Contribution ID: f8fd439d-29b7-46c1-b3ce-cd9f9cfc125d
Date: 11/12/2024 19:03:33

MULTI-STAKEHOLDER CONSULTATION FOR COMMISSION GUIDELINES ON THE APPLICATION OF THE DEFINITION OF AN AI SYSTEM AND THE PROHIBITED AI PRACTICES ESTABLISHED IN THE AI ACT

Fields marked with * are mandatory.

MULTI-STAKEHOLDER CONSULTATION FOR COMMISSION GUIDELINES ON THE APPLICATION OF THE DEFINITION OF AN AI SYSTEM AND THE PROHIBITED AI PRACTICES ESTABLISHED IN THE AI ACT

Disclaimer: This document is a working document for consultation and does not prejudge the final decision that the Commission may take on the final guidelines. The responses to this consultation paper will provide important input to the Commission when preparing the guidelines.

The European AI Office is launching this multi-stakeholder consultation on the application of the definition of an AI system and the prohibited AI practices established in the AI Act. This consultation is **targeted to stakeholders of different categories**, including providers and deployers of AI systems such as businesses, authorities (including local public authorities) and other organisations, academia and research institutions, trade unions and other workers' representatives, civil society organisations, public supervisory authorities, and the general public.

As not all questions may be relevant for all stakeholders, respondents may reply only to the section(s) and the questions they consider relevant. Respondents are

encouraged to provide **explanations and concrete cases** as part of their responses to support the practical usefulness of the guidelines.

The targeted consultation is available in English only and will be **open for 4 weeks starting on 13 November until 11 December 2024 (till 23:59). We strongly encourage early submissions.**

The questionnaire for this consultation is structured along 2 sections with several questions.

1. Questions in relation to the definition of an AI system

2. Questions in relation to prohibited AI practices

We **welcome collective answers from organisations.** You have the option to indicate if you a submitting such a collective answer in the end of the first section and identify the organisations on whose behalf the submission is made.

We welcome full or partial replies from all respondents based on their expertise and perspective.

All contributions to this consultation may be made publicly available. Therefore, please do not share any confidential information in your contribution. Individuals can request to have personal information removed from their contribution.

The Commission may publish a summary of the results of the consultation. In that case, results will be based on aggregated data and respondents will not be directly quoted.

Please allow enough time to submit your application before the deadline to avoid any issues. In case you experience technical problems which prevent you from submitting your application within the deadline, please take screenshots of the issue and the time it occurred.

In case you face any technical difficulties or would like to ask a question, please contact: CNECT-AIOFFICE@ec.europa.eu

---

General Introduction

The Artificial Intelligence Act (Regulation (EU) 2024/1689, hereinafter 'the AI Act'), which entered into force on 1 August 2024, improves the internal market by laying down harmonised rules for trustworthy and human-centric Artificial Intelligence (AI) in the EU (Article 1 AI Act). It aims to promote innovation and uptake of AI, while ensuring a high level of protection of health, safety and fundamental rights, including democracy and the rule of law.

The AI Act establishes a common definition of an AI system, aligned with the OECD definition (OECD Recommendation on Artificial Intelligence (OECD /LEGAL/0449, 2019, amended 2023)), as a central element of the scope of the AI Act (Article 3(1) AI Act and Recital 12). The AI Act follows a risk-based approach to regulating AI systems, by classifying such systems into different risk categories. One of which are the prohibited AI practices covering AI systems posing unacceptable risks to fundamental rights and European values (Article 5 AI Act).

Pursuant to Article 96(1) AI Act, the Commission must develop guidelines on the practical implementation of the Regulation, *inter alia*, on the prohibited AI practices referred to in Article 5 AI Act and the application of the definition of an AI system as set out in Article 3(1).

The purpose of the present targeted stakeholder consultation is to collect input from a wide range of stakeholders on concrete examples of AI systems and issues with the practical application of the relevant AI Act provisions that could be clarified in the Commission's **guidelines** on the **definition of an 'AI system'** as well as guidelines on the **prohibited AI practices**. The definitions and prohibitions are applicable six months after the entry into force of the AI Act, as from 2 February 2025. The input from this consultation will feed into the Commission guidelines to be adopted in early 2025. It should be noted that the

legal concepts in relation to the AI system definition and the prohibitions are already set out in the AI Act. The Commission launches the present consultation to seek additional practical examples from stakeholders to feed into the guidelines and provide further clarity on practical aspects and use cases.

The objective of the guidelines is to provide consistent interpretation and practical guidance to assist competent authorities in their enforcement actions as well as providers and deployers subject to the AI Act in their compliance actions with a view to ensuring consistent, effective and uniform application of the prohibitions and understanding of what constitutes an AI system within the scope of the AI Act.

About you

* 1. Do you represent one or more organisations (e.g., industry organisation or civil society organisation) or act in your personal capacity (e.g., independent expert)?

- (●) Organisation(s)
- ( ) In a personal capacity

If you are organisation(s), please specify the name(s):

Deep Law for Tech (DL4T), with the individual participation of
Marina Teller, Marylou Leroy, Caroline Berard-Gourisse, Romain Maillot, Alaadin Maraqa, Jingyan Wu, Godefroy de Boiscuille, Mina Ilhan, Mélanie Olivari, Julie Charpenet

If you would like to share any affiliation, please specify:

Université Côte d'Azur

* First name

Julie

* Surname

Charpenet

* E-Mail address (this won't be published)

julie.charpenet@univ-cotedazur.fr

* Are you headquartered/residing in the EU?

- (●) Yes
- ( ) No
- ( ) Other (e.g. multiple organisations)

* Headquarter / Country of residence

- ( ) AF - Afghanistan
- ( ) AL - Albania
- ( ) DZ - Algeria
- ( ) AD - Andorra
- ( ) AO - Angola
- ( ) AG - Antigua and Barbuda
- ( ) AR - Argentina
- ( ) AM - Armenia
- ( ) AU - Australia
- ( ) AT - Austria
- ( ) AZ - Azerbaijan
- ( ) BS - Bahamas
- ( ) BH - Bahrain
- ( ) BD - Bangladesh
- ( ) BB - Barbados
- ( ) BY - Belarus
- ( ) BE - Belgium
- ( ) BZ - Belize
- ( ) BJ - Benin
- ( ) BT - Bhutan
- ( ) BO - Bolivia
- ( ) BA - Bosnia and Herzegovina
- ( ) BW - Botswana
- ( ) BR - Brazil
- ( ) BN - Brunei Darussalam
- ( ) BG - Bulgaria
- ( ) BF - Burkina Faso

- BI - Burundi
- CV - Cabo Verde
- KH - Cambodia
- CM - Cameroon
- CA - Canada
- CF - Central African Republic
- TD - Chad
- CL - Chile
- CN - China
- CO - Colombia
- KM - Comoros
- CG - Congo
- CR - Costa Rica
- CI - Côte D'Ivoire
- HR - Croatia
- CU - Cuba
- CY - Cyprus
- CZ - Czechia
- CD - Democratic Republic of the Congo
- DK - Denmark
- DJ - Djibouti
- DM - Dominica
- DO - Dominican Republic
- EC - Ecuador
- EG - Egypt
- SV - El Salvador
- GQ - Equatorial Guinea
- ER - Eritrea
- EE - Estonia
- SZ - Eswatini
- ET - Ethiopia
- FJ - Fiji
- FI - Finland
- FR - France

- GA - Gabon
- GM - Gambia
- GE - Georgia
- DE - Germany
- GH - Ghana
- GR - Greece
- GD - Grenada
- GT - Guatemala
- GN - Guinea
- GW - Guinea Bissau
- GY - Guyana
- HT - Haiti
- HN - Honduras
- HU - Hungary
- IS - Iceland
- IN - India
- ID - Indonesia
- IR - Iran
- IQ - Iraq
- IE - Ireland
- IL - Israel
- IT - Italy
- JM - Jamaica
- JP - Japan
- JO - Jordan
- KZ - Kazakhstan
- KE - Kenya
- KI - Kiribati
- KW - Kuwait
- KG - Kyrgyzstan
- LA - Laos
- LV - Latvia
- LB - Lebanon
- LS - Lesotho

