Council of the European Union
General Secretariat

Brussels, 20 May 2021

WK 6771/2021 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:	Proposal for an Artificial Intelligence Act : PowerPoint presentation by the Commission (COSI meeting 19 May)

Delegations will find in annex a PowerPoint presentation on Artificial Intelligence Act made by the Commission at the COSI meeting on 19 May 2021

Proposal for an Artificial Intelligence Act

Lucilla Sioli
DG CNECT, European Commission

COSI Working Party
19 May 2021

COORDINATED PLAN ON ARTIFICIAL INTELLIGENCE: FOUR KEY POLICY OBJECTIVES

SET ENABLING CONDITIONS FOR AI DEVELOPMENT AND UPTAKE IN THE EU

- Acquire, pool and share policy insights
- Tap into the potential of data
- Foster critical computing capacity

MAKE THE EU THE RIGHT PLACE; EXCELLENCE FROM LAB TO THE MARKET

- Collaboration with stakeholders, Public-private Partnership on AI, data and robotics
- Research capacities
- Testing and experimentation (TEFs), uptake by SMEs (EDIHs)
- Funding and scaling innovative ideas and solutions

ENSURE AI TECHNOLOGIES WORK FOR PEOPLE

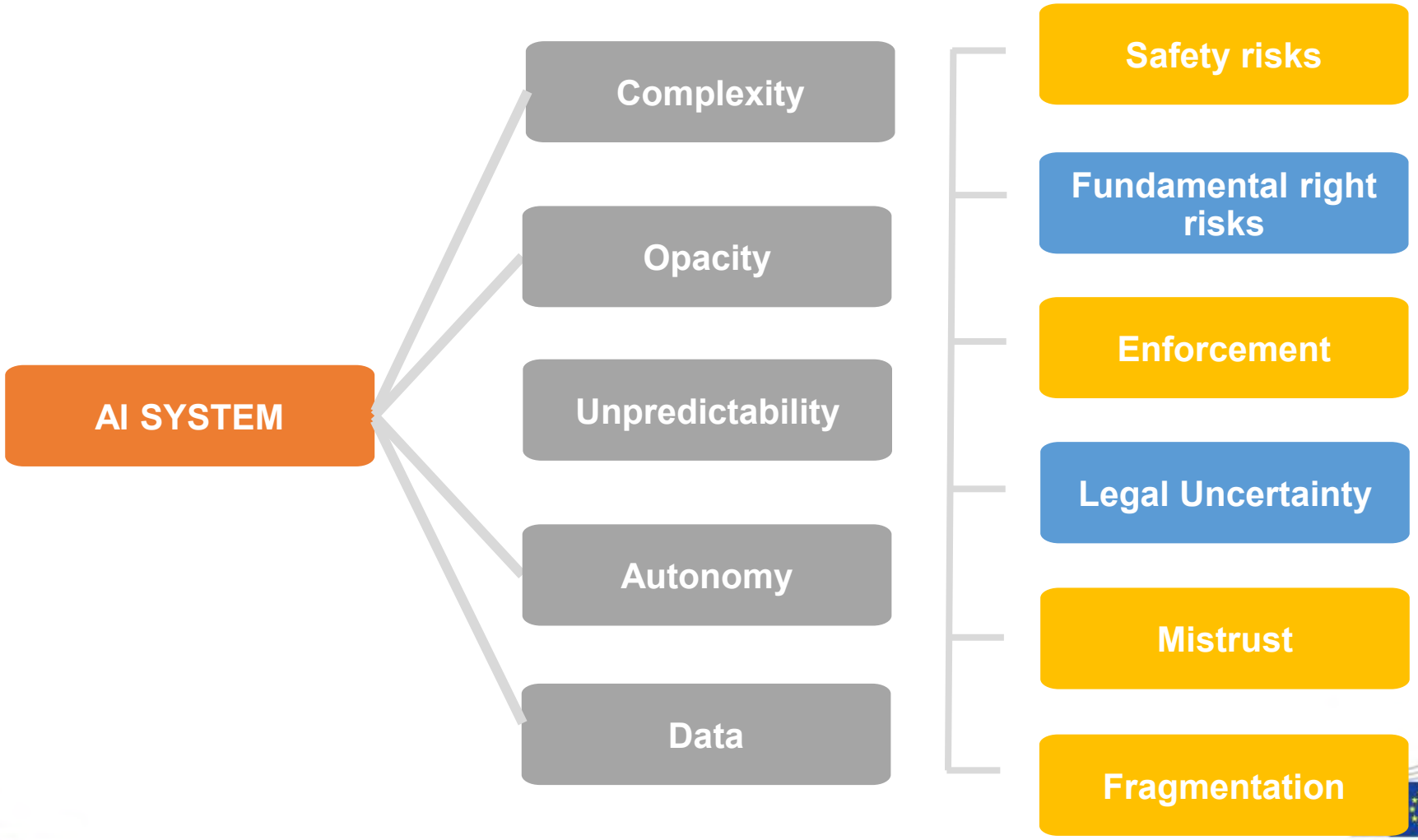
- Talent and skills
- A policy framework to ensure trust in AI systems
- Promoting the EU vision on sustainable and trustworthy AI in the world

