Siinda

EU Proposal on Artificial Intelligence – short analysis

Context

EU proposal on Artificial Intelligence unveiled by European Commission on 21 April 2021, together with an overarching coordinated plan with Member States, to ensure both EU horizontal rules and national actions and enforcement.

Link of press release and overview: Europe fit for the Digital Age: Artificial Intelligence (europa.eu)

Major points

Cf presentation made by Lucilla Sioli, Director for AI at DG CNECT on 23 April 2021.

Definition and scope

- Horizontal regulation to be applicable in all EU and to all AI systems and products which create an outcome for EU subjects.
- Technologically neutral definition of AI
- Large scope, aim to include all AI. cf art 3 definition: "*a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".*
- List of AI techniques and approaches detailed in Annex I, can be updated by the European Commission.

Risk-based approach

AI classified under the level of risk they represent.

- **Unacceptable risk**: Prohibited- e.g. social scoring
- **High risk**: Permitted subject to compliance with AI requirements and ex ante conformity assessment – e.g. : recruitment, medical devices, credit scoring for individuals…
- **AI with specific transparency obligations**: Permitted but subject to information/transparency obligations - e.g. 'Impersonation' (bots)
- **Minimal or no risk**: Permitted with no restrictions.

Transparency obligations

For AI providers of certain AI systems (art 52) :

- **Notify humans that they are interacting with an AI** system unless this is evident.
- Notify humans that **emotional recognition or biometric categorisation** systems are applied to them.
- Apply **label to deep fakes** (unless necessary for the exercise of a fundamental right or freedom or for reasons of public interests)

Codes of Conduct

- Possible only for non-high-risk AI
- Specific **transparency** requirements
- **No mandatory** obligations
- Commission and Board to encourage drawing up of codes of conduct intended to foster the voluntary application of requirements to low risk AI systems.

High Risk AI Systems

One step down on the risk scale, the proposal lists artificial intelligence systems with "**high-risk**" use, which are systems with a variety of sensitive applications, from transport (such as self-driving vehicles), to essential private and public services (such as credit scoring) to education (e.g. exam scoring). The proposal also targets **public applications of AI**, especially in the fields of law enforcement, migration and border control management, and administration of justice.

High-risk systems will be allowed to be commercialized and used in the EU only after complying with **conformity assessment procedures**, to ensure that the systems or their application respect the EU standards. Although the proposal plans for national authorities to conduct checks to ensure that systems are compliant, the text still intends for many applications to be evaluated through **self-assessment**, meaning that the AI providers will assess themselves if they meet the conformity criteria set by the EU. Those criteria notably include: having in place adequate risk assessment and mitigation systems, using high quality datasets to avoid algorithmic bias, and ensuring appropriate human oversight. This flexibility is likely to be positively welcomed by the tech industry, but MEPs have already warned that they would support stricter compliance rules.

As the proposal is likely to be reworded and amended during the negotiation process, the impact it will have on the tech sector is not easy to evaluate. However, if the proposal were to be accepted as is, the first impact for the tech sector would be that companies commercializing banned AI systems, or putting on the market high-risk systems that have not gone through the conformity assessment procedure, could be subject to financial penalties of 6% of the company's total annual turnover. Considering the vague wording used by the Commission, it is difficult to understand how this law will be practically enforced.

Scope

- Can be in various sectors such as safety components of regulated products, biometric identification, education and vocational training, employment and worker management or access to and enjoyment of essential private services and public services and benefits .
- In the latter, credit scoring denying access of individual to a loan is explicitly cited as an example of high-risk AI

Requirements for High-risk AI

- Use high-quality training, validation and testing data
- Have clear documentation and keep logging information (traceability)
- Give users enough transparency and explain how to use the system.
- Ensure human oversight is built into the system.
- Guarantee accuracy and cybersecurity.

Obligations of AI providers

- Establish and Implement quality management system in its organisation
- Draw up and keep up to date technical documentation
- Logging obligations to enable users to monitor the operation of the high-risk AI system
- Undergo conformity assessment and potentially re assessment of the system (in case of significant modifications)
- Register AI system in EU database
- Affix CE marking and sign declaration of conformity
- Conduct post market monitoring
- Collaborate with market surveillance authorities

Obligations of AI users

- Operate AI system in accordance with instructions of use
- Ensure human oversight when using of AI system.
- Monitor operation for possible risks

- Inform the provider or distributor about any serious incident or any malfunctioning.
- Existing legal obligations continue to apply (e.g., under GDPR)

The Commission has launched a consultation for feedback period of 8 weeks on the whole proposal : [Artificial intelligence – ethical and legal requirements (europa.eu)]

Major articles and recitals

Most crucial points are in title I (scope and definitions), title III (High-risk AI systems) and Annex III, title IV (transparency obligations for AI systems) , and titles VI, VII and VIII on governance and implementation requirements.

