Council of the European Union
General Secretariat

Brussels, 21 September 2021

WK 11117/2021 INIT

LIMITE

TELECOM

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Telecommunications and Information Society
Subject:	Artificial Intelligence Act - PowerPoint Presentation : AI Act proposal: Article 7, Annex III, Art 16-23

Delegations will find in annex the PowerPoint Presentation on Artificial Intelligence Act made by the Commission at the Telecommunications and Information Society Working Party on 21 September 2021.

Proposal for an Artificial Intelligence Act Art. 7, Annex III, Artt. 16-23

Kilian Gross
DG CNECT, European Commission

Telecom Council Working Party
21 September 2021

Recap of CWP of 7.9.2021

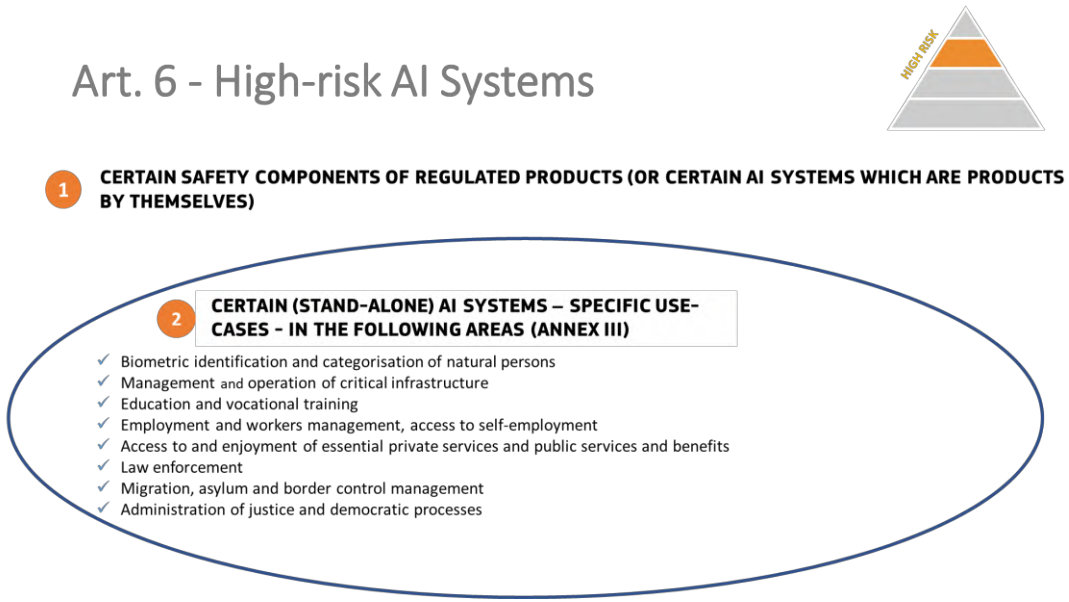
- Art. 6(1) – classification of high-risk for AI systems in relation to products already regulated by EU law

- Art. 5 – prohibited AI & biometrics

Article 7

Art. 7 - Empowerment to amend Annex III

- **Art. 6(2)** → AI systems **explicitly listed in Annex III (and only those)** are high-risk



Art. 7 & impact assessment (SWD(2021) 84 final)

HIGH RISK

Table 7: List of high-risk AI use cases (stand-alone) identified following application of the risk assessment methodology

HIGH-RISK USES	POTENTIAL HARMS	ESPECIALLY RELEVANT INDICATIVE CRITERIA*	EVIDENCE & OTHER SOURCES
AI systems intended to be used for the remote biometric identification of persons in publicly accessible spaces	Intense interference with a broad range of fundamental rights (e.g. private life and data protection, human dignity, freedoms expression, freedom of assembly and association) Systemic adverse impact on society at large (i.e., on democratic processes, freedom and chilling effect on civic discourse)	Already used by an increasing number of public and private actors in the EU Potentially very severe extent of multitude of harms High potential to scale and adversely impact a plurality of people Vulnerability of affected people (e.g. people cannot object freely, imbalance if used by public authorities) Indication of harm (legal challenges and decisions by courts and DPAs)	AlgorithmWatch and Bertelsma Stiftung, *Automating Society Rep 2020*, 2020 (pp. 38-39, p. 104); European Data Protection Boa *Facial recognition in school rend Sweden's first GDPR fine*, 2019; European Data Protection Boa *EDPS Opinion on the Europe Commission's White Paper Artificial Intelligence – A Europe approach to excellence and tr* 2020 (pp. 20-21); Agency for Fundamental Rigl *Facial recognition technolo fundamental rights considerati in the context of law enforceme* 2019; Court of Appeal, United Kingdc Decision R (Bridges) v. CC So Wales, EWCA Civ 1058 of August 2020; Buolamwini, I./ Gebru, T., *Gen Shades: Intersectional Accur Disparities in Commercial Gen Classification*, 2018; National Institute of Standards a Technology, U.S. Department Commerce, *Face Recognit Vendor Test (FRVT) Part Demographic Effects*, 2019.