BUILD STRATEGIC LEADERSHIP IN THE SECTORS

- Climate and environment
- Health
- Strategy for Robotics in the world of AI
- Public sector
- Law enforcement, immigration and asylum
- Mobility
- Agriculture

Investments: Horizon Europe, Digital Europe, Recovery and Resilience Facility

Why do we regulate AI use cases?



Scope of application (Art. 2)

Regulation applicable to:

- **Providers (public or private)** placing on the market or putting into service AI systems in the Union independent from their origin
- **Users (public or private)** located within the Union
- **Providers and users** located in a third country, where the output produced by the system is used in the Union

Excluded from the scope:

- Public authorities in a third country or international organisations who use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States
- AI developed or used exclusively for military purposes

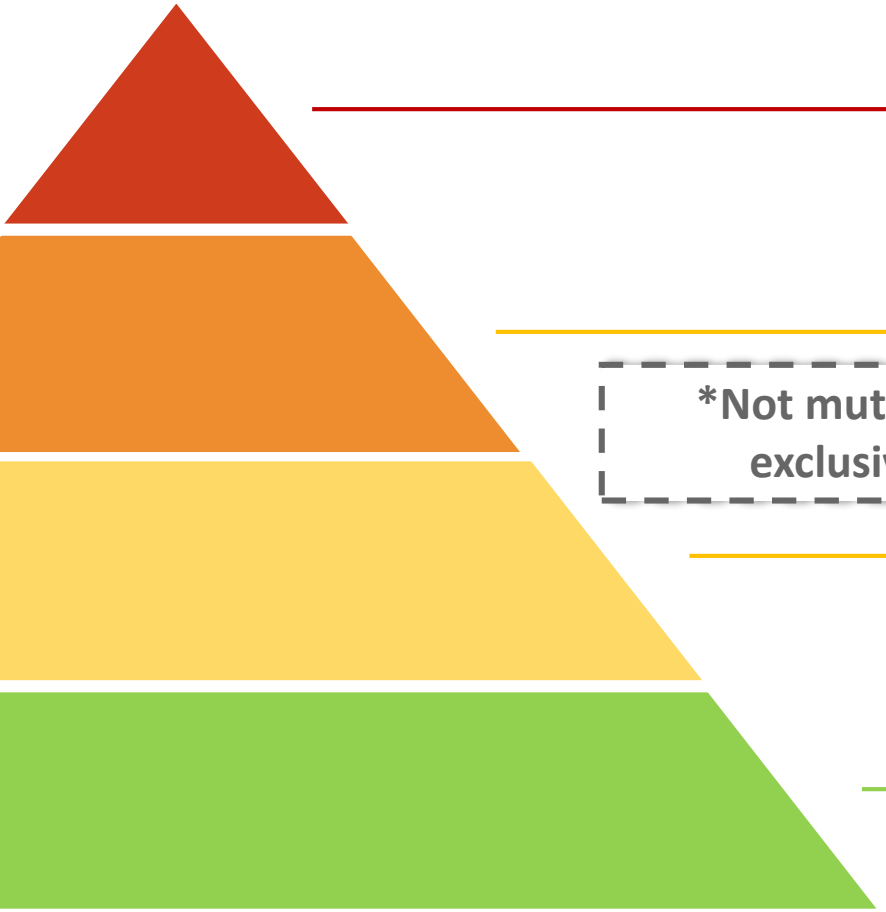
Definition and technological scope of the regulation (Art. 3)

Definition of Artificial Intelligence

- Definition of AI should be **as neutral as possible** in order to cover techniques which are not yet known/developed
- **Overall aim is to cover all AI**, including traditional symbolic AI, Machine learning, as well as hybrid systems
- **Annex I**: list of AI techniques and approaches should provide for legal certainty (adaptations over time may be necessary)

> *"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"*

A risk-based approach to regulation



Unacceptable risk
e.g. social scoring

Prohibited

High risk
e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

*Not mutually exclusive

AI with specific transparency obligations
'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

Minimal or no risk

Permitted with no restrictions

European Commission

Most AI systems will not be high-risk (Titles IV, IX)

MINIMAL OR NO RISK

New transparency obligations for certain AI systems (Art. 52)

- **Notify humans** that they are **interacting with an AI system** unless this is evident or the system is authorised by law to detect, prevent, investigate and prosecute criminal offences (exception: system for the public to report a criminal offence).
- **Notify humans** that **emotional recognition or biometric categorisation systems** are applied to them unless the system is used for biometric categorisation, permitted by law to detect, prevent and investigate criminal offences
- Apply **label to deep fakes** unless necessary for the exercise of a fundamental right or freedom or for reasons of public interests or authorised by law to detect, prevent, investigate and prosecute criminal offences

Possible voluntary codes of conduct for AI with specific transparency requirements (Art. 69)

- 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 Artificial Intelligence Systems (Title III, Annexes II and III)

Certain applications in the following fields:

1 **SAFETY COMPONENTS OF REGULATED PRODUCTS**

(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

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

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

European Commission

High-risk AI Systems used by law enforcement and competent public authorities (Annex III)

Low enforcement	▸ individual risk assessments of natural persons (**risk of offending/reoffending or potential victims**); ▸ assessment of profile, personality or past criminal behaviour of natural persons or groups **involved in crime**; ▸ profiling of natural persons in the course of **detection, investigation or prosecution** of criminal offences; ▸ **crime analytics regarding** natural persons (use of complex related and unrelated data sets to identify unknown patterns or discover hidden relationships in the data); ▸ **polygraphs** and similar tools or to detect the emotional state of a natural person; ▸ to detect **deep fakes**; ▸ **evaluation of the reliability of evidence** in the course of investigation or prosecution of criminal offences.
Migration, asylum & border control	▸ **polygraphs** and similar tools or to detect the emotional state of a natural person; ▸ **risk assessment**, 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; ▸ **verification of the authenticity** of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features; ▸ **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.

CE marking and process (Title III, chapter 4, art. 49.)

CE marking is an indication that a product complies with the requirements of a relevant Union legislation regulating the product in question. In order to affix a CE marking to a high-risk AI system, a provider shall undertake **the following steps:**

1 **Determine** whether its AI system **is classified as high-risk** under the new AI Regulation

2 **Ensure** design and development and quality management system are **in compliance with the AI Regulation**

3 **Conformity assessment procedure**, aimed at assessing and documenting compliance

4 **Affix the CE marking to the system** and sign a declaration of conformity

5 **PLACING ON THE MARKET or PUTTING INTO SERVICE**

European Commission

Requirements for high-risk AI (Title III, chapter 2)

Establish and implement **risk management** processes

&

In light of the **intended purpose** of the AI system

- Use high-quality **training, validation and testing data** (relevant, representative etc.)
- Establish **documentation** and design logging features (traceability & auditability)
- Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)
- Ensure **human oversight** (measures built into the system and/or to be implemented by users)
- Ensure **robustness**, **accuracy** and **cybersecurity**

Overview: obligations of operators (Title III, Chapter 3)

Provider obligations

- 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** (self assessment for law enforcement AI systems, third party assessment for remote biometric identification systems) and potentially re-assessment of the system (in case of significant modifications)
- Register AI system in EU database (no publication of the instruction of use for law enforcement policies, Annex VIII, 11.)
- Affix CE marking and sign declaration of conformity
- Conduct **post-market monitoring**
- **Collaborate** with market surveillance authorities (data protection or supervisory authority, Art. 63(5))

User obligations

- 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)

Remote biometric identification (RBI)
(Title II, Art. 5, Title III - Art. 6, Annex III (1)(a)

Use of real-time RBI systems for law enforcement purposes (Art. 5)

Prohibition of use for law enforcement purposes in publicly accessible spaces with exceptions:

- Search for victims of crime
- Threat to life or physical integrity or of terrorism
- Serious crime (EU Arrest Warrant)