Scope and definitions

Recital 11: this Regulation should also apply to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union.

Recital 14: In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed.

Article 3: For the purpose of this Regulation, the following definitions apply:

> (1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;
>
> (2) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;
>
> (3) 'small-scale provider' means a provider that is a micro or small enterprise within the meaning of Commission Recommendation 2003/361/EC61;
>
> (4) 'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;

Article 4: Amendments to Annex I

The Commission is empowered to adopt delegated acts in accordance with Article 73 to amend the list of techniques and approaches listed in Annex I, in order to update that list to market and technological developments on the basis of characteristics that are similar to the techniques and approaches listed therein.

Prohibited AI systems

Recital 17: AI systems providing social scoring of natural persons for general purpose by public authorities or on their behalf may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify the trustworthiness of natural persons based on their social behaviour in multiple contexts or known or predicted personal or personality characteristics. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. **Such AI systems should be therefore prohibited**.

Article 5: The following artificial intelligence practices shall be prohibited:

(c) the placing on the market, putting into service or use of AI systems by public authorities or on their behalf for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

> (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
>
> (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

High-Risk AI systems

Recital 27: High-risk AI systems should only be placed on the Union market or put into service if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any.

Recital 37 : Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, AI systems used to evaluate the credit score, or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services **such** as housing, electricity, and telecommunication services. AI systems used for this purpose may lead to discrimination of persons or groups and perpetuate historical patterns of discrimination, for example based on racial or ethnic origins, disabilities, age, sexual orientation, or create new forms of discriminatory impacts**.** Considering the very limited scale of the impact and the available alternatives on the market, it is appropriate to exempt AI systems for the purpose of creditworthiness assessment and credit scoring when put into service by small-scale providers for their own use. Natural persons applying for or receiving public assistance benefits and services from public authorities are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. **If AI systems are used for determining whether such benefits and services should be denied, reduced, revoked or reclaimed by authorities, they may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy. Those systems should therefore be classified as high-risk**. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. Finally, AI systems used to dispatch or establish priority in the dispatching of emergency first response services should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

Recital 43 : **Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity**. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.

Recital 45: Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency, and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety, and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.

Recital 46: Requirements should apply to high-risk AI systems as regards the quality of data sets used, technical documentation and record-keeping, transparency, and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety, and fundamental rights, as applicable in the light of the intended purpose of the system, and no other less trade restrictive measures are reasonably available, thus avoiding unjustified restrictions to trade.

Recital 48: High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning. For this purpose, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training, and authority to carry out that role.

Recital 62: In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.

Recital 67: High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

Recital 69 : providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, should be required to register their high-risk AI system in a EU database, to be established and managed by the Commission.

Recital 70 : In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. Moreover, natural persons should be notified when they are exposed to an emotion recognition system or a biometric categorisation system. Such information and notifications should be provided in accessible formats for persons with disabilities

Recital 73 : In order to promote and protect innovation, it is important **that the interests of small- scale providers and users of AI systems** are taken into particular account. To this objective, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Moreover, the specific interests and needs of small-scale providers shall be taken into account when Notified Bodies set conformity assessment fee

Recital 80 : Union legislation on financial services includes internal governance and risk management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legislation, the authorities responsible for the supervision and enforcement of the financial services legislation, including where applicable the European Central Bank, should be designated as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions

Article 6 : Classification rules for high-risk AI systems

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product

pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

Article 7: Amendments to Annex III

1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

> (a) the AI systems are intended to be used in any of the areas listed in points 1 to 8 of Annex III;
>
> (b) the AI systems pose a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights, that is, in respect of its severity and probability of occurrence, equivalent to or greater than the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

Article 8: Compliance with the requirements

1. High-risk AI systems shall comply with the requirements established in this Chapter.

2. The intended purpose of the high-risk AI system and the risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

Article 9: Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

2. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:

(a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

(b) estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse;

(c) evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system referred to in Article 61;

(d) adoption of suitable risk management measures in accordance with the provisions of the following paragraphs.