- LR - Liberia
- LY - Libya
- LI - Liechtenstein
- LT - Lithuania
- LU - Luxembourg
- MG - Madagascar
- MW - Malawi
- MY - Malaysia
- MV - Maldives
- ML - Mali
- MT - Malta
- MH - Marshall Islands
- MR - Mauritania
- MU - Mauritius
- MX - Mexico
- FM - Micronesia
- MC - Monaco
- MN - Mongolia
- ME - Montenegro
- MA - Morocco
- MZ - Mozambique
- MM - Myanmar
- NA - Namibia
- NR - Nauru
- NP - Nepal
- NL - Netherlands
- NZ - New Zealand
- NI - Nicaragua
- NE - Niger
- NG - Nigeria
- KP - North Korea
- MK - North Macedonia
- NO - Norway
- OM - Oman

- PK - Pakistan
- PW - Palau
- PA - Panama
- PG - Papua New Guinea
- PY - Paraguay
- PE - Peru
- PH - Philippines
- PL - Poland
- PT - Portugal
- QA - Qatar
- MD - Republic of Moldova
- RO - Romania
- RU - Russian Federation
- RW - Rwanda
- KN - Saint Kitts and Nevis
- LC - Saint Lucia
- VC - Saint Vincent and the Grenadines
- WS - Samoa
- SM - San Marino
- ST - Sao Tome and Principe
- SA - Saudi Arabia
- SN - Senegal
- RS - Serbia
- SC - Seychelles
- SL - Sierra Leone
- SG - Singapore
- SK - Slovakia
- SI - Slovenia
- SB - Solomon Islands
- SO - Somalia
- ZA - South Africa
- KR - South Korea
- SS - South Sudan
- ES - Spain

- LK - Sri Lanka
- SD - Sudan
- SR - Suriname
- SE - Sweden
- CH - Switzerland
- SY - Syrian Arab Republic
- TJ - Tajikistan
- TZ - Tanzania
- TH - Thailand
- TL - Timor-Leste
- TG - Togo
- TO - Tonga
- TT - Trinidad and Tobago
- TN - Tunisia
- TR - Turkey
- TM - Turkmenistan
- TV - Tuvalu
- UG - Uganda
- UA - Ukraine
- AE - United Arab Emirates
- GB - United Kingdom
- US - United States of America
- UY - Uruguay
- UZ - Uzbekistan
- VU - Vanuatu
- VE - Venezuela
- VN - Viet Nam
- YE - Yemen
- ZM - Zambia
- ZW - Zimbabwe

* Do you have an office or other kind of representation in the EU?

- Yes, we have a subsidiary, branch office or similar in the EU
- Yes, other
- No

- (●) Not applicable

If applicable, please specify

*If you are an organisation, what is the size of your organisation and does it qualify as a small or medium sized enterprise according to the EU recommendation 2003 /361, if applicable ?

- (●) Small
- ( ) Medium
- ( ) Large
- ( ) Other (e.g. multiple organisations, local authorities)
- ( ) Not applicable

If other, please specify

*Which stakeholder category would you consider yourself in?

- ( ) Provider of an AI system
- ( ) Deployer of an AI system
- ( ) Other industry organisation, or acting on behalf of such organisations
- (●) Academia
- ( ) Civil Society Organisation
- ( ) Public authority
- ( ) Citizen
- ( ) Others

If other, please specify

*In which sector do you operate?

- [ ] Information technology
- [ ] Public sector
- [x] Law enforcement
- [ ] Security

- [ ] Media
- [ ] Healthcare
- [ ] Employment
- [ ] Education
- [ ] Consumer services
- [ ] Business services
- [ ] Banking and finance
- [ ] Manufacturing
- [ ] Energy
- [ ] Transport
- [ ] Telecommunications
- [ ] Retail
- [ ] E-commerce
- [ ] Advertising
- [ ] Arts & Entertainment
- [ ] Others
- [ ] Not applicable

If other, please specify

* Please briefly describe the activities of your organisation or yourself:

1000 character(s) maximum

The Deep Law for Tech project (DL4T) at Université Côte d'Azur explores the interaction between law and emerging technologies. Its goal is to envision legal solutions tailored to the challenges of digital transformation and artificial intelligence. Activities include interdisciplinary research on legal frameworks for advanced technologies, such as AI, quantum and so on, training legal professionals specialized in tech, and collaborating with industrial and institutional partners.

Is your organisation submitting a collective answer on behalf of other organisations?

- ( ) Yes
- (•) No
- ( ) Not applicable

Please specify

All contributions to this consultation may be made publicly available. Therefore, please do not share any confidential information in your contribution. For organisations, their organisation details would be published while respondent details can be requested to be anonymised. Individuals can request to have their contribution fully anonymised. Your e-mail address will never be published.

Please select the privacy option that best suits you. Privacy options default based on the type of respondent selected.

* **For natural persons: Contribution publication privacy settings**

If you act in your personal capacity: All contributions to this consultation may be made publicly available. You can choose whether you would like your details to be made public or to remain anonymous.

- ○ **Anonymous.** The type of respondent that you responded to this consultation as, your answer regarding residence, and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself.
- ○ **Public.** Your name, the type of respondent that you responded to this consultation as, your answer regarding EU nationality, and your contribution may be published.
- ◉ Not applicable

* **For organisations: Contribution publication privacy settings**

If you represent one or more organisations: All contributions to this consultation may be made publicly available. You can choose whether you would like respondent details to be made public or to remain anonymous.

- ○ **Anonymous.** Only organisation details may be published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its size, its presence in or outside the EU and your contribution may be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

- **Public.** Organisation details and respondent details may be published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its size, its presence in or outside the EU and your contribution may be published as received. Your name will also be published.
- Not applicable

Privacy statement

- I acknowledge the attached privacy statement.

  Privacy_Statement.pdf

Questionnaire

Section 1. Questions in relation to the definition of an AI system

The **definition of an AI system** is key to understanding the scope of application of the AI Act. It is a first step in the assessment whether an AI system falls into the scope of the AI Act.

The definition of an 'AI system' as provided in Article 3(1) AI Act is aligned with the OECD definition: '*AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.*'

Recital 12 provides further clarifications on the definition of an AI system.

The following seven elements can be extracted from the definition:

1) 'a machine-based system'
2) 'designed to operate with varying levels of autonomy'
3) 'may exhibit adaptiveness after deployment',
4) 'for explicit or implicit objectives',
5) 'infers, from the input it receives, how to generate outputs'

6) ‘predictions, content, recommendations, or decisions’
7) ‘can influence physical or virtual environments’

Question 1: Elements of the definition of an AI system

The definition of the AI system in Article 3(1) AI Act can be understood to include the above mentioned main elements. The key purpose of the definition of an AI system is to provide characteristics that distinguish AI systems from ‘simpler traditional software systems or programming approaches’. A key distinguishing characteristic of an AI system is its capability to infer, from the input it receives how to generate outputs. This capability of inference, covers both the process of obtaining output in the post-deployment phase of an AI system as well as the capability of an AI system to derive models or algorithms or both from inputs or data at the pre-deployment phase. Other characteristics of an AI system definition such as the system’s level of autonomy, type of objectives, and degree of adaptiveness, help to define main elements of the AI system as well as to provide clarity on the nature of the AI system but are not decisive for distinguishing between AI systems and other type of software systems. In particular, AI systems that are built on one of the AI techniques but remain static after deployment triggered questions related to the scope of the AI Act, understanding of the concept of inference and the interplay between the different characteristics of the AI system definition. The guidelines are expected to provide explanation on the main elements of the AI system definition.

1.1: Based on Article 3(1) and Recital 12 AI Act, what elements of the definition of an AI system, in particular, require further clarification in addition to the guidance already provided in Recital 12?

Elements of an AI system - please rate the importance of further clarification from 1 to 10, 10 indicating 'most important':

'a machine based system'

Only values between 1 and 10 are allowed

5

'designed to operate with varying levels of autonomy'

Only values between 1 and 10 are allowed

10

'may exhibit adaptiveness after deployment'

Only values between 1 and 10 are allowed

10

'for explicit or implicit objectives'

Only values between 1 and 10 are allowed

10

'infers, from the input it receives, how to generate outputs'

Only values between 1 and 10 are allowed

5

'predictions, content, recommendations, or decisions'

Only values between 1 and 10 are allowed

8

'can influence physical or virtual environments'

Only values between 1 and 10 are allowed

5

Explain why one or more of these elements require further clarification and what part of this element needs further practical guidance for application in real world applications?