Ex-ante authorisation by judicial authority or independent administrative body

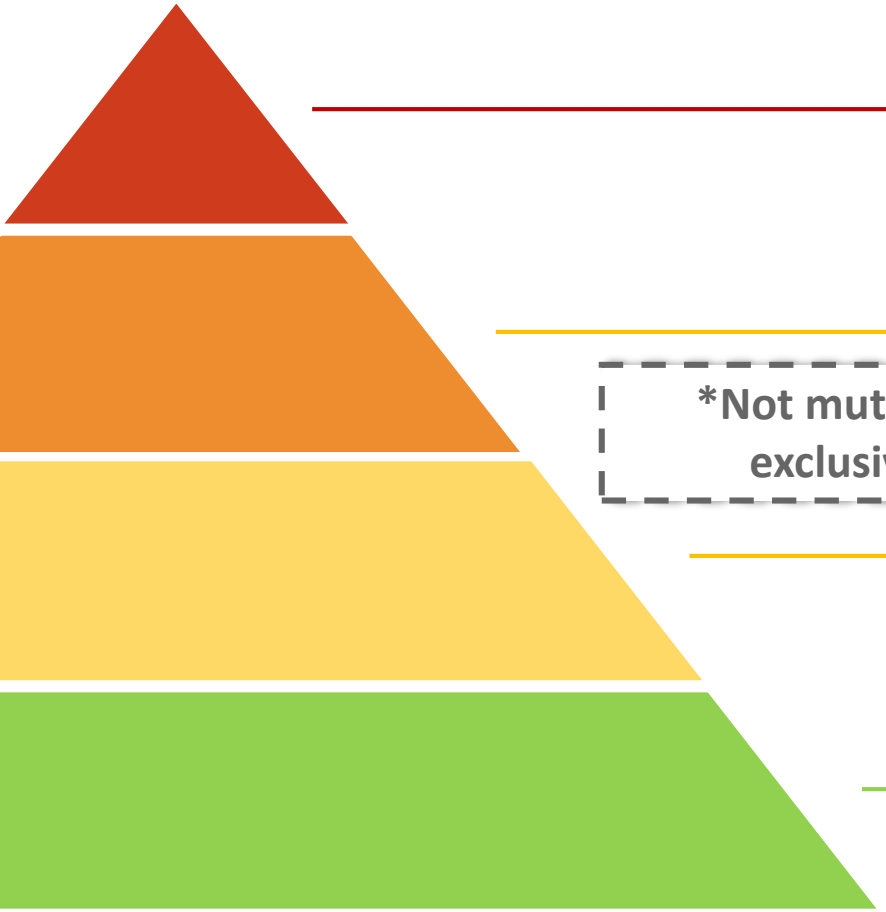
Member States shall lay down in their national law the respective national provisions.

Putting on the market of RBI systems (real-time and post, public and private)

- **Requirements for high-risk systems**
  - **Ex ante third party conformity assessment** by market surveillance authority
  - Enhanced logging requirements
  - "Four eyes" principle

No additional rules foreseen for use of real-time and post RBI systems: existing data protection rules apply

A risk-based approach to biometrics



*Not mutually exclusive

Unacceptable risk

Real-time RBI systems for law enforcement purposes in publicly accessible spaces

Prohibited (with limited exceptions)

High risk

All RBI systems

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

AI with specific transparency obligations

Emotional recognition and categorisation systems

Permitted but subject to information /transparency obligations (with limited exceptions)

Minimal or no risk

Biometric authentication/verification
Closed set identification/ controlled environment

Permitted with no restrictions

European Commission

The governance structure (Titles VI and VII)

European level

European Commission to act as Secretariat

- Artificial Intelligence Board

- Expert Group*

National level

National Competent Authority/ies

- **For law enforcement**: MS to designate data protection or sectoral supervisory authority, Art. 63(5)
- Special rules on **confidentiality of information** Art. 70 (2)

*Not foreseen in the regulation but the Commission intends to introduce it in the implementation process

Exceptions for large-scale systems already placed on the market or put into service (Article 83, Annex IX)

- The regulation does not apply to

  AI systems which are components of large-scale IT systems and have been placed on the market or put into service before *12 months after the date of application of the Regulation (24 months after the entering into force of the Regulation)*,

- unless the replacement or amendment of the legal acts underlying the large IT systems leads to a significant change in the design or intended purpose of the AI system or AI systems concerned.
- The requirements of the AI Regulation shall be taken into account – where applicable - in the evaluation the large-scale IT systems.

Large-scale systems (Annex IX)

- Schengen Information System,
- Visa Information System,
- Eurodac,
- Entry/Exit System,
- European Travel Information and Authorisation System,
- European Criminal Records Information System on third-country nationals and stateless persons,
- Interoperability .

Supporting innovation (Title V)

Regulatory sandboxes Art. 53 and 54

Support for SMEs/start-ups Art. 55

Art. 54(1)(a)(i)

Further processing of personal data for development of AI systems for law enforcement purposes

European Commission

Next steps

- The European Parliament and the Council as co-legislators will negotiate the proposal and agree on a compromise in the ordinary legislative procedure

- Once adopted, there will be 2 years of transitional period before the **Regulation becomes directly applicable** across the EU.

- In parallel, **harmonized standards of CEN/CENELEC** should be ready and support operators in the practical implementation of the new rules& conformity assessment procedures

European Commission

Thank you