9. For credit institutions regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.

Article 10 Data and data governance

1. High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5.

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,

(a) the relevant design choices;

(b) data collection;

(c) relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation;

(d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent;

(e) a prior assessment of the availability, quantity and suitability of the data sets that are needed;

(f) examination in view of possible biases;

(g) the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed.

Article 11 Technical documentation

1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

Article 12 Record-keeping

1. High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events (‘logs’) while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications.

Article 13 Transparency and provision of information to users

1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately

Article 14 Human oversight

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.

2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter.

3. Human oversight shall be ensured through either one or all of the following measures:

> (a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;
>
> (b) identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the user.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition, no action or decision is taken by the user on the basis of the identification resulting from the system unless this has been verified and confirmed by at least two natural persons.

Obligations of providers

Article 16 Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

- (a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;
- (b) have a quality management system in place which complies with Article 17;
- (c) draw-up the technical documentation of the high-risk AI system;
- (d) when under their control, keep the logs automatically generated by their high-risk AI systems;

(e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

(f) comply with the registration obligations referred to in Article 51;

(g) take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;

(h) inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;

(i) to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;

(j) upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

Article 18 Obligation to draw up technical documentation

1. Providers of high-risk AI systems shall draw up the technical documentation referred to in Article 11 in accordance with Annex IV.

2. Providers that are credit institutions regulated by Directive 2013/36/EU shall maintain the technical documentation as part of the documentation concerning internal governance, arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Article 19 Conformity assessment

1. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. Where the compliance of the AI systems with the requirements set out in Chapter 2 of this Title has been demonstrated following that conformity assessment, the providers shall draw up an EU declaration of conformity in accordance with Article 48 and affix the CE marking of conformity in accordance with Article 49.

Governance and implementation

Article 30 Notifying authorities

1. Each Member State shall designate or establish a notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

2. Member States may designate a national accreditation body referred to in Regulation (EC) No 765/2008 as a notifying authority.

Article 32 Notification procedure

1. Notifying authorities may notify only conformity assessment bodies which have satisfied the requirements laid down in Article 33.

2. Notifying authorities shall notify the Commission and the other Member States using the electronic notification tool developed and managed by the Commission.

3. The notification shall include full details of the conformity assessment activities, the conformity assessment module or modules and the artificial intelligence technologies concerned.

Article 43 Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Chapter 2 of this Title, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall follow one of the following procedures:

(a) the conformity assessment procedure based on internal control referred to in Annex VI;

(b) the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

Article 48 EU declaration of conformity

1. The provider shall draw up a written EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.

2. The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into an official Union language or languages required by the Member State(s) in which the high-risk AI system is made available.

Article 52 Transparency obligations for certain AI systems

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate and prosecute criminal offences, unless those systems are available for the public to report a criminal offence.

Article 60 EU database for stand-alone high-risk AI systems

1. The Commission shall, in collaboration with the Member States, set up and maintain a EU database containing information referred to in paragraph 2 concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Article 51.

2. The data listed in Annex VIII shall be entered into the EU database by the providers. The Commission shall provide them with technical and administrative support.

3. Information contained in the EU database shall be accessible to the public.

4. The EU database shall contain personal data only insofar as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider.

5. The Commission shall be the controller of the EU database. It shall also ensure to providers adequate technical and administrative support.

Penalties

Article 71 Penalties

1. In compliance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties, including administrative fines, applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are properly and effectively implemented. The penalties provided for shall be effective, proportionate, and dissuasive. They shall take into particular account the interests of small-scale providers and start-up and their economic viability.

2. The Member States shall notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.

3. The following infringements shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher:

(a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;

(b) non-compliance of the AI system with the requirements laid down in Article 10.

4. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

ANNEX I ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometric identification and categorisation of natural persons:

    (a) AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons;

2. Management and operation of critical infrastructure:

    (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.

3. Education and vocational training:

(a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;

(b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.

4. Employment, workers management and access to self-employment:

(a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;

(b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

5. Access to and enjoyment of essential private services and public services and benefits:

(a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;

(c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.

6. Law enforcement:

(a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;

(b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);

(d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;

(e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;

(f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;

(g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

7. Migration, asylum and border control management:

(a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;

(b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;

(c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;

(d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.

8. Administration of justice and democratic processes:

(a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

Siinda