

MACHINES WE TRUST

Perspectives on
Dependable AI

edited by Marcello Pelillo and Teresa Scantamburlo

MACHINES WE TRUST

Perspectives on
Dependable AI

edited by Marcello Pelillo and Teresa Scantamburlo

MACHINES WE TRUST

Perspectives on
Dependable AI

edited by Marcello Pelillo and Teresa Scantamburlo

DEFINING AI SYSTEMS

**FROM THE PERSPECTIVE OF
LAW AND THE RULE OF LAW**

Steels (focusing on 'intelligence' and history of AI):

- *Functional approach* (task oriented, focused on 'mental' tasks)
 - Three types of learning (data, transfer, experimentation)
 - But: shifting horizons, focus on 'human tasks', **testing, deceit**
- *Mechanistic approach* (circular definition, defined by 'AI' mechanisms)
 - Information processing, known AI algorithms (data-based, knowledge-based, behaviour-based)
 - But: shifting horizons (AI-CS), narrowing effects (e.g. DL)
- *Issue oriented approach* (properties of problems to be solved)
 - Tasks not amenable to be performed by standard algorithms
- **Complexity, epistemological, open task-environment, human-interaction**
 - But (Hildebrandt): shifting horizons, very narrow definition

Law and Rule of Law

- *Issue oriented approach*
 - *Disagreement within the domain*
 - *Who can speak 'for' AI: who should decide?*
 - *The providers, consultants and policy makers who have PR interests?*
 - *In science: the scientists*
- *In law: need for an impact oriented approach*
 - *In democracy (legislature): those who will be affected*
 - *Under the Rule of Law (courts):*
 - *who must be protected against what? who decides?*
 - *what values, rights, interests, public goods must be protected? who decides?*
- *Impact targeted by the AI Act:*
 - *Safety, health, fundamental rights*

The concept of Artificial Intelligence is a misnomer

- *Simon (1956): complex information processing*
- *MacCarthy (1956): we need to get funding*
- *A computing system used to solve problems may be all there is to it*
- *A computing system used to solve problems that cannot be solved by standard algorithms*
 - *That narrows down the field too much*
 - *We need protection against unwarranted claims, threats to safety and fundamental rights*
 - *Threats to safety health and fundamental rights also derive from less fancy software systems*

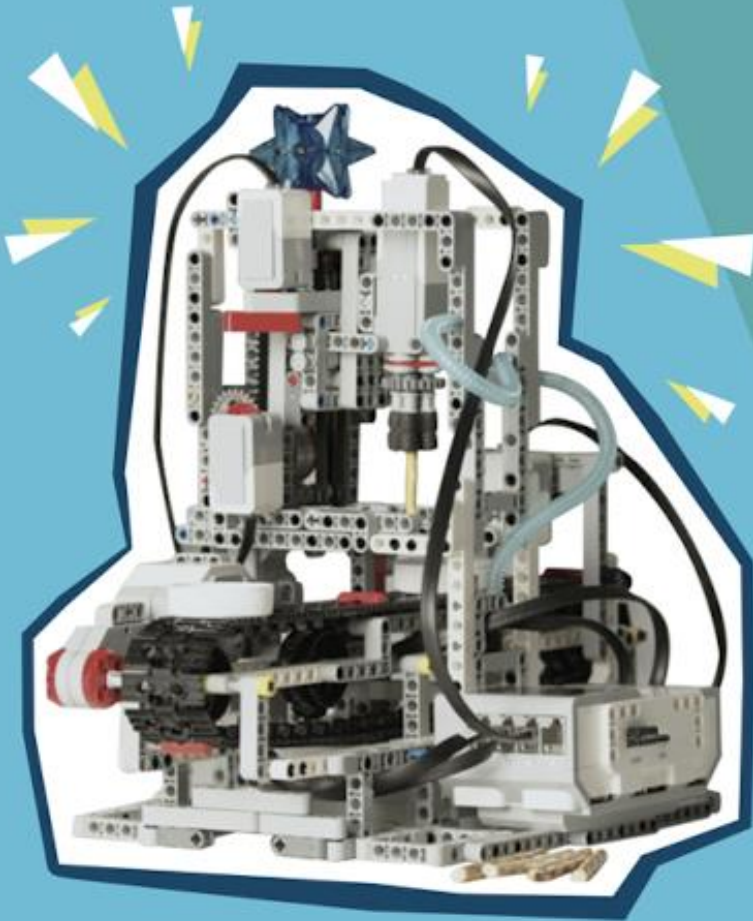
Develop a new term (will not solve any problem)?

