to human oversight in accordance with Article 14 of the AI Regulation. It is unclear when human intervention at the "human-machine interface" (see Article 14(1) of the AI Regulation) deprives the system of its machine-based nature.

Recital 12 further states that "reference to explicit or implicit objectives" would "underscore that AI systems can operate according to explicit defined objectives or to implicit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific context." The exact difference between objectives and purposes remains a mystery. The standard text uses the term "objectives"; for data processing under the GDPR, the lawful "purposes" must be made clear to consumers. Legally compliant applications for data protection purposes that serve completely different AI "objectives" are difficult to imagine. The explanations raise more questions in this regard than they provide answers.

Differentiation from simple software:

Simpler software should be excluded under Recital 12, especially rule-based systems that perform operations automatically (such as, according to the consultation document, "statistical methods, such as logistic regression, triggered questions related to the conditions under which certain software should be considered out of the scope of AI system definition").

Some of these examples of exclusions do not emerge either from the text of the standard or from Recital 12 and are also diametrically opposed to the list in Annex I of the Commission's original draft. This also contained in (c) "Statistical approaches" (and also "Bayesian estimation, search and optimization methods").

There is an urgent need to clarify the justification for this restriction. In view of the protective purpose of the regulation, which is to ensure that only safe and transparent AI products are placed on the market with regard to fundamental rights, health, financial risks, etc., restrictions in terms of the complexity or simplicity of algorithms would be detrimental to consumer interests. Even simpler algorithms (whatever that happens to mean) can cause serious harm to consumers by scoring their characteristics, creditworthiness or behaviour. This further differentiation feature, which is mentioned in Recital 12 but does not appear in the text of the standard, should therefore not be used.

II. Prohibited AI practices:

Prohibition of subliminal influencing or intentionally manipulative or deceptive techniques (Article 5(1)(a) of the AI Regulation):

There is an urgent need for clarification of almost all of the elements of Article 5(1)(a) of the AI Regulation. For example, what counts as "subliminal techniques" in times of severe manipulation on the Internet? In psychological terms, the term has long stood for the ultra-short, subliminal playout of images and audio sounds, in other words: beyond conscious perception. The term should be reinterpreted from the consumer's point of view: all "dark patterns" and behaviourist tricks from behavioural psychology should fall under the offence. Otherwise, the subsumption of these cases of manipulation under the second element of the prohibition standard ("purposefully manipulative or deceptive techniques") would be unacceptably difficult. The prohibition of manipulative or deceptive techniques requires proof of subjective "purpose". Consumer associations would have to prove that the manufacturer or user of an AI technology pursues the objectives of significantly changing the behaviour of consumers or strives for that effect. This detection threshold is not only set inexplicably high; it would also be diametrically opposed to comparable standards of consumer protection law, in which unlawfulness is linked exclusively to objective corporate behaviour.

Also according to the Unfair Commercial Practices Directive (UCPD), the Audiovisual Media Services Directive (AVMSD), the Digital Services Act, etc., no deception, misleading, behaviour-influencing "dark patterns" may be used and the easy suggestibility of children and adolescents may never be exploited. It would be unacceptable for AI to fall significantly short of this level of protection.

From the consumer's point of view, the manipulation of people is objectionable per se. It would be difficult to prove intent and an at least probable occurrence of damage in individual cases. Overreaching and damage caused by AI technologies would be significantly favoured over conventional unfair, prohibited market practices. This unequal treatment would benefit non-European online platforms in particular, given the technological lead of Big Tech companies from third countries.

The requirement to prove these two elements should therefore be waived in as far as this is possible. Instead, the European Commission should explain that the deliberate use of these techniques and their tendency to take advantage of or harm consumers must be assumed for companies that benefit from the use of such practices.

Subliminal, manipulative or deceptive techniques requiring further clarification:

From the point of view of AK, there is an urgent need for clarification: The digital economy is gaining more and more power over consumers and citizens through excessive data usage and the use of AI. "Take it or leave it" is often the motto of online providers. Those who go along with that have their behaviour monitored and attempts are made to influence how they

act. Consumers are seen as data material and guinea pigs to be manipulated. AK misses fair treatment in the sense of autonomy, respect and transparency for consumers who are disadvantaged in the light of massive power and knowledge asymmetries. This development is perilous not only for consumers, but also for free, democratic societies.