1500 character(s) maximum

Definition risks being overly narrow or overly broad.
"levels of autonomy" requires precise categorization without falling into a purely quantitative definition.
Autonomy can be more effectively understood through a categorization that distinguishes between assisted intelligence, augmented intelligence, automated intelligence, and autonomous intelligence (human-in-the-loop, to those with a human-in-command, to those with human-out-of-the-loop interactions)
This approach allows for the identification of the points in the system's operational chain where autonomy is exerted and the potential human interventions and their impact on autonomy. Moreover, autonomy can be a risk factor by itself.
Adaptiveness should differentiate between minor updates and fundamental changes post-deployment.
We believe that "implicit objectives" complicates the definition because, ultimately, the AI system should be evaluated based on its effects. Thus, it is important to distinguish between the effects and implicit objectives.
Expanding the restrictive list of "outputs" to an open-ended form, such as "in particular," ensures adaptability for future developments.
Clarifying direct and indirect impacts under "influences physical or virtual environments" will help to assess integration into broader systems. Introducing this distinction aligns withRecital 12 and the EU Directive on liability for defective products.
These clarifications reduce definitional complexity.

Question 2: Simple software systems out of scope of the definition of an AI system

The AI Act does not apply to all software systems but only to systems defined as 'AI systems' in accordance with Article 3(1) AI Act. According to recital 12, the notion of AI system should be distinguished from 'simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations'. In particular the use of statistical methods, such as logistic regression, triggered questions related to the conditions under which certain software systems should be considered out of the scope of AI system definition. The Commission guidelines are expected to provide methodology for distinguishing AI systems from simpler traditional software systems or programming approaches and thus would help define systems that are outside the scope of the AI Act.

Please provide examples of software systems or programming approaches that **does not fall** under the scope of the AI system definition in Article 3(1) AI Act and explain why, in your opinion, the examples are not covered by one or more of the seven main elements of the definition of an AI system in Article 3(1) AI Act.

1500 character(s) maximum

Rule-based systems (if-then logic): Operate on human-defined rules without statistical methods, adaptability, or inference. Examples include tax calculators, fault diagnosis tools using decision trees, or simple chatbots with predefined responses.
Spreadsheet functions: Perform deterministic operations like calculations or comparisons, lacking autonomy, adaptability, or inference beyond predefined formulas.
Fixed statistical models (linear or logistic regression): Use techniques like linear regression but remain static after training, unable to adapt or infer beyond the training stage.
Automated scripts (shell or batch scripts): Pre-programmed tasks, like backups or factory automation, lack decision-making, predictions, or adaptive responses to input changes. For instance, the automation of daily backups in a company, automating production lines in a factory, or automated reporting systems.
Search algorithms (Dijkstra): Solve problems like optimization deterministically, without inference, adaptation, or autonomous improvement.
However, these systems can be integrated into systems that meet the definition of AI systems.

Section 2. Questions in relation to the prohibitions (Article 5 AI Act)

Article 5 AI Act prohibits the placing on the EU market, putting into service, or the use of certain AI systems that can be misused and provide novel and powerful tools for manipulative, exploitative, social control and/or surveillance

practices.

The Commission guidelines are expected to include an introductory section explaining the general interplay of the prohibitions with other Union legal acts, the high-risk category and general-purpose AI systems as well as relevant specifications of some horizontal concepts such as provider and deployer of AI systems, 'placement on the market', 'putting into service' and 'use' and relevant exceptions and exclusions from the scope of the AI Act (e.g. research, testing and development; military, defense and national security, personal non-professional activity).

Pursuant to Article 5(1) AI Act, the following practices are prohibited in relation to AI systems:

Article 5(1)(a) – Harmful subliminal, manipulative and deceptive techniques

Article 5(1)(b) – Harmful exploitation of vulnerabilities

Article 5(1)(c) – Unacceptable social scoring

Article 5(1)(d) – Individual crime risk assessment and prediction (with some exceptions)

Article 5(1)(e) – Untargeted scraping of internet or CCTV material to develop or expand facial recognition databases

Article 5(1)(f) – Emotion recognition in the areas of workplace and education (with some exceptions)

Article 5(1)(g) – Biometric categorisation to infer certain sensitive categories (with some exceptions)

Article 5(1)(h) – Real-time remote biometric identification (RBI) in publicly accessible spaces for law enforcement purposes (with some exceptions)

This section includes questions on each of the aforementioned prohibitions separately and one final question pertaining to all prohibitions alike and the interplay with other acts of Union law.

A. Questions in relation to harmful subliminal, manipulative or deceptive practices

The prohibition under Article 5(1)(a) AI Act targets AI systems that deploy subliminal techniques, purposefully manipulative or deceptive techniques that materially influence behaviour of people or aim to do so in significantly harmful ways. The underlying rationale of this prohibition is to protect individual autonomy and well-being from manipulative, deceptive and exploitative AI practices that can subvert and impair individuals' autonomy, decision-making, and free choice.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(a) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition*
    - *AI systems deploying subliminal, purposefully manipulative and deceptive techniques*
    - *with the objective or the effect of materially distorting behaviour*
    - *in a manner (reasonably likely to) cause significant harm*
- *AI systems out of scope of the prohibition*
- *Interplay with other Union law (e.g. data protection, consumer protection, digital services regulation, criminal law)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(a) AI Act to apply:*

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putting into service'** (Article 3(11) AI Act), or **'use'** of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

*2) The AI system must 'deploy **subliminal techniques** beyond a person's consciousness (e.g. deploying imperceptible images or audio sounds), **purposefully manipulative** (e.g. exploiting cognitive biases, emotional or other manipulative techniques) or **deceptive techniques**' (e.g. presenting false and misleading information to deceive individuals and influence their decisions in a manner that undermines their free choices). These techniques are alternative, but they can also apply in combination.*

*3) The techniques deployed by the AI system should have the **objective or the effect of materially distorting the behaviour of a person or a group of persons**. The distortion must **appreciably impair their ability to make an informed decision, resulting in a decision that the person or the group of persons would not have otherwise made.** This requires a substantial impact whereby the technique deployed by the AI system does not merely influence a person's (or group of persons) decision, but should be capable of effectively undermining their individual autonomy and ability to make an informed and independent free choice. This suggests that 'material distortion' involves a degree of coercion, manipulation or deception that goes beyond lawful persuasion that falls outside the ban.*

*4) The distorted behaviour must **cause or be reasonably likely to cause significant harm** to that person, another person, or a group of persons. In this context, important concepts that will be examined in the guidelines are the types of harms covered, the threshold of significance of the harm and its reasonable likelihood from the perspective of the provider and/or the deployer. 'Significant*

harms' implies sufficiently important adverse impacts on physical, psychological health or financial interests of persons and groups of persons that can be compound with broader group and societal harms. The determination of 'significant harm' is fact and context specific, necessitating careful consideration of each case's individual circumstances.

For the prohibition to apply, all elements must be in place and there must be a causal link between the techniques deployed, the material distortion of the behaviour of the person and the significant harm that has resulted or is reasonably likely to result from that behaviour.

Question 3: Taking into account the provisions of the AI Act, what elements of the prohibition of harmful manipulation and deception do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- [ ] *placement on the market, putting into service or use of an AI system*
- [x] *deploying subliminal, purposefully manipulative or deceptive techniques*
- [x] *with the objective or the effect of materially distorting behaviour of a person or groups of persons*
- [x] *in a manner that causes or is reasonably likely to cause significant harm*
- [ ] *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

Placement, Use, or Service of AI Systems :
- Clarify distinctions between "placed on the market," "put into service," and "used" for AI systems.
- Detail the obligations of providers versus deployers in each phase.
- Address cross-border or globally available AI systems.

Subliminal, Manipulative, or Deceptive Techniques :
- Define and give examples of "subliminal," "manipulative," and "deceptive" techniques.
- Explain how combinations of these techniques are assessed under the prohibition.

Materially Distorting Behavior of Individuals or Groups
- Clarify how intentionality (objective) and unintentional outcomes (effect) are weighed.
- Specify how impacts on diverse or loosely defined groups are assessed.
- Define contours of collective harm and explore collective means of action.

Significant Harm and Reasonable Likelihood
- Define "significant harm" with thresholds or examples.