- We need protection against software/products that use computing systems
 - made available with all kinds of claims
 - that have major impact on the real world
 - whether or not sold under the heading of AI
- That protection should consist of:
 - checking the substantiation of the claims
 - anticipation of threats to safety, health, fundamental rights
- That is what the Act does

See our new Working Paper on
Text-Driven Normativity and Legal Protection:

<https://publications.cohubicol.com/working-papers/text-driven-normativity/chapter-1/>

Why Rule of Law Matters – and How



**WHENEVER THE
CHALLENGE SEEMS
TOO COMPLEX,**

**JUST SHRINK
THE REALITY!**

SIEMENS ADVANTA

- For a map or a model to be useful the reality it wants to portray must be shrunk
- Maps or models do this by framing reality, such that one can:
 - navigate, control, influence, manipulate, act upon the reality it depicts
- Modelling can always be done in different ways (take google maps (2 perspectives), street view, google earth, upped with information on traffic, congestion, restaurants, museums etc.)
- The framing of reality is based on
 - assumptions and these have implications
 - intended purposes that drive the design of the model
- Different types of framing have different impacts
 - Due to whether assumptions fly or don't fly
 - In line with the **intended purpose** (which defines robustness, resilience, reliability)
 - Due to **potential misuse** (for other purposes than those intended, whose responsibility)

- The AIA demands that those who provide high risk AI systems:
 - Ensure that they are 4R AI systems in terms of the intended purpose
 - Which is closely aligned with the claimed functionality
 - 4R: robust, resilient, reliable and responsible
- The Act also demands that two types of risk are assessed, and prevented or mitigated:
 - Safety risks (including health) and risks of fundamental rights infringements
 - This regards both their potential use for:
 - The intended purpose
 - Reasonably foreseeable misuse

Reasonably foreseeable misuse:

- A hilariously and dangerously vague term?
- NO
- It is a very precise term
- If we were to make it more concrete:
 - It would be either overinclusive or underinclusive
- If we were to make it more abstract:
 - It would lose meaning
- It is these kinds of concepts ('reasonable') that
 - Ensure the adaptive nature of text-driven law
 - Require judgement rather than calculation
 - Enable protection of incompatible rights based on rule-based discretion
 - Rules as in Wittgenstein (use IRL)

What's up?

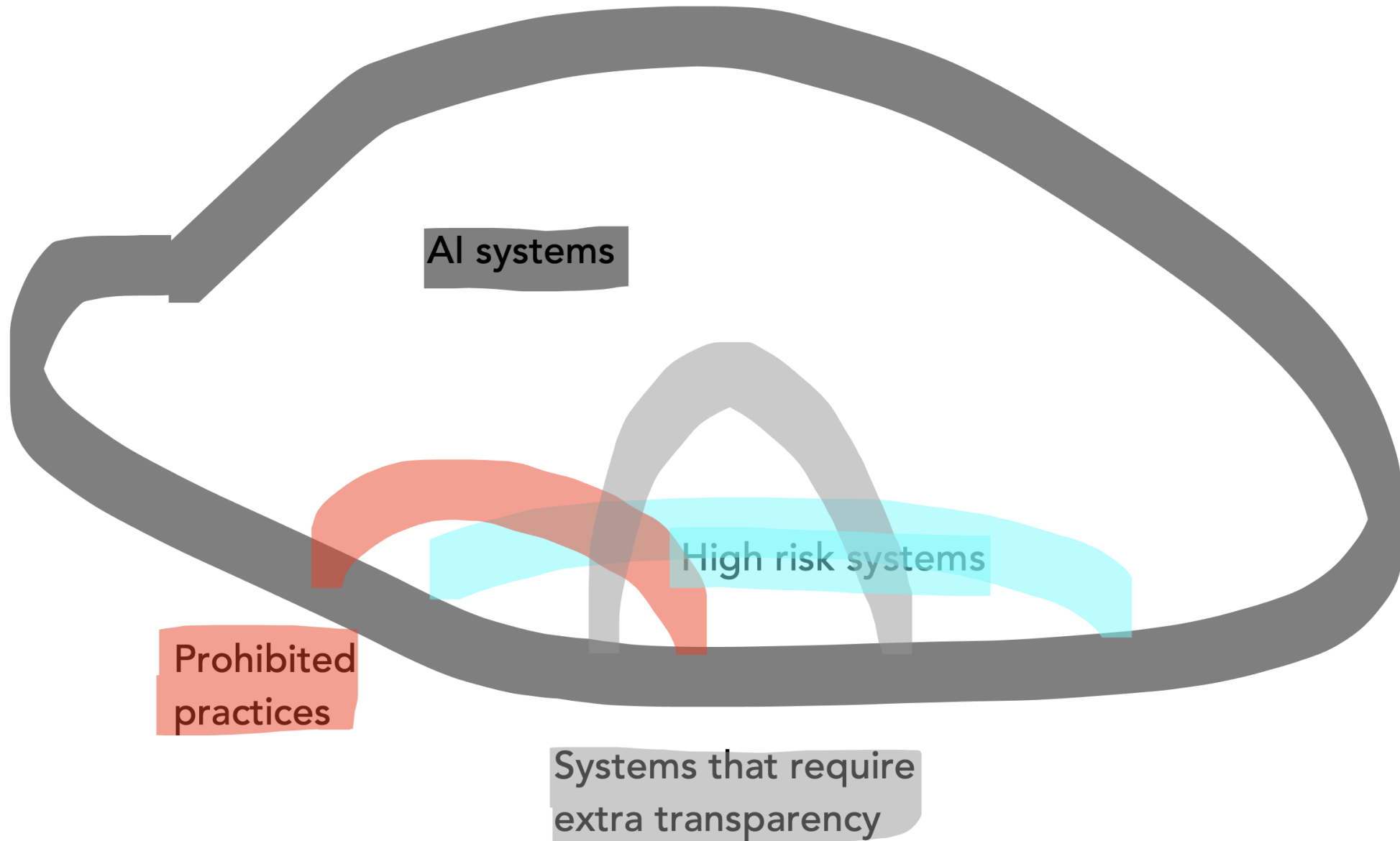
- The architecture of the Act
- Defining AI in the AI Act
- Details
- Connection with the GDPR