Digital fairness is unthinkable without digital sovereignty. Consumers do not want to be at the mercy of opaque online tactics that undermine their self-determination. Fairness and sovereignty do not arise of their own accord. The imbalance of power and knowledge between the parties involved is too great for that. Digital self-determination rights and fairness towards consumers must be formulated in detail as an AI standard.

The European Commission should therefore also include the results of the two consultations on the "Digital Fairness Initiative" of the Directorate-General for Consumer Protection in its guidelines on the prohibited practices under Article 5 of the AI Regulation.

There are countless AI practices that would be worth banning. Let's take just one example to illustrate this. From a consumer perspective, the AI-based setting of individual prices for consumers on the internet would be worth prohibiting. In this regard, AK refers to the BEUC position paper on personalised pricing ("Each consumer a separate market?"). The aim of any price personalisation is to set the price at a level that the individual person is just about willing to pay instead of jumping ship. The idea that the weapons of customer data analysis, neuropsychological tricks and individual price adjustments can be used to manipulate vulnerable consumers (addictive behaviour, necessary purchases, etc.) is extremely worrying. From a consumer perspective, fully individualised prices should therefore be prohibited, and especially AI-based determination of individual willingness to pay should be prohibited. Where prices are target group-specific (third degree price discrimination such as senior citizen tickets or student subscriptions), consumers must be informed in advance of the range of possible prices (amendment to the Consumer Rights Directive and the Price Indication Directive). They must be able to easily recognise why they belong to a certain price category (indication of the price parameters and their weighting). The segmentation of customers who are "too unprofitable" or "undesirable" can lead to a provider-driven strategy of inflated prices to simply get rid of certain customer groups. Behavioural forecasts and prices based on their outcomes are therefore unjustifiable, especially for essential services. The (in)admissibility of price discrimination must therefore be precisely regulated. The prohibitions of the ECHR (age, gender, ethnicity, etc.) should be extended to economic prognoses (income, creditworthiness) and other characteristics with a high potential for discrimination (place of residence, profitability). Limits for personalised marketing techniques through profiling must also be defined.

Many manipulative practices also affect other legal acts (GDPR, AVMSD, Unfair Commercial Practices Directive, DSA, etc.). The AI bans should be coordinated with consumer protection legislation and case law. As long as there is no clear regulation at an EU level on how consumers can navigate the internet in a sovereign and self-determined manner without being profiled and without the risk of manipulation, consumers are permanently exposed to countless marketing practices that they cannot defend against, or cannot defend against with reasonable effort. Only the introduction of practicable "stop tracking" tools and rigorous enforcement of opt-in and opt-out requirements for data use under the GDPR would protect the average consumer from constant attempts at manipulation. However, as long as there are enormous loopholes in protection and no easily manageable defence mechanisms for consumers, the majority of AI-based marketing and sales techniques should be banned in light of their behaviour-influencing and harmful tendencies.

Prohibition of harmful exploitation of particular vulnerability (Article 5(1)(b) of the AI Regulation):

Almost all elements of the offence require clarification.

The assumption that consumers act in a sovereign manner when detailed information is available to them is outdated. See the reasoning of the European Law Institute. Trust may easily be abused and behaviour may readily be manipulated in the digital economy. We know from our everyday work advising citizens that even extremely well-informed and well-educated individuals, in the hope of fabulous profits, transfer their entire fortunes to dubious online investment scammers. These are increasingly often misusing AI (profiling, deep fakes, voice imitation, phishing news, etc.). Consumers are unable to see through complex products or services and the interests of other players in the digital value chain (such as advertising networks). Disinformation is commonplace. AI is capable of exploiting human vulnerabilities. The AI Regulation fails to properly acknowledge this reality. For instance, Article 5 of the AI Regulation only prohibits AI systems that exploit the weakness of consumers due to their age, disability or a specific social or economic situation, and that are likely to cause mental or physical harm.