- Clarify "reasonable likelihood" and evidentiary standards for manipulation or harm.
- Specify proof burdens, considering collective/individual harm and opacity of systems.
- Explore presumptions of causality when victims lack proof, aligning with the EU Directive on defective products.

Question 4: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- (●) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

Catbox, an emotional companionship app launched in China, aligns with these prohibitions. Although this specific app has not appeared in the European app market, similar apps are already available for download from the Apple/Google app stores, and some even support English gameplay.

Question 5: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- (●) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

Content recommendation AI systems, used by platforms, especially Very Large Platforms under the Digital Services Act, manage vast content while capturing user attention. Using techniques like collaborative filtering, neural networks, or reinforcement learning, they may meet Article 5's prohibition criteria:

Manipulative/Deceptive Techniques: Algorithms exploit biases or emotions to manipulate decisions (e.g., misleading users with false information). They can also manipulate the information itself.

Behaviour Distortion: They shape what users see, read, or buy, significantly influencing behavior and potentially undermining informed decisions, even if users are aware of criteria per section 26 of the Digital Services Act.

Substantial Prejudice: They threaten freedom of information, fostering "echo chambers" or "filter bubbles," harming, for instance, mental health (e.g., TikTok's role in cases of suicide/mutilation), or encouraging compulsive purchases.

Despite this, recommendation algorithms can be virtuous and only "potentially" harmful. They cannot therefore systematically fall under the prohibition. It may be necessary to clarify that to meet the prohibition,

a system must consistently fulfill all its criteria. This aligns with a well-known distinction in competition law between appearance and evidence.

B. Questions in relation to harmful exploitation of vulnerabilities

The prohibition under Article 5(1)(b) AI Act targets AI systems that exploit vulnerabilities of certain persons or groups of persons that materially influence behaviour of people or aim to do so in a significantly harmful way. The underlying rationale of the prohibition is to protect individual autonomy and well-being from exploitative AI practices that can subvert and impair individuals' autonomy, decision-making, and free choice similar. This prohibition in particular aims to protect those that are most vulnerable and susceptible to manipulation and exploitation because of their specific characteristics that make them particularly vulnerable due to their age, disability and or specific socio-economic situation.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(b) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition*
    - *AI system exploiting vulnerabilities due to age, disability or specific socio-economic situation*
    - *with the objective or the effect of materially distorting behaviour*
    - *in a manner (reasonably likely to) cause significant harm*
- *Interplay between the prohibitions in Article 5(1)(a) and (b) AI Act, with the latter acting as lex specialis in case of overlap*
- *AI systems out of scope of the prohibition*
- *Interplay with other Union law (e.g. data protection, non-discrimination law, digital services regulation, criminal law)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the*

prohibition in Article 5(1)(b) AI Act to apply:

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putting into service'** (Article 3(11) AI Act), or **'use'** of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

*2) The AI system must exploit **vulnerabilities due to age** (covering both children as well as elderly), **disability** (as defined in EU equality law encompassing a wide range of physical, mental, intellectual and sensory impairments that hinder full participation of individuals in the society), or **specific socio-economic situations** (e.g. persons living in extreme poverty, ethnic or religious minorities). Vulnerabilities of these persons should be understood to encompass a broad spectrum of categories, including cognitive, emotional, physical and other forms of susceptibility that can affect the ability of an individual or a group of persons pertaining to those groups to make informed decisions or otherwise influence their behaviour. 'Exploitation' should be understood as objectively making use of such vulnerabilities in a manner which is harmful for the exploited vulnerable (groups of) persons and/or other persons.*

*3. The techniques deployed by the AI system should have the **objective or the effect of materially distorting the behaviour** of a person or a group of persons. Article 5(1)(a) and (b) AI Act make use of the same concept and should therefore be interpreted in the same way to the extent they overlap.*

*4. The distorted behaviour must **cause or be reasonably likely to cause significant harm** to that person, another person, or a group of persons. Article 5 (1)(a) and (b) AI Act make use of the same concept and should therefore be interpreted in the same way, while taking into account that the harms that can be suffered by vulnerable groups can be particularly severe and multifaceted due to their heightened susceptibility to exploitation.*

For the prohibition to apply, all elements must be in place and there must be a causal link between the vulnerability exploitation by the AI system, the material

distortion of the behaviour of the person and the significant harm that has resulted or is reasonably likely to result from that behaviour.

Question 6: Taking into account the provisions of the AI Act, what elements of the prohibition of harmful exploitation of vulnerabilities do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- [ ] *placement on the market, putting into service or use of an AI system*
- [x] *exploiting vulnerabilities due to age, disability or specific socio-economic situation*
- [x] *with the objective or the effect of materially distorting behaviour of a person or groups of persons*
- [x] *in a manner that causes or is reasonably likely to cause significant harm*
- [ ] *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

The European Commission must clarify several aspects of Article 5(1)(b) of the AI Act to ensure effective enforcement. First, the definition of vulnerabilities (age, disability, socio-economic situations) requires concrete examples and clear criteria, particularly for cognitive, emotional, or physical vulnerabilities. However, we believe that quantifiable measures of vulnerability through thresholds would not be appropriate, as they risk excluding specific vulnerabilities. It should also be clarified whether vulnerabilities can be cumulative and, if so, whether their combination constitutes an aggravating factor.
The notion of "exploitation" requires further refinement: does it require intent, or can unintentional exploitation also fall under the prohibition? Additionally, the "objective or the effect" of exploitation implies a reasoning based on either purpose or consequence. However, lessons from competition law reveal that these concepts are particularly difficult to interpret and apply, even in jurisprudence.
The causal link between exploitation, distortion, and significant harm remains vague and demands clearer standards of evidence. Finally, these concepts must be harmonized with the GDPR and DSA to avoid regulatory contradictions.

Question 7: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- (•) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

Video games incorporating dependency mechanisms, such as loot boxes, include titles like Electronic Arts' FIFA Ultimate Team, which utilizes AI-driven loot box systems.

These systems are likely to meet the criteria for prohibition:

Psychological exploitation of vulnerable audiences: They exploit psychological vulnerabilities through reward-optimization algorithms designed to foster dependency, particularly in children and adolescents.
Distortion of spending behavior: These mechanisms encourage compulsive purchasing habits.
Harm caused: They result in significant financial losses and negatively impact mental health, including the development of addictive behaviors.

Question 8: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

As hinted to in our response to question 5, it should be clarified that AI systems which are designed to protect and support people identified as vulnerable due to specific socio-economic circumstances, age or disability, should not fall under the prohibited practices. These systems which intervene for instance regarding consumer debt restructuring, overdrafts and card limits, should be seen as instruments to a tailor-made offer to vulnerable populations.
Although banking scoring is not part of prohibited practices per se, it may be useful to highlight the interplay with the GDPR (in particular Article 22) and its safeguards (e.g., consent, fair and transparent treatment, human intervention, right of deletion in case of illicit treatment). This would help attracting the attention to the necessity, in line with the Court rulings (e.g., CJUE Case C-634/21, German Federal Court Case Schufa), to prepare for the assessment of such systems before entering the market and along their life-cycle (based on the principles of transparency, consent, and data usage and accuracy). The understandable concern regarding the potential disruption of ongoing credit banking scoring systems may be dealt with a clarified definition of software system as suggested in our response to Q2.

C. Questions in relation to unacceptable social scoring practices

The prohibition under Article 5(1)(c) AI Act aims to prevent 'social scoring' practices that evaluate persons over a certain period of time based on their social behaviour or personal characteristics leading to detrimental and unfair outcomes for certain individuals and groups. The prohibition applies in principle to both the public and the private sector. The underlying rationale of this

prohibition is to prevent such unacceptable 'social scoring' practices that may lead to discriminatory and unfair outcomes for certain individuals and groups, including their exclusion from society. The prohibition of 'social scoring' aims to protect in particular the right to human dignity and other fundamental rights, including the right to non-discrimination and equality, to data protection and to private and family life. It also aims to safeguard and promote the European values of democracy, equality and justice.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(c) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition*
    - *'Social scoring': evaluation or classification based on social behaviour or personal or personality characteristics over a certain period of time*
    - *Whether provided or used by public or private entities*
    - *Leading to detrimental or unfavourable treatment in unrelated social contexts and/or unjustified or disproportionate treatment*
- *AI systems out of scope of the prohibition*
- *Interplay with other Union law (e.g. data protection, non-discrimination)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(c) AI Act to apply:*

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putting into service'** (Article 3(11) AI Act), or **'use'** of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

*2) The AI systems must be intended or used for the **evaluation or classification** of natural persons or groups of persons over a certain period of time based on: (i)their **social behaviour**; or*

*(ii) known, inferred or predicted personal or personality **characteristics**;*

*3) The social score created with the assistance of the AI system must lead to the **detrimental or unfavourable treatment** in one or more of the following scenarios:*
(i) in social contexts unrelated to those in which the data was originally generated or collected; and/or
(ii)treatment that is unjustified or disproportionate to their social behaviour or its gravity.