Annex 5, point 5.4 Impact Assessment:

- list of Annex III identified on the basis of conditions and criteria of Art. 7

European Commission

Art. 7 – Rationale

HIGH RISK

POLICY CHOICE

- Focus regulatory intervention on **concrete and specific use cases**, **NOT on the technology as such** or **broad sectors/areas**
- Allow addresses to **easily and immediately check** whether their AI system is subject to rules of the AIA or not

TOOL NEEDED

- Regulatory system must be **flexible & swiftly adaptable**
- Without agile tools, the **risk is too regulate too much or too little** with likely **suboptimal effects** (overregulation when not needed or lack of protection when needed)

Delegated powers of the EC with well defined limitations

European Commission

Art. 7 – delegated power and conditions

HIGH RISK

Update the list of Annex III by **adding high-risk AI systems** provided that:

1) AI system intended to be used in any of the **areas listed in points 1-8 Annex III**;

&

1) AI system pose a **risk** of harm to health & 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 AI systems already listed in Annex I

NOT ALLOWED

- Delete use cases from Annex III
- Extend or reduce scope of application of AIA by amending areas in points 1-8
- Add use cases with lower risk-levels

European Commission

Art. 7 – Criteria

HIGH RISK

a) **intended purpose** of the AI system

b) AI system **in use** or **about to be used**

c) AI system already **caused harm** or there are **significant concerns** around materialization of harm (reports and documented allegations)

d) **extent of harm** (intensity and ability to affect plurality of persons)

e) impacted persons **dependent on the outcome** produced with AI system

f) impacted persons in **vulnerable position** vis-à-vis user of AI system

g) **reversibility of outcome** produced with AI system

h) effective measures in **Union law** providing for **redress** and **preventing/substantially minimizing risks**

Annex III

Annex III High-risk AI systems referred to in Art. 6(2)

HIGH RISK

CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS:

1. Biometric identification and categorisation of natural persons
2. Management and operation of critical infrastructure
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

Annex III, 1 - Biometric identification and categorisation

HIGH RISK

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

*AI system **for the purpose of identifying natural persons at a distance** through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified (Art.3(36))*

*whereby the capturing of biometric data, the comparison and the identification all occur **without a significant delay**. This comprises not only instant identification, but also limited short delays in order to avoid circumvention(Art.3(37))*

*a remote biometric identification system **other than a 'real-time' remote** biometric identification system (Art.3(38))*

YES

- Real-time RBI in private places
- Screening of video footage to identify a suspect
- RBI online (e.g. check a face with images on internet)

NO

- Fingerprint/face to unlock a phone
- Authentication of clients by banks during onboarding process/access to bank account…

European Commission

Annex III, 2 - Management and operation of critical infrastructure

HIGH RISK

'a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property' (Art. 3(14) AIA)

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**

YES

- AI system managing the traffic of self-driving cars
- AI system for safe maintenance of electricity grids

NO

- AI system managing maritime traffic

Annex III, 3 - Education and vocational training

HIGH RISK

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

YES

- AI system for screening and triaging of applications for admission to education and vocational training institutions

NO

- Chat bot on a school website
- Data analytics comparing statistics of all school applications

(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**

YES

- AI-enabled evaluation of tests
- Emotion recognition systems used during exams (e.g. to identify if students cheat)

NO

- AI systems for internal reporting of grades and comparison between classes

European Commission

Annex III, 4 - Employment and workers management, access to self-employment

HIGH RISK

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;

YES

- AI system filtering job applications
- Emotion recognition system used during a job interview

NO

- Chatbot on a website replying to questions from job seekers
- Automated spell check of job vacancies