From AK's perspective, manipulation must be unacceptable and inadmissible per se, regardless of the

consumer's individual situation. Permanently vulnerable consumers must replace the model of average (informed, understanding, careful, etc.) consumers in legislation and case law. It should be recognised that, in addition to particularly vulnerable groups (such as children), each and every one of us is constantly vulnerable online due to complex issues, lack of technical expertise, information deficits and information overload. In order to do justice to this state of science, "social and economic situation" in Article 5(1)(b) of the AI Regulation should be interpreted so broadly that it also covers the average, overburdened Internet user.

As already explained in more detail in the prohibition of subliminal influence or intentionally manipulative or deceptive techniques, the proof of probability of harm is an inexplicably high hurdle that is not found in other fairness law, which is intended to protect consumers from overreaching. Against this background, we consider it necessary to assume that there is a probability of harm if AI users derive an advantage from a manipulative practice.

Prohibition of social scoring (Article 5(1)(c) of the AI Regulation):

The majority of the elements of the offense require clarification, especially the following two, which only turn scoring, which is permitted in principle, into a prohibited offence:

(i) "in social contexts […] unrelated to the contexts in which the data was originally generated or collected"

(ii) "treatment […] that is unjustified or disproportionate to their social behaviour or its gravity"

Many types of scoring would therefore be permitted and unregulated (unless covered by Annex III to the AI Regulation and also high-risk according to Article 6(3) of the AI Regulation). Only social scoring based on data that was originally collected for other purposes or in the case of disadvantages that are disproportionate in terms of social (mis)behaviour is prohibited. In other words: If data that was originally collected for scoring purposes were available for AI training and the use of AI, this would apparently not be a problem from the European Commission's perspective. Even discrimination against persons would be admissible as long as it is not disproportionate to the person's social (mis) behaviour.

The question is, which company and which authority in a democratic system can even presume to collect personal data with the intention of numerically evaluating the personal characteristics, personality traits and social behaviour of its citizens?

Projects of this kind soon touch upon human dignity, so there is little scope for permissible uses. At this point, we may recall a milestone in fundamental rights jurisprudence, the German "census judgment" of 1983: *"A societal order and its underlying legal order would not be compatible with the right to informational self-determination if citizens were no longer able to tell who knows what kind of personal information about them, at what time and on which occasion. Individuals who worry that non-conformist behaviour could be recorded at any time and that such information could permanently be stored, used or shared will try not to draw attention to themselves by not engaging in such behaviour. […] Not only would this impair opportunities of personal development for the individual, it would also affect the common good because self-determination is a fundamental prerequisite for the functioning of a free and democratic society which relies on the agency and participation of its citizens."*

From the consumer's point of view, what is needed is a comprehensive ban on social surveillance. Otherwise, all considerations would have to be left to the courts to decide on a case-by-case basis. This leads to a shocking lack of legal certainty about the extent to which social scoring is permitted. Just about anything can be subsumed under the "classification of natural persons or groups of persons over a certain period of time based on their social behaviour" within the meaning of Article 5(1)(c) of the AI Regulation (customer segregation according to characteristics, politically coordinated messages, fraud prevention, prioritisation of scarce funds and resources, triage in the health care system, control of social transfer payments, etc.)?

The only legally relevant barrier is that the use of primary data for scoring purposes as required by the AI Regulation must also be permitted under the GDPR. The AI Regulation does not prohibit scoring, except for grossly disproportionate disadvantages in relation to undesirable social behaviour. It merely specifies Article 6(4) of the GDPR, according to which existing data (for another purpose) may not be used for scoring purposes.

If a company were to come up with the idea that it is in its legitimate interest under the GDPR to assess the tendency of its policyholders to commit fraud, the tendency of its subscribers to cancel their subscriptions, etc. on the basis of the person's previous behaviour (or even their merely statistically calculated, i.e. merely assumed characteristics), there is nothing in the AI Regulation to stop them from doing so. A scoring ban is hardly going to happen. To achieve this, at least to some extent, the individual elements would have to be designed to be as consumer-friendly as possible:

- Social conduct must be narrowly defined and may only relate to direct contractual transactions (or the statutory eligibility requirements for the receipt of social benefits, etc.).