The detrimental or unfavourable treatment must be the consequence of the score, and the score the cause of the treatment. It is not necessary for the evaluation performed by the AI system to be 'solely' leading to the detrimental or unfavourable treatment (covering thus AI-enabled scoring practices that may be also subject to or combined with other human assessments). At the same time, the AI output has to play a sufficiently important role in the formation of the social score. For the prohibition to apply all elements described above must be in place at the same time.

Question 9: Taking into account the provisions of the AI Act, what elements of the prohibition of social scoring do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- ☐ *placement on the market, putting into service or use of an AI system*
- ☑ *for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour, or known, inferred or predicted personal or personality characteristics*
- ☑ *with the social score leading to the detrimental or unfavourable treatment of the person or groups of persons*
- ☑ *in social contexts unrelated to those in which the data was originally generated or collected*
- ☑ *treatment that is unjustified or disproportionate to their social behaviour or its gravity*
- ☐ *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

As already emphasize, the current wording of the AI Act could allow practices and systems that facilitate the spread of AI-based social scoring across the EU (Human Rights Watched, EU: Artificial Intelligence Regulation Should Ban Social Scoring
Strong Social Scoring Ban Needed to Protect Rights, October 9, 2023, https://www.hrw.org/news/2023/10/09/eu-artificial-intelligence-regulation-should-ban-social-scoring).

The elements of the AI Act concerning the prohibition of social scoring must be clarified to ensure a strong ban of social scoring. In this regard, it appears important to specify with concrete examples:
the difference between classification and evaluation of natural persons and groups of persons;
the application to the ban of social scoring for moral persons in the notion “groups of persons”;
the determination of the notion “certain period of time”;
the distinction, limits and clarification of what could be known, inferred or predicted on the personal or personality characteristics of citizens;
the definition of the notion of social behavior which is not a legal-known notion;
the notion and limit of what are “social contexts unrelated to those in which the data was originally generated or collected” and the fact that they are limited or not to public services;
the difference of an unjustified or disproportionate treatment to a social behavior;
the difference of an unjustified or disproportionate treatment to its gravity.

Question 10: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- (●) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

As observed by Human Rights Watch, La Quadrature Du Net and EDRi “investigations in France, the Netherlands, Austria, Poland and Ireland have revealed that AI-based social scoring systems are disrupting people’s access to social security support, compromising their privacy, and profiling them in discriminatory ways and based on stereotypes about poverty”.

More especially in France, it has been revealed that the CAF (Caisse aux Affaires Familiales) uses algorithms to predict which beneficiaries would be “(un)worthy” of trust and must be controlled. The algorithms are responsible for giving a score to each recipient, supposed to represent the “risk” that they benefit from unduly excessive social assistance. This note, updated monthly, is then used by the CAF teams of controllers to select those requiring in-depth control.

Question 11: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- (●)

Yes

No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

The guidelines of the Commission must specify that AI systems used to determine and allocate public assistance benefits and services that draw on a wide range of personal and sensitive data to assess whether beneficiaries are a fraud “risk” must be banned as an unacceptable risk and not as a high risk system.

If a bank uses AI to develop a scoring system that categorizes customers based on their social behavior or personal characteristics (as floated in the UK and emerging jurisdictions), this could be considered as a prohibited practice, especially if it influences creditworthiness. However, such recourse to social scoring may be acceptable in case it would enable consumers to have a wider and more personalized access to services. This would imply though that all the safeguards are in place, namely i) no discriminatory and unfair outcome; ii) respect of fundamental rights; iii) respect of data protection rules; iv) transparency and explainability of the outputs.

Individual scoring for ecological purposes must also be questioned. The principle of a carbon account (“Compte carbone individuel”), which is an annual quota of greenhouse gas emissions (accounted for in CO2 equivalent according to an international protocol), adjustable and decreasing, which each citizen would have equal access to, must be analyzed as a social scoring prohibited.

D. Questions in relation to individual crime risk assessment and prediction

The prohibition under Article 5(1)(d) AI Act targets AI systems assessing or predicting the risk of a natural person committing a criminal offence solely based on profiling or assessing personality traits and characteristics, without objective and verifiable facts directly linked to criminal activity and a human assessment thereof. The underlying rationale for the ban is to prevent unacceptable law enforcement practices where AI is used to make an individual a suspect solely based on profiling or their personality traits and characteristics rather than as support of human assessment, which is already based on objective and verifiable facts directly linked to a criminal activity. Such 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. They also endanger individual’s liberty without the necessary procedural and judicial safeguards and violate the right to be presumed innocent. Other fundamental rights at risk that the ban aims to safeguard are the right to human dignity, non-discrimination, the right to fair trial,

the right to defence, effective remedy, privacy and data protection and the rights of the child if these practices affect children.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(d) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition*
    - *Individual crime prediction of a natural person committing a criminal offence*
    - *solely based on profiling or the assessment of personality traits and characteristics*
    - *without verifiable facts directly linked to criminal activity and human assessment thereof*
- *Interplay with other Union law (e.g. data protection)*
- *AI systems that are out of the scope of the prohibition (e.g. support of the human assessment)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(d) AI Act to apply:*

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putting into service for this specific purpose'** (Article 3(11) AI Act), or **'use'** of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

*2) The AI system must be intended or used for the specific purpose **of making a risk assessment or prediction of a natural person or persons committing a criminal offence**. The individual crime predictions can be made at any stage of the law enforcement activities such as prevention and detection of crimes, but also investigation, prosecution and execution of criminal penalties. Excluded from the scope are therefore location- and event-based predictions and*

individual predictions of administrative offences since these are not assessing the risk of individuals ***committing a criminal offence****.*

3) The assessment or the prediction must be ***solely*** *based on either or both of the following:*
*(i)****profiling*** *of a natural person (defined in Article 4(4) of the General Data Protection Regulation as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person), or*
*(ii)****assessing a person's personality traits and characteristics*** *(such as nationality, place of birth, place of residence, number of children, level of debt or type of car)*

4) Excluded are ***AI systems used to support human assessment based on objective and verifiable facts directly linked to a criminal activity****. This means that predictive AI tools could be used for supporting the human assessment of the involvement of a person in the criminal activity if there are objective and verifiable facts linked to a criminal activity on the basis of which a person can be reasonably suspected of being involved in a criminal activity.*

Question 12: Taking into account the provisions of the AI Act, what elements of the prohibition of harmful manipulation and deception do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- ☐ *placement on the market, putting into service or use of an AI system*
- ☑ *for making risk assessment or prediction of a natural person or persons committing a criminal offence*
- ☑ *solely based on the profiling of a natural person or their traits and characteristics*
- ☑ *excluded are AI systems used to support human assessment based on objective and verifiable facts directly linked to a criminal activity*
- ☐ *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

It is important to underline it is already affirmed that the current article 5(1)(d) could “reduce the ban on predictive policing to a symbolic gesture rather than a substantial protection of fundamental rights” (Levano Jessie,“Predictive Policing in the AI Act: Meaningful Ban or Paper Tiger?” European Law Blog, 2024 : https://doi.org/10.21428/9885764c.6d0aa28c) .

All of the elements of the prohibition of individual crime risk assessment and prediction must be clarified more especially with attention for natural persons who are already marginalised, for example minority communities and individuals from non-Western backgrounds and with a nuanced approach to national security exceptions.

Priorities questions that must be clarified are the following. What is a risk assessment or prediction related to a criminal offence? Which traits and characteristics would be admissible? What type of AI systems are excluded because they aim to support human assessment based on objective and objective and verifiable facts directly linked to a criminal activity? What is the difference and limitation between the notions? What constitutes or not objective and verifiable facts? What is the sense of the wording “which is already based on” considering the fact that there are differing standards in criminal law and scientific validity.

