Summary of our response to the european Commission's public consultation on the AI Regulation

December 11, 2024

Respondents: *Marina Teller, Marylou Leroy, Caroline Bérard-Gourisse, Romain Maillot, Alaadin Maraqa, Jingyan Wu, Godefroy de Boiscuille, Mina Ilhan, Mélanie Olivari, Julie Charpenet.*

Through this public consultation, the European Commission seeks to gather opinions and recommendations from various stakeholders (industry representatives, civil society members, academics, etc.) regarding Article 3 of the AI Act, which defines AI systems, and Article 5, which outlines prohibited practices.

Article 3 AI Act – Definition of AI Systems

Regarding the definition of AI, the DL4T team urges the Commission to clarify the degrees of autonomy while cautioning against a purely quantitative definition. Autonomy can be better understood through a classification distinguishing assisted intelligence, augmented intelligence, automated intelligence, and autonomous intelligence (ranging from human-in-the-loop to human-in-command to fully autonomous systems). Furthermore, the DL4T team highlights that autonomy itself can be a risk factor.
We also recommend that the Commission clarify the concept of adaptiveness by differentiating between minor updates and substantial modifications to AI systems after deployment.
Additionally, clarifying direct and indirect impacts under the phrase "which influences physical or virtual environments" would help assess AI integration into broader systems. This distinction aligns with Recital 12 and the EU Directive on liability for defective products.
Finally, the distinction between implicit and explicit objectives complicates the definition, as AI systems will ultimately be assessed based on their effects. We believe it would be more appropriate to distinguish between an AI system's objectives and its outcomes.

Article 5 AI Act – Prohibited Practices

Article 5(1)(a) – Subliminal, Manipulative, and Deceptive Techniques

Regarding the three cumulative conditions, we suggest clarifications on the following points:

- **Placement, Use, or Service of AI Systems:** The distinction between "placed on the market," "put into service," and "used" for AI systems should be clarified, along with the respective obligations of providers and deployers at each phase.
- **Definition and Illustration:** The terms "subliminal," "manipulative," and "deceptive" techniques should be more precisely defined and illustrated. Additionally, the Commission should explain how combinations of these techniques are assessed under the prohibition.

- **Materially Distorting Behavior of Individuals or Groups:** The Commission should clarify how intentionality (objective) and unintentional outcomes (effect) are weighed, specify how impacts on diverse or loosely defined groups are assessed, and define the contours of collective harm and explore collective means of action.
- **Recommendation Algorithms:** The Commission should also clarify the status of personalized recommendation algorithms, which may meet some criteria but should not automatically fall under the prohibition given user information obligations under Article 26 of the Digital Services Act.

Article 5(1)(b) – Exploitation of Vulnerabilities

The European Commission must clarify several aspects to ensure effective enforcement:

- **Definition of Vulnerabilities:** Age, disability, and socio-economic situations require clear criteria and concrete examples, particularly for cognitive, emotional, or physical vulnerabilities. For instance, do banking credit scoring algorithms, which rely on socio-economic situations, fall under the prohibition? We do not believe they should.
- **Quantifiable Measures:** Using thresholds to quantify vulnerabilities may be inappropriate, as this could exclude specific cases. Additionally, if vulnerabilities can be cumulative, should their combination be considered an aggravating factor?
- **Exploitation:** The term "exploitation" needs refinement: Does it require intent, or can unintentional exploitation also fall under the prohibition?
- **Regulatory Consistency:** The concepts within this provision should align with GDPR and DSA to avoid regulatory contradictions.

Article 5(1)(c) – Social Scoring

To ensure a strong ban on social scoring, the AI Act should provide:

- A clear distinction between classification and evaluation of individuals or groups.
- Clarification on whether the ban applies to corporate entities within "groups of persons."
- A precise definition of "certain period of time."
- Limits on what can be inferred or predicted about an individual’s personal traits.
- A definition of "social behavior," which lacks legal clarity.
- Clarification on whether the ban applies solely to public services or extends to private sectors.

- Distinctions between unjustified or disproportionate treatments based on social behavior and their gravity.

We believe that AI systems used to determine and allocate public assistance benefits and services based on personal and sensitive data to assess fraud risk should be classified as an unacceptable risk rather than a high-risk system.

Article 5(1)(d) – Individual Crime Risk Assessment and Prediction

Key questions that require clarification include:

- What qualifies as risk assessment or prediction related to a criminal offense?
- What traits and characteristics are admissible for assessment?
- Which AI systems are excluded because they merely support human decision-making based on objective and verifiable facts?
- What constitutes an objective and verifiable fact?
- How should the phrase "which is already based on" be interpreted in light of differing standards in criminal law and scientific validity?

Article 5(1)(e) – Untargeted Scraping of Facial Images

The following clarifications are needed:

- **Database Expansion:** The distinction between "creating" and "expanding" facial recognition databases should be specified. For example, does adding a single image to an existing database trigger the prohibition?
- **Scope:** Does the prohibition apply only to commercial databases, or does it also include research, security, and educational uses?
- **Untargeted Collection:** The meaning of "untargeted collection" should be clarified—does it include both automated and manual large-scale collection?
- **Internet and CCTV:** The term "Internet" should be defined—does it include social networks, public forums, or only unrestricted websites? For CCTV, guidelines should outline when and for what purposes such images can be used.

Article 5(1)(f) – Emotion Recognition

- **Fundamental Rights Compliance:** For instance, Article L1121-1 of the French Labor Code prohibits restrictions on individual and collective freedoms unless justified by job requirements and proportionate to the aim pursued.

- **Defining Emotion:** The AI Act should clarify whether emotion recognition applies only to primary emotions (happiness, sadness, anger, etc.) or also to physical states.
- **Distinguishing Emotional from Physical State Recognition:** Without clear definitions, this distinction could significantly impact fundamental rights.

Article 5(1)(h) – Real-Time Remote Biometric Identification

- **Regulatory Ambiguities:** The use of AI for customer identity verification in banking under PSD2 may conflict with Article 5(1)(h), which focuses on real-time biometric identification in public spaces for law enforcement.
- **Clear Exceptions:** The Commission should clarify that AI tools used for regulatory compliance (e.g., PSD2) or fraud prevention do not fall under the prohibition.
- **Public vs. Private Use:** Guidance should distinguish between biometric applications for law enforcement and broader compliance use cases.