- There are hardly any applications that comply with constitutional rights that involve the "known, inferred or predicted personal or personality characteristics". Who must be aware of the characteristic for it to be considered applicable and relevant? Which predicted characteristics must consumers permissibly allow to be attributed to them without this contradicting the GDPR or even the ECHR (human dignity)? It would at least be appropriate to limit the assessable characteristics to externally perceptible circumstances (period of unemployment, number of orders, etc.) and not to make presumed character traits, emotions, attitudes, convictions, intelligence, etc. accessible for assessment. Particularly sensitive data (such as data relating to health) should not be allowed to be used for social scoring at all.

- In social contexts, discrimination would be acceptable to the person concerned if the discrimination is proportionate or even disproportionate in relation to the social behaviour, but is covered by data collected lawfully for scoring purposes. From a consumer perspective, it is alarming that the AI Regulation does not contain any additional safeguards in view of the potential depth of the encroachment on fundamental rights (such as official or judicial authorisation, as in the case of remote biometric identification). In the interest of all potentially affected consumers and citizens, AK therefore hopes that the European Commission will limit the permissible range of applications to a minimum that can still be reconciled with the wording of Article 5 of the AI Regulation. In the future, AK considers it a matter of urgency to tighten this provision in the first revision of the Regulation.

- A latent mistrust of consumers with regard to the legality of their behaviour violates the principle of trust in a constitutional state in a very fundamental way and leads to an extremely undemocratic security society that monitors and evaluates consumer behaviour at every turn through data collection and its algorithmic evaluation.

Prohibition of individual crime risk assessment and prediction of crime risk (Article 5(1)(d) of the AI Regulation):

The majority of the factual elements require clarification. There is a strikingly obvious need for clarification with regard to the exception to the ban. This excludes support systems linked to verifiable facts about a person's involvement in a criminal act.

With regard to consumers, the parties which this regulation targets must be clarified.

It should be made clear that companies that assess consumers in relation to conduct relevant to criminal law (e.g. falsification of documents or identity, false self-disclosure, misuse of online services, insurance or payment fraud, violation of platform regulations for messenger services) are also subject to the ban.

Prohibition of the untargeted scraping of facial images (Article 5(1)(e) of the AI Regulation):

With this prohibition standard, it is particularly questionable when it is no longer a case of untargeted scraping. If, for example, images are analysed by AI according to certain categories of people, this activity should fall within the scope of application.

Prohibition of emotion inference (Article 5(1)(f) of the AI Regulation):

At this point it should be mentioned once again, as it has been in numerous AK statements prior to the adoption of the AI Regulation, that it is extremely disappointing from a consumer perspective that the inference of emotions is only prohibited in the workplace and in education institutions. The justification in the recital that this is necessary due to the particularly asymmetrical positions of power is not convincing. This imbalance of power is also present in the supplier-consumer relationship. Against this background, it can only be hoped that this gross omission will be rectified in the first revision of the Regulation. The current classification as Annex III material and thus as a high-risk application is by no means sufficient to protect consumers. Too much legal uncertainty, not least with regard to the exceptions in Article 6(3) of the AI Regulation, gives rise to fears that consumers will be exposed to a variety of practices of emotion analysis for the purposes of marketing, sales promotion and manipulation of their behaviour, to which consumers would never actively consent and which ultimately generally violate their personal rights in the sense of human dignity under the ECHR.

Prohibition of biometric categorisation (Article 5(1)(g) of the AI Regulation):

The majority of the elements of the offence require clarification, especially the exception to the prohibition in the last sentence of the standard. Accordingly, the ban "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. "The extent to which the most relevant and sensitive use case in the field of criminal prosecution is excluded would need to be

clarified. There is probably no need for further studies to prove that categorisation according to ethnicity or skin colour is one of the areas most prone to discrimination. Why the prohibited categorisation does not also include health data, which is equally sensitive and particularly worthy of protection, needs to be clarified.