Question 13: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- Yes
- No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

Since a decade, the use of predictive police using AI systems has been well documented by many authors, institutions and NGOs. For example, in France, we can mention :
PAVED, a software developed from 2017 by the Gendarmerie and trialed from 2018 before being paused in 2019 in various departments to assess the risk of car thefts or burglaries.
M-Pulse, previously named Big Data of Public Tranquility, developed by the city of Marseille in partnership with the company Engie Solutions originally created to assess the suitability of municipal police deployments in urban public space, it seems to be actually used for predict the population density in the streets depending on the time.
Smart Police, an application that includes a “predictive” module and that is developed by French startup Edicia which, according to its website, is used by 350 cities to improve “the peace and security of their citizens with our solutions”.
Analyst's Notebook (ANB1) is a software for analyzing data used by the Central Criminal Intelligence Service under the name ANACRIM2.

Furthermore, in November 2023, the media Disclose revealed that the French police would be equipped with Israeli software Briefcam, which contains facial recognition functionality. This has even been activated by default on the software since 2018. According to Disclose, the Briefcam software equips the municipal police in nearly 200 municipalities.

Question 14: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

Question 15: Do you have or know concrete examples of AI systems that fulfil all necessary criteria for the prohibition to apply, but fall under the exception of systems that support the human assessment of the involvement of a person in a criminal activity, based on objective and verifiable facts linked to a criminal activity?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice and which exception would apply and why

1500 character(s) maximum

E. Questions in relation to untargeted scraping of facial images

Article 5(1)(e) AI Act prohibits AI systems with the specific purpose of creating or expanding facial recognition databases through untargeted scraping of the internet or CCTV footage.

As to the rationale of the prohibition, untargeted scraping of a large number of facial images from the Internet or CCTV material, along with associated metadata and information, without consent of the data subject(s), to create large-scale facial databases, violates individuals' rights and individuals lose the possibility to be anonymous. Recital 43 of the AI Act justifies the prohibition of Article 5(1)(e) AI Act based on the 'feeling of mass surveillance' and the risks of 'gross violations of fundamental rights, including the right to privacy'.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(e) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition*
  - *Facial recognition databases*
  - *through untargeted scraping of facial images*
  - *from the internet or CCTV footage*
- *AI systems out of scope of the prohibition*
- *Interplay with other Union law (e.g. data protection)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(e) AI Act to apply:*

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putting into service for this specific purpose'** (Article 3(11) AI Act), or **'use'** of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

*2) The AI system must be intended or used for the specific purpose of untargeted scraping. The prohibition applies to **scraping AI systems** that are placed on the market or being put into service 'for this specific purpose' of **untargeted scraping of the internet/CCTV** material. This implies that the prohibition does not apply to all scraping tools with which one can build up a database, but only to tools for untargeted scraping.*

*3) The prohibition covers AI system used to **create or expand facial recognition databases**. Database in this context refers to any collection of data, or information, that is specially organized for rapid search and retrieval by a computer. A facial recognition database is a technology that matches a human face from a digital image or video frame against a database of faces, compares it to the database and determines whether there is a match in the database.*

*4) The sources of the images are either the **Internet or CCTV footage**.*

Question 16: Taking into account the provisions of the AI Act, what elements of the prohibition of untargeted scraping of facial images do you think require further clarification in the guidelines?

Please select all relevant options from the list

- [x] *placement on the market, putting into service or use of an AI system*
- [x] *for creating or expanding facial recognition databases*
- [x] *through untargeted scraping of facial images*
- [x] *from the internet or CCTV footage*
- [ ] *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the guidelines?

1500 character(s) maximum

1) Placement on the market, putting into service, or use of an AI system
- Placement on the market: Does this include only commercial sales or also free distribution and open-source access?
- Putting into service: Does it cover system integration into existing infrastructures (e.g., surveillance systems)?
- Use: Does it encompass internal usage for database development or only final applications?

2) Creating or expanding facial recognition databases
- Clarify the difference between "creation" or "expansion". For example, does adding a single image to an existing database suffice to trigger this prohibition?
- clarify the scope of the "databases" covered: only those for commercial purposes, or also those for research, security, or educational use?

3) Untargeted collection of facial images
The concept of "untargeted collection" remains ambiguous. Does it only include automated processes (e.g., bots collecting images on the internet) or also manual large-scale collections?
Guidelines should precise the criteria distinguish targeted collection (images of a specific individual with consent) from untargeted collection?

4) Internet or CCTV images:
- Clarify the perimeter of Internet : does this include social networks, public forums, or only unrestricted websites?
- Regarding CCTV images, guidelines should detail under what circumstances and purposes the use of these images is prohibited.

Question 17: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

Question 18: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

F. Questions in relation to emotion recognition

Article 5(1)(f) AI Act prohibits AI systems to infer emotions in the areas of workplace and education institutions except for medical or safety reasons.

As to the rationale of the prohibition, emotion recognition technology is quickly evolving and comprises different technologies and processing operations to detect, collect, analyse, categorise, re- and interact and learn emotions from persons. Emotion recognition can be used in multiple areas and domains for a wide range of applications, such as for analysing customer behaviour, targeted advertising, in the entertainment industry, in medicine and healthcare, in education, employment, wellbeing, or for law enforcement and public safety.

Emotion recognition can lead to 'discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons', in particular the right to privacy. It is therefore in principle prohibited in asymmetric relationships in the context of workplace and education institutions, where both workers and

students are in particularly vulnerable positions. The AI Act states in Recital 44 that there are 'serious concerns about the scientific basis of AI systems aiming to identify or infer emotions, particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such systems are the limited reliability, the lack of specificity and the limited generalisability.' At the same time, emotion recognition in specific use contexts, such as for safety and medical care (e.g. health treatment and diagnosis) has benefits and is therefore not prohibited. In such cases, emotion recognition is classified as a high-risk AI system and subjected to requirements aimed to ensure accuracy, reliability and safety.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(f) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition*
    - *AI systems to infer emotions*
    - *Identification and inference of emotions*
    - *Emotions*
    - *On the basis of their biometric data*
- *Limitation of the prohibition to workplace and educational institutions*
    - *Workplace*
    - *Educational institutions*
- *Exceptions for medical and safety reasons*
- *More favourable Member State law*
- *AI systems out of scope of the prohibition*
- *Interplay with other Union law (e.g. data protection)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(f) AI Act to apply:*

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putt***

ing into service for this specific purpose' *(Article 3(11) AI Act), or* ***'use'*** *of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

2) AI systems to infer emotions, as defined in the light of Article 3(39) AI Act, are systems for ***identifying or inferring emotions or intentions of natural persons on the basis of their biometric data****. 'Identification' occurs when the processing of the biometric data (for example, of the voice or a facial expression) allows to directly compare and identify with an emotion that has been previously programmed in the emotion recognition system. 'Inferring' is done by deducing information generated by analytical and other processes by the system itself. In this case, the information about the emotion is not solely based on data collected on the natural person, but it is concluded from other data, including machine learning approaches that learn from data how to detect emotions. Emotions have to be defined in a broad sense, but do not include physical states such as pain or fatigue and readily apparent expressions such as smiles.*

*3) The prohibition in Article 5(1)(f) AI Act is limited to emotion recognition systems in the '****areas of workplace and educational institutions****', because there is a power imbalance, an asymmetric relation and a risk of continuous surveillance.*

4) The prohibition contains an explicit exception for emotion recognition systems used in the areas of the workplace and educational institutions ***for medical or safety reasons****, such as systems for therapeutical use.*

Question 19: Taking into account the provisions of the AI Act, what elements of the prohibition of emotion recognition in the areas of workplace and education do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- ☐ *placement on the market, putting into service or use of an AI system*
- ☑ *for identifying or inferring emotions of natural persons*
- ☑ *in the area of workplace and educational institutions*
- ☑ *except for medical and safety reasons*
- ☐ *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

Compliance with fundamental rights, particularly respect for French national labor law, is also crucial. Article L1121-1 of the French Labor Code provides that "no one may impose restrictions on individual and collective rights and freedoms unless justified by the nature of the task to be performed and proportionate to the aim pursued." Here, a specific exclusion is provided for "physical exclusion solely for the purpose of accessing a service, unlocking a device, or securing access to premises. This exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights."
It would be prudent to delineate the contours of what constitutes an emotion in particular, as it seems imprecise to limit the concept to primary emotions—happiness, sadness, anger, surprise, disgust, embarrassment (etc.)—while permitting the recognition of physical states.
The boundary between emotional recognition and physical state recognition is narrow, and if not clearly defined and specified through technical criteria, it could significantly impact fundamental rights. Additionally, what are the consequences of monitoring gestures? What happens when biometric data of a sensitive nature is processed? These provisions would benefit from further clarification. (Article 9 of the GDPR on sensitive data, particularly in the medical field, clarification regarding patient consent?)

Question 20: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- (●) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

It seems that the Academy of Toulouse has resources for teachers for a classroom entitled “How can AI help identify the emotional state of students in a class?” in 2022 (https://pedagogie.ac-toulouse.fr/sii /Traam21-22-5eme-IA-Accompagnement-Emotion).

Question 21: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- ( ) Yes
- (●) No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

Question 22: Do you have or know concrete examples of AI systems that fulfil all necessary criteria for the prohibition to apply, but fall under the exception of medical and safety reasons?

- (●) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice and which exception would apply and why

1500 character(s) maximum

A clinical study has been realized by the Parisian start-up MyndBlue, published in the journal “Scientific Reports”. It reveals that some machine learning algorithms could be used to identify a biosignature to provide a clinical score of depressive symptoms using individual physiological data (Source : Ricka, N., Pellegrin, G., Fompeyrine, D.A. et al. Predictive biosignature of major depressive disorder derived from physiological measurements of outpatients using machine learning. Sci Rep 13, 6332 (2023), https://doi.org /10.1038/s41598-023-33359-w). Furthermore, some robots developed by french companies (Nao, Leka, Buddy) could be a help for autistic children in order to learn to recognize emotions.

We also can imagine that recognition of emotions with biometric data could be mobilized with other techniques for preventive or investigation purposes. This application falls into the ban of relation to individual crime risk assessment and the ban of prediction and emotion recognition.

The DL4T authors of this public consultation want to remind that the analysis of emotions is subjective, qualitative and depending on context and is based on cognitive and psychological sciences that don't make unanimity.

G. Questions in relation to biometric categorisation

Article 5(1)(g) AI Act prohibits biometric categorisation systems (as defined in Article 3(40) AI Act) that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. This prohibition does not cover the lawful labelling, filtering or categorisation of biometric data sets acquired in line with Union or national law according to biometric data, which can for example be used in the area of law enforcement (Recital 30 AI Act).

As to the rationale of the prohibition, AI-based biometric categorisation systems for the purpose of assigning natural persons to specific groups or categories relating to aspects such as sexual or political orientation or race violate human

dignity and pose significant risks to other fundamental rights such as privacy and discrimination.
A wide variety of information, including 'sensitive' information can be extracted, deduced or inferred from biometric information, even without the individuals knowing it, to categorise them. This can lead to unfair and discriminatory treatment, for example when a service is denied because somebody is considered to be of a certain race.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(g) AI Act:

- *Rationale and objectives of the prohibition*
- *Main elements of the prohibition:*
  - *Biometric categorisation system*
  - *Persons are individually categorised based on their biometric data*
  - *To deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation*
  - *On the basis of their biometric data*
- *AI systems out of scope of the prohibition*
  - *Labelling and filtering based on biometric data*
- *Interplay with other Union law (e.g. data protection)*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(g) AI Act to apply:*

*1) The activity must constitute **'placing on the market'** (Article 3(9) AI Act), **'putting into service for this specific purpose'** (Article 3(11) AI Act), or **'use'** of an AI system (Article 3(1) AI Act). The prohibition applies to both providers and deployers of AI systems, each within their own responsibilities.*

*2) The AI system must be a **biometric categorisation system** for the purpose*

of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons (Article 3(40) AI Act).

*3) **Individual persons** are categorised,*

*4) Based on their **biometric data** (Article 3(34) AI Act),*

*5) Article 5(1)(g) AI Act prohibits only biometric categorisation systems which have as objective **to deduce or infer a limited number of sensitive characteristics: race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation**.*

*The prohibition does not **cover labelling or filtering of lawfully acquired biometric datasets**, including in the field of law enforcement.*

Question 23: Taking into account the provisions of the AI Act, what elements of the prohibition of biometric categorisation to infer certain sensitive characteristics do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- [ ] *placement on the market, putting into service or use of an AI system*
- [x] *that is a biometric categorisation system individually categorising natural persons based on their biometric data*
- [x] *to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation*
- [x] *excluded are labelling or filtering of lawfully acquired biometric datasets, including in the field of law enforcement*
- [ ] *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

That is a biometric categorisation system individually categorising natural persons based on their biometric data:
This issue can be illustrated by AML-CFT legislation. Article 3(c) of the french decree of 3 November 2014 on internal control requires the establishment of systems that assess risks and produce results. If AI systems are applied in this domain, they may highlight specific "type" of high-risk profile.
Compliance with Internal Control Requirements
How can sensitive data be categorised in a way that complies with internal control legislation without

violating the prohibition on biometric categorisation ?
What safeguards can ensure that risk assessments are non-discriminatory while still effective?
Exemptions for High-Risk Industries
Are there provisions or exemptions for industries like banking that require robust risk evaluation systems to comply with legal obligations?
How can AI be integrated into such frameworks without introducing artificial constraints that hinder its potential for improving compliance and operational efficiency?
Excluded are labelling or filtering of lawfully acquired biometric datasets including in the field of law enforcement :
Under Article R561-5, the application of AML-CFT legislation requires the collection of sensitive datas, need a clarification: The conditions under which biometric data qualifies as "lawfully acquired" within the scope of AML-CFT or other legal frameworks.

Question 24: Do you have or know concrete examples of AI systems that in your opinion fulfil all elements of the prohibition described above?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice and how all the necessary elements described above are fulfilled

1500 character(s) maximum

Question 25: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- ◉ Yes
- ○ No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

AI systems used by firms operating within the scope of AML-CFT legislation represent a key area where further clarification is needed. For instance, systems such as those implemented by the ACPR (Bank of France) to assess the compliance of regulated entities with AML-CFT requirements. These systems leverage AI to enhance the evaluation and monitoring processes, but it remains unclear whether such applications fall within the scope of the prohibition outlined in Article 5(1)(g) AI Act.

Question 26: Do you have or know concrete examples of AI systems that fulfil all necessary criteria for the prohibition to apply, but fall under the exception of labelling or filtering of lawfully acquired biometric datasets?

- ○

Yes

No

Please specify the concrete AI system, how it is used in practice and which exception would apply and why

1500 character(s) maximum

H. Questions in relation to real-time remote biometric identification

Article 5(1)(h) AI Act contains a prohibition on real-time use of remote biometric identification systems (Article 3(41) and (42) AI Act) in publicly accessible spaces for law enforcement purposes subject to limited exceptions exhaustively and narrowly defined in the AI Act.

Recital 32 AI Act acknowledges 'the intrusive nature of remote biometric identification systems (RBIS) to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities.'

At European level, RBIS are already regulated by EU data protection rules, as they process personal and biometric data for their functioning.

Due to the serious interferences that real-time RBI use for the purpose of law enforcement poses to fundamental rights, its deployment is, in principle, prohibited under the AI Act. However, as most of these fundamental rights are

not absolute, objectives of general interest, such as public security, can justify restrictions on exercising these rights as provided by Article 52(1) of the Charter. Any limitation must comply with the requirements of legality, necessity, proportionality and respect for the essence of fundamental rights. Therefore, when the use is strictly necessary to achieve a substantial public interest and when the exceptions are exhaustively listed and narrowly defined, their use outweighs the risks to fundamental rights (Recital 33 AI Act). To ensure that these systems are used in a 'responsible and proportionate manner', their use can only be made if they fall under one of the explicit exceptions defined in Article 5(1)(i) to (iii) AI Act and subject to safeguards and specific obligations and requirements, which are detailed in Article 5(2)-(7) AI Act. When the use falls under one or more of the exceptions, the remote biometric identification system is classified as a high-risk AI system and subject to requirements aimed to ensure accuracy, reliability and safety.