(b) AI systems 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

YES

- AI system assisting the annual assessment of staff for promotion exercises (e.g. analysis of work performance)
- AI system allocating tasks to Uber drivers/riders

NO

- AI system supporting HR in payroll execution (without monitoring or evaluation of staff performance)

Annex III, 5 - Access to and enjoyment of 'essential' private services, public services & benefits

HIGH RISK

'necessary for people to fully participate in society or to improve one's standard of living' (recital 37)

a) AI systems 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;

YES

- AI system for determining eligibility for housing and other social benefits
- AI system to detect fraudulent reception of benefits

NO

- AI systems used to detect irregularities in the allocation of funds to companies

(b) AI systems 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;

YES

- AI systems used by credit bureaux
- Credit-scoring models used by medium and large banks

NO

- Small fintech developing in-house an AI tool for creditworthiness assessment of its own customers
- AI tools for credit scoring of legal persons

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

YES

- Digital operator in a 112 call center

NO

- AI system recommending locations for regular patrolling (no emergency)

European Commission

Annex III, 6 - Law enforcement

Art. 3(40) AIA: same as Law Enforcement Directive

HIGH RISK

The following AI systems **intended to be used by *'law enforcement authorities':***

a) 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 *(e.g. AI tool assessing the risk of re-offending of criminals to influence sentencing and probation outcomes)*

b) **polygraphs** and similar tools or to detect the **emotional state** of a natural person *(e.g. lie detectors used in interrogations)*

c) for detection of **deep fakes** *(e.g. determine authenticity of a video footage during police investigations)*

d) for **evaluation of the reliability of evidence** in the course of investigation or prosecution of criminal offences *(e.g. AI tool supporting prosecutors to analyse the reliability of evidence, like DNA samples, collected from a crime scene)*

e) **predicting the occurrence or reoccurrence of an actual or potential criminal offence** based on **i) profiling** of natural persons or ii) **assessing personality traits and characteristics or past criminal behaviour** of natural persons or groups *(e.g. AI tool profiling internet users based on their behavior to predict who is a pedophile);*

f) for **profiling of natural persons in the course of detection, investigation or prosecution** of criminal offences *(e.g. AI tool used to profile residents in a certain area to predict who are the likely suspects of a past terrorist attack);*

g) 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** *(e.g. complex crime analytics tools such as Palantir)*

Annex III, 7 - Migration, asylum and border control management

HIGH RISK

The following AI systems **intended to be used by 'competent public authorities':**

a) **polygraphs** and similar tools or to **detect the emotional state** of a natural person

YES
- Lie detector used by border control authorities

NO
- Drone patrolling EU borders

b) 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

YES
- PNR profiling of air passengers

NO
- Data analytics used to detect general patterns of illegal immigration

c) 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

YES
- AI tool used to detect fraudulent passports

NO
- Facial recognition system at automated border control

d) 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.

YES
- AI triaging system filtering visa applications in different strands of priority

NO
- AI tool allocating visa applications to case handlers (no priority triaging)

European Commission

Annex III point 8 Administration of justice and democratic processes

HIGH RISK

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.

YES

- AI tool supporting judges in researching and analysing case-law
- AI tool analysing the facts of concrete case and recommending outcomes

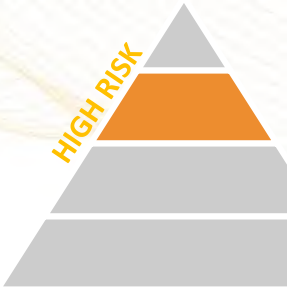
NO

- AI tool for anonymisation or pseudonymisation of judicial decisions, documents or data
- AI systems to support administrative tasks or allocation of resources

European Commission

Articles 16-23

Article 16 - Overview of obligations of providers



'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' (Art. 3(2) AIA)

- Ensure that AI system is compliant with the requirements (Art. 8-15)
- **Establish and implement quality management system in its organisation**
- **Draw-up and keep up to date technical documentation**
- **Keep the logs automatically generated by the system**
- **Undergo conformity assessment of the system**
- **Take necessary corrective actions in case of non-compliance of the system**
- **Information and cooperation obligations vis-à-vis competent authorities and notified bodies**
- Register AI system in EU database (Art. 51)
- Affix CE marking (Art. 49)