Prohibition of biometric remote real-time identification systems (Article 5(1)(h) of the AI Regulation):

Reference may be made to the Joint Opinion of the EDPS and the EDPB, which are fundamentally critical of real-time remote biometric identification. Initially, the European Commission also considered a temporary moratorium to improve the study situation on the effects of such surveillance, which are contrary to fundamental rights and harmful to society (behavioural adaptation, feeling of constant surveillance, discrimination).

From a consumer perspective, AK hopes for an interpretation that restricts the permissible controls of public spaces through real-time remote identification with as broad a reach as possible. Unfortunately, given the broad definition of "public space", consumers will often be affected by measures of this kind (accessibility for an indefinite number of people, privately or publicly owned, with the possibility of restrictive access conditions). Shopping centres, shops and airports all fall within the defined area. It can be assumed that the right to privacy will likely be hugely impaired for many citizens and consumers despite the protective guarantees that have been withdrawn (such as approval procedures under Article 5(3) of the AI Regulation). Above all, the anti-democratic developments in some Member States give rise to fears that moving away from a ban on surveillance without exception harbours great potential for discrimination against marginalised population groups.

Prohibitions and their relationship to other EU legislation:

The prohibitions under Article 5 of the AI Regulation sometimes affect areas that are already regulated in other EU legal acts. The relationship between Article 5 of the AI Regulation and, in particular, the following provisions from other EU legal acts must be clearly regulated.

- **Stricter rules in Article 9 of the AVMSD:**

According to Article 9(1)(b) of the AVMSD, audiovisual commercial communications may not use subliminal techniques.

According to Article 9(1)(c) of the AVMSD, audiovisual commercial communications may not

i. "prejudice respect for human dignity;

ii. include or promote any discrimination based on sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation;

iii. encourage behaviour prejudicial to health or safety;

iv. encourage behaviour grossly prejudicial to the protection of the environment."

- **Article 25 of the Digital Services Act (DSA) – online interface design and organisation**

Article 25 of the DSA stipulates that providers of online platforms shall not design, organise or operate their online interfaces in a way that "deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions."

- **Article 28 of the DSA – online protection of minors**

Article 28(1) of the DSA requires providers of online platforms accessible to minors to put in place measures to ensure a high level of privacy, safety and security of minors. According to Article 28(2) of the DSA, advertising based on profiling as defined in Article 4(4) of the GDPR is prohibited for minors.

- **Article 5(3) of the Unfair Commercial Practices Directive (UCPD) –prohibition of unfair commercial practices**

Article 5(3) of the UCPD prohibits practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity. According to this provision in the UCPD, it is not necessary to prove certain elements of the offense as under Article 5 of the AI Regulation (e.g. probability of damage).

- **Article 9(4) of the GDPR – processing of special categories of personal data**

Article 9(4) of the GDPR states: "Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health."

- **Article 22 of the GDPR – automated individual decision-making, including profiling**

Article 22(1) of the GDPR reads: "The data subject shall have the right not to be subject to a decision based

solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

According to Article 22(1) of the GDPR, this prohibition of exclusively automated decision-making does not apply if the data subject has consented, if it is necessary entering into, or performance of, a contract or if legal provisions permit such decisions and if these lay down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

These safeguards are either completely absent (namely in the unregulated area of the AI Regulation) or are not fully reflected in the AI Regulation (Article 22(3) of the GDPR – "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision").

Article 22(4) of the GDPR reads: "Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

Contact us!

In Vienna:

Daniela Zimmer
T +43 (0) 1 501 65 12722
daniela.zimmer@akwien.at

Louise Beltzung
T +43 (0) 1 501 65 12324
louise.beltzung@akwien.at

Jasmin Reininger
T +43 (0) 1 501 65 12801
jasmin.reininger@akwien.at

In Brussels:

Sarah Bruckner
T +32 (0) 2 230 62 54
sarah.bruckner@akeuropa.eu

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Vienna, Austria
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

AK EUROPA
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54

www.akeuropa.eu

About us

The Austrian Federal Chamber of Labour (AK) is the legal body which represents the interests of approximately 4 million employees and consumers in Austria. It represents its members on all social, educational, economic and consumer policy-related issues at national level and at EU level in Brussels. Furthermore, the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectives of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Information from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.