What's up?

- The architecture of the Act
- Defining AI in the AI Act
- Details
- Connection with the GDPR

Architecture of the Act

- **Applicable to**
 - AI systems (broad definition)
 - AI practices (narrowly defined)
 - High risk AI systems (rather narrowly defined)
- **Addressing providers, importers, distributors:**
 - Putting on the market (first making available on the market)
 - Making available on the market
 - Putting into service (supply for first use)
- **Addressing users (not end-users):**
 - Using
- **Prohibitions of 4 AI practices**
- **Requirements for high risk AI systems**
- **Transparency for 4 types of AI systems**
- **Conformity assessment for high risk:**
- **Risk assessment system, data and data governance, technical documentation, record keeping, transparency and information for users, human oversight, accuracy robustness and cybersecurity, quality management system**
- **Post market monitoring**



A risk-based approach to regulation (commission slide)



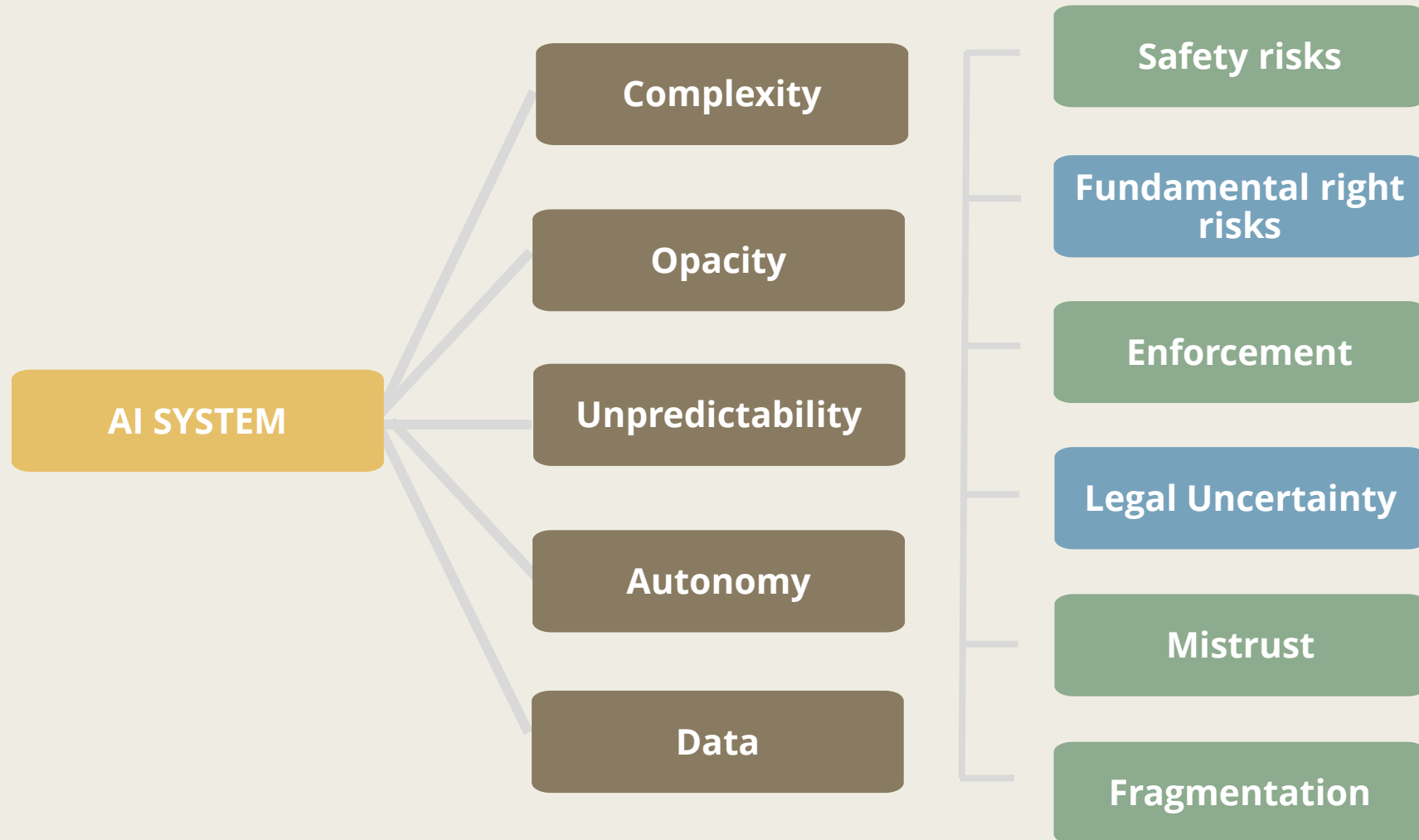
What's up?