European Commission

Art. 17 – Quality management system (1/2)

- **Concept**
  - widely known and used in **companies and organizations** alike
  - already developed in **standardization** (e.g. ISO 9000, ISO(draft) 42001)
  - already adopted **in EU legislation**:
    - Reg. 2017/745 and 2017/746 (Medical Devices)
    - Conformity assessment modules based on control of quality system under New Legislative Framework acquis (Decision 768/2008/EC)

- **Rationale**
  - ensure that procedures and processes in providers' organizations lead to consistent and continuous compliance with AIA

Article 17 – Quality management system (2/2)

Documented in written policies, procedures and instructions

At least:

- strategy for regulatory compliance
- techniques, procedures and systematic actions to be used for:
  - the design, design control and design verification of the high-risk AI system
  - the development, quality control and quality assurance of the high-risk AI system
- examination, test and validation procedures
- technical specifications, including standards, to be applied
- systems and procedures for data management and record keeping
- risk management system (Art. 9)
- post-market monitoring system (Art. 61)
- procedures related to the reporting of serious incidents and of malfunctioning (Art. 62)
- handling of communication with national competent authorities, notified bodies, other operators, customers
- resource management and accountability framework

Implementation **proportionate to the size of the provider**

Art. 18 - Draw-up technical documentation (Annex IV)

- demonstrate compliance with requirements (Title III, Ch. 2)

&

- enable authorities and notified bodies to assess such compliance

Before AI system placed on the market and **kept up-to date**

At least (Annex IV):

- general description of the AI system
- detailed description of **the elements of the AI system** and of the **process for its development**
- detailed **information about the monitoring, functioning and control of the AI system**
- detailed **description of the risk management system**
- (as applicable) description of any **change made to the system through its lifecycle**
- list of **harmonised standards applied** or description of **other technical solutions adopted**
- copy of the **EU declaration of conformity**
- detailed description of the **system to evaluate the AI system performance in the post-market phase**

Art. 19 – Conformity assessment

procedure whereby compliance of AI system with requirements (Title III, Ch. 2) is verified

To be carried out **prior to the placing on the market/putting into service**

- **In accordance with the procedures laid down in Art. 43**
  - internal controls or third-party conformity assessment body/notified body

- Successful conformity assessment is **pre-condition for:**
  - Drawing up of a EU declaration of conformity
  - Affixing of CE mark to the AI system
  - Placing on the market/putting into service of AI system

Art. 20 – Automatically generated logs

- **Must be stored by provider**
  - **to the extent these logs are under the control of the provider** by means of
    - contractual arrangement with user or
    - otherwise by law
  - **for a period appropriate** in the light of
    - intended purpose of the AI systems and
    - legal obligations under Union or national law

Ad hoc provisions for credit institutions

- **Artt. 17, 18, 19 and 20:** credit institutions regulated by Directive 2013/36/EU
- **Rationale:** avoid duplication and ensure full integration of AIA obligations in existing framework regulating such credit institutions
- **Specific provisions:**
  - Quality management system fulfilled by complying with similar rules on internal governance under Art. 74 of Directive 2013/36
  - Technical documentation to be part of documentation established as per Art. 74 of Directive 2013/36
  - Conformity assessment to be carried out as part of the supervisory review and evaluation process foreseen in Artt. 97-101 of Directive 2013/36
  - Logs to be maintained as part of the documentation established as per Art. 74 of Directive 2013/36

Artt. 21, 22, 23: other obligations

Similar obligations in product legislation

CORRECTIVE ACTION

When providers consider or have reason to consider that a distributed **AI system is not in compliance** they shall

- ▸ Immediately **take necessary corrective actions** (e.g. bring the system into conformity, withdraw, recall)
- ▸ **Inform** distributors, authorized representatives, importers accordingly

INFORMATI

Where the **system presents a risk** (within the meaning of Article 65(1)) & **the risk is known to provider**

- ▸ The provider shall **inform the national competent authorities and notified body**
- ▸ Information shall include non-compliance and any corrective actions taken

COOPERATION

Upon request by national competent authorities, the provider shall

- ▸ **provide that authority with all the information and documentation** necessary to demonstrate the conformity of the high-risk AI system
- ▸ **(**reasoned request**) give that authority access to the logs automatically generated** by the high-risk AI system (to the extent the logs are under his control)

Thank you