Proposed structure of the guidelines

It is proposed that the Commission guidelines would cover the following aspects regarding Article 5(1)(h) AI Act:

- *Rationale and objectives of the prohibition*
- *Definition of*
  - *remote biometric identification*
  - *'real-time'*
  - *publicly accessible spaces*
  - *law enforcement purposes*
- *AI systems out of scope of the prohibition*
- *Interplay with other Union law*
- *Conditions and safeguards for exceptions*

Main elements of the prohibition

*Several **cumulative elements must be in place** at the same time for the prohibition in Article 5(1)(h) AI Act to apply:*

*1) The activity must constitute **the 'use' of an AI system** (Article 3(1) AI Act),*

so, contrary to the previously mentioned prohibitions, this prohibition applies only to deployers of AI systems.

*2) The AI system must be a **remote biometric identification system** (Article 3 (41) AI Act), i.e. an AI system for the purpose of identifying natural persons, **with out their active involvement**, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database. This **excludes systems for verification or authentication of persons**.*

*3) The system is used in '**real-time**' (Article 3(42) AI Act), i.e. the biometric systems capture and further process biometric data 'instantaneously, near-instantaneously or in any event without any significant delay.*

*4) The AI system is used in **publicly accessible spaces**, i.e. 'any publicly or privately owned physical space accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions'. This excludes online spaces, border control points and prisons.*

*5) The prohibition of Article 5(1)(h) AI Act applies to **law enforcement purposes** , irrespective of the entity, authority, or body carrying out the activities. Law enforcement is defined in Article 3(46) AI Act as the 'activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.' These activities are also those that constitute the subject matters in Article 1 of the Law Enforcement Directive.*

Question 27: Taking into account the provisions of the AI Act, what elements of the prohibition of real-time remote biometric identification for law enforcement purposes do you think require further clarification in the Commission guidelines?

Please select all relevant options from the list

- ☐ *use of an AI system*
- ☐ *that is a remote biometric identification system*
- ☐ *used 'real-time'*
- ☐ *for law enforcement purposes*

- [ ] *in publicly accessible spaces*
- [ ] *none of the above*

Please explain why the elements selected above require further clarification and what needs to be further clarified in the Commission guidelines?

1500 character(s) maximum

As highlighted in the context of AML-CFT compliance, further clarification is needed regarding the verification of customers' identities by banking institutions. This is particularly crucial for addressing fraud in payment systems, where accurate and efficient verification methods are necessary.
For example, under the PSD2 regulation, there is a requirement for "two-factor authentication," which often includes biometric data. However, Article 5(1)(h) AI Act raises ambiguities as it primarily focuses on restricting real-time biometric identification in publicly accessible spaces for law enforcement purposes. This creates uncertainty regarding the use of similar AI tools in private contexts, such as banking, which do not directly fall under law enforcement but are essential for compliance with regulatory frameworks and fraud prevention.
To ensure alignment with the AI Act, the Commission should provide:
Clear exceptions for cases where AI tools are deployed to meet regulatory obligations (e.g., PSD2) or prevent financial fraud.
Guidance on the interplay between public and private applications of biometric data, distinguishing between law enforcement purposes and broader compliance use cases.
Currently, no widely adopted AI system specifically addresses fraud prevention through biometric identification in this manner. Nonetheless, as AI tools develop, it is essential to delineate how they can be used responsibly and effectively without conflicting with the prohibition.

Question 28: Do you have or know concrete examples of AI systems where you need further clarification regarding certain elements of this prohibition to determine whether the AI system is in the scope of the prohibition or not?

- (•) Yes
- ( ) No

Please specify the concrete AI system, how it is used in practice as well as the specific elements you would need further clarification in this regard

1500 character(s) maximum

AI systems used for identity verification to combat fraud should be carefully assessed to determine whether they fall under the scope of the prohibition. For instance, Signicat, a company specializing in helping businesses verify their clients' identities, has highlighted significant concerns about AI-driven fraud in banking institutions.
A study from Signicat (https://www.signicat.com/the-battle-against-ai-driven-identity-fraud) underlined an alarming trends: Fraud attempts have surged by 80% over the past 3 years, with AI-driven schemes becoming a major threat. Deepfakes now account for 6.5% of total fraud attempts, representing a staggering 2137% increase in 3 years. The report underscores the evolving complexity of AI-driven fraud, which goes beyond traditional concerns by enabling highly effective fraud strategies that are difficult to detect and prevent. This includes the use of deepfakes for identity fraud and other malicious purposes.
To address this, further clarification is needed on: Whether identity verification tools employing AI, especially to combat fraud, fall within the prohibition when deployed in non-public contexts. The interplay between

private-sector fraud prevention efforts and the restrictions on real-time biometric identification in publicly accessible spaces for law enforcement purposes.
These clarifications are essential to help financial institutions and fintech companies effectively combat fraud while ensuring compliance with the AI Act.

Article 5(1)(h)(i) to (iii) AI Act provides for three exceptions to the prohibition for:

*(1) The **targeted search** of victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons, i. e. persons whose existence has become uncertain, because he or she has disappeared.*

*(2) The prevention of a **specific, substantial and imminent threat** to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack. A terrorist attack can include a threat to life, whereas a threat to life does not necessarily qualify as a terrorist attack.*

*(3) The **localisation and identification of a person suspected of having committed a criminal offence**, for the purpose of conducting a **criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II** and punishable in the Member States concerned by a custodial sentence or a detention order for a maximum period of at least four years. Annex II of the AI Act provides an exhaustive list of serious crimes for which the real-time use of RBI can be authorised.*

The exceptions have to be authorised by national legislation and comply with certain conditions and safeguards (Article 5(2) to (7) AI Act). These include – among others – temporal, geographic and personal limitations, a duty to perform a fundamental rights impact assessment and to register the system in the EU database (Article 49 AI Act), a need for prior authorisation by a judicial or independent administrative authority, and a notification to the relevant market surveillance authorities and data protection authorities.

Question 29: Do you have or know concrete examples of AI systems that fulfil all necessary criteria for the prohibition to apply, but which could fall under one or more of the exceptions of Article 5(1)(h)(i) to (iii) AI Act?

- ○ Yes
- ◉ No

Please specify the concrete AI system, how it is used in practice and which exception would apply and why

1500 character(s) maximum

Question 30: Do you need further clarification regarding one or more of the exceptions of Article 5(1)(h)(i) to (iii) AI Act or the conditions or safeguards under Article 5(2) to (7) AI Act?

- ○ Yes
- ◉ No

Please specify the concrete condition or safeguard and the issues for you need further clarification; please provide concrete examples

1500 character(s) maximum

I. Question in relation to interplay with other Union legislation

The prohibitions under the AI Act are without prejudice to prohibitions and specific rules provided for in other Union legislation such as data protection, consumer protection, digital services regulation, etc. As explained above, each section of the Commission guidelines are expected to explain relevant interplay of the prohibitions in relation to other Union law.

Question 31: Do you have or know concrete examples of AI systems where you need further clarification regarding the application of one or more of the prohibitions under the AI Act in relation to other Union legislation?

- ○ Yes
- ○ No

Please specify the concrete AI system and the prohibition under the AI Act, the relevant provision of a specific Union legislation and where further clarification is needed

1500 character(s) maximum

As already underlined (J. Sénéchal, “La réglementation, par le droit de la consommation, de la protection de l'humain confronté à l'intelligence artificielle”, Dalloz IP/IT 2024. 564), the regulation of dark patterns is forbidden by GDPR, the article 25 of the DSA and the directive on unfair commercial practices. The article 7 of the DMA imposes obligations on gatekeepers related to dark patterns. The AI Act prohibits dark patterns using AI practices that manipulate individuals below the threshold of consciousness and AI practices that exploit individuals' economic or physical vulnerabilities. The Digital Fairness Act will protect consumers from unfair online practices such as dark patterns. The risk of overlap between the six texts will probably make the prohibition of dark patterns difficult to enforce.

Another practice is publicity using sensible data. Indeed, paragraph 3 of article 26 of the DSA states that “Providers of online platforms shall not present advertisements to recipients of the service based on profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679 (…).” But potentially, all the data and their combinations are sensible. Targeted advertising for minors is also prohibited according to article 28, paragraph 2, of the DSA. In consequence, targeted advertising using AI systems, which could be identified as practices that manipulate individuals and exploit individuals' economic or physical vulnerabilities, need further clarification.

Thank you

Thank you for your interest in participating in the consultation. Please do not forget to click on submit.

Contact

Contact Form