- The architecture of the Act
- Defining AI in the AI Act
- Details
- Connection with the GDPR

Defining AI system

- Definition of AI system in art. 3(1):
 - 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;


Why do we regulate AI use cases? (commission slide)



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

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”

Software?

- Does the Act not apply to hardware?

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.

Software?

- Does the Act not apply to hardware?

Article 24 Obligations of product manufacturers

Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service **together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer**, the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider

Software?

- Does the Act not apply to *hardwired software*?
- Why shouldn't it? Software refers to computer code,
 - whether hardwired or not?
- Let's please not speak of:
 - 'algorithms' (overinclusive) or e.g.
 - 'autonomous systems' (underinclusive)

Developed with one or more of the techniques and approaches listed in Annex I

Annex 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.

Logic and knowledge-based approaches

This sounds to me like all rule-based software systems?

IMHO this implies that all (or almost all) software systems will be qualified as AI systems *if the other conditions apply*:

- an excel sheet (if used to interact with the environment)
- robot SPOT (also if remotely controlled)
- a thermostat that operates based on computer code (probably not high risk)

Human-defined objectives?

- This relates to the oft-used 'intended purpose' and highlights that AI systems must have an intended purpose
- Why? Because otherwise you cannot test its accuracy, reliability, safety etc.

Generates outputs (...) influencing the environments they interact with

- Good question: does an excel sheet interact with its environment?
- Good answer: it depends on how it has been integrated in a specific practice
 - If output supports decisions to reject social security application?
 - If output decides on such applications?
 - Much will depend on the meaning of 'interact'

Defining AI system

- Definition has a **broad scope** and is meant to provide **broad protection**
- It is not about what AI truly is (no metaphysical discussions on GAI or AGI)
- Note that only high risk, prohibited practices and 4 other types of systems are regulated – all AI systems as defined fall within the scope of the Act, but most are **not regulated (yet)**
- The discussion should be about:
 - whether **the right level of protection** has been implemented
 - depending on the qualification as prohibited, high risk or other

What's up?

- The architecture of the Act
- Defining AI in the AI Act
- Details
- Connection with the GDPR



DETAILS OF THE ACT

Roles Those addressed by the Act

- Provider: entity that **develops or has others develop** and AI system 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
- User: **using an AI system under its authority**, except where the AI system is used in the course of a **personal non-professional activity**
 - Also: importer, distributor, etc.

Layered approach

- **Prohibition AI practices:**
 - Manipulation or exploitation of vulnerable groups or individuals, social credit scoring by governments, remote real time biometric identification by police (with exceptions)
- **High risk AI systems**
 - Products or **safety** components of products regulated in Annex II
 - Standalone AI systems as defined in Annex III (focused on **fundamental rights**)
- **Transparency requirements for certain AI systems**
 - Systems interacting with natural persons
 - Emotion recognition systems
 - Biometric categorisation systems
 - Systems producing deepfakes
- An AI system may be high risk and nevertheless prohibited, if part of a prohibited practice
- An AI system may be due to special transparency requirements and also be high risk or even prohibited

Requirements for high risk AI systems

Risk management system (Art. 9)

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

Requirements for high risk AI systems

Risