European Commission

SHAPING EUROPE'S DIGITAL FUTURE

Introduction to the Artificial Intelligence Act proposal

Gabriele Mazzini
DG CNECT, European Commission

CDDF Digital Tools and Artificial Intelligence Workshop
27 September 2021

Key regulatory concepts

Internal market legislation (mainly based on Art. 114 TFEU)

- "Classic" internal market rules for the **placing on the market and putting into service of** AI systems
- Aligned to vast EU acquis on product safety which shall be jointly applied (e.g. AI embedded in products)

Excluded: AI developed used exclusively for military purposes

Layered risk-based approach

- No regulation of the technology as such, but of **concrete high-risk use cases**
- Covers **risks to health, safety and fundamental rights**

Level playing field for EU and non-EU players

- Independent of origin of producer or user

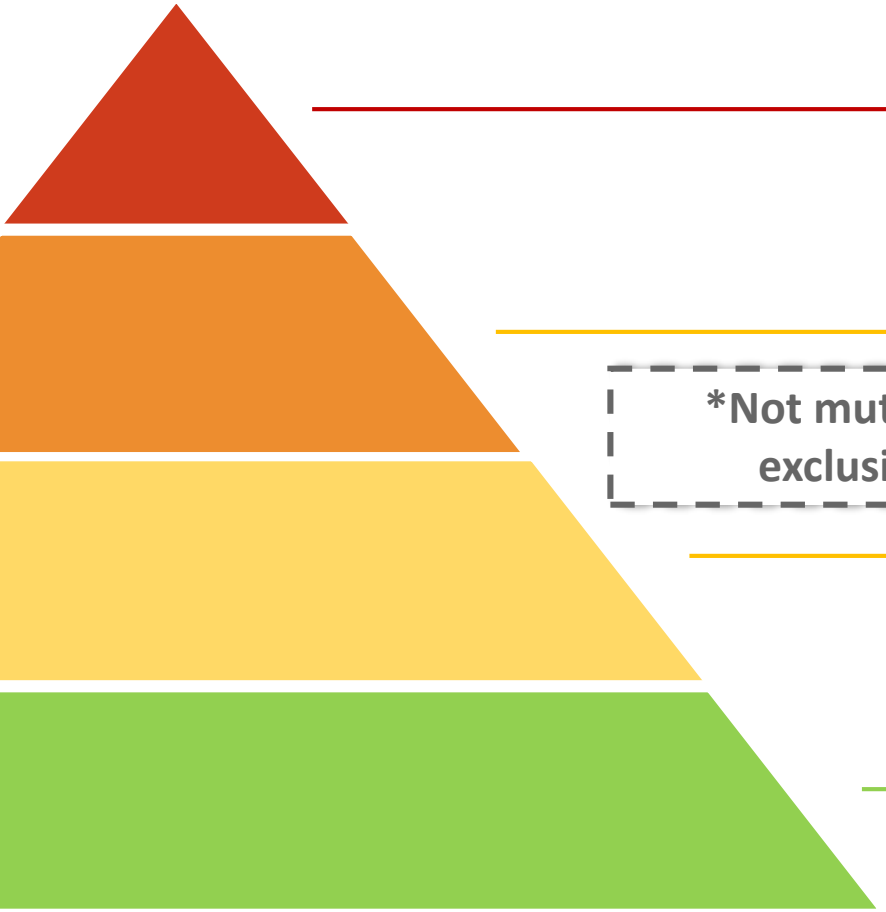
European Commission

Definition of Artificial Intelligence

> *"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"*

- 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 risk-based approach



*Not mutually exclusive

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

'Transparency' risk
'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)

Transparency obligations for certain AI systems (Art. 52)

- **Notify humans** that they are **interacting with an AI system** unless this is evident
- **Notify humans** that they are **exposed to emotional recognition or biometric categorisation systems**
- Apply **label to deep fakes**

Possible voluntary codes of conduct (Art. 69)

- No mandatory obligations
- Commission and Board to encourage drawing up of codes of conduct (**voluntary application of requirements for high-risk AI systems or other requirements)**

European Commission

High-risk Artificial Intelligence Systems (Title III, Chapter 1 & Annexes II and III)

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 AREAS

- ✓ 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

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

Establish and implement **risk management system**

&

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

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

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

CE marking = indication that product complies with requirements of applicable Union legislation

In order to affix a CE marking, 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 of AI systems are **in compliance with the AI Regulation**

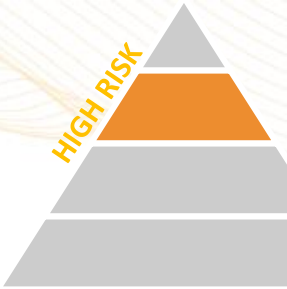
3 **Undergo conformity assessment procedure** to assess and demonstrate compliance

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

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



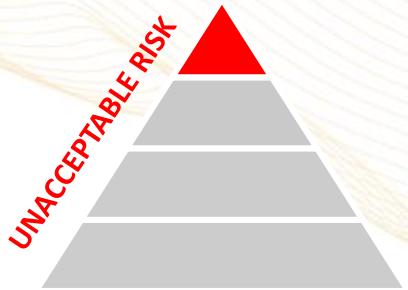
Provider obligations

- Establish and implement **quality management** system in its organisation
- **Register AI system** in EU database
- Conduct **post-market monitoring**
- **Collaborate** with market surveillance authorities

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)

AI that contradicts EU values is prohibited (Title II, Art. 5)



EXAMPLES

✗ **Subliminal manipulation** resulting in physical/ psychological harm

Extended Reality (XR) applications controlling the sensory experience of users

✗ **Exploitation of vulnerabilities** resulting in physical/psychological harm

Addictive AI-enabled applications intended for children (i.e., gambling-like random rewards or sending systematic push-notifications when 'off')

✗ **'Social scoring'** by public authorities

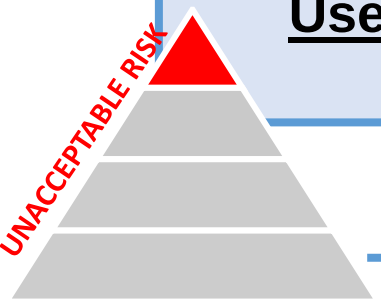
An AI system **identifies at-risk children** in need of social care **based on insignificant or irrelevant social 'misbehavior'** of parents, e.g. missing a doctor's appointment or divorce

✗ **'Real-time' remote biometric identification for law enforcement purposes in publicly accessible spaces** (with exceptions)

All faces in the town square captured live by cameras are **cross-checked, in real time,** against a **database of terrorists** held by the law enforcement agencies

European Commission

Remote biometric identification (RBI)



Use of real-time RBI systems for law enforcement (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

Putting on the market of RBI systems (real-time and ex-post)

- **Ex ante third party conformity assessment**
- Enhanced logging requirements
- "Four eyes" principle

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

The governance structure (Titles VI and VII)

European level

Artificial Intelligence Board

- National Supervisory Authorities
- EDPS
  - European Commission Secretariat

- Collect and **share best practices & expertise**
- Contribute to **uniform administrative practices** in the MS
- Provide **advice, opinions, recommendations** on AI issues:
  - Standards (including harmonized standards) & technical specifications
  - Preparation of guidance documents

National level

National Competent Authorities, incl. National Supervisory Authority

- Responsible for the application and implementation of the Regulation
  - Oversight of conformity assessment bodies
  - Market surveillance activities ex Regulation (EU) 2019/1020

Thank you

gabriele.mazzini@ec.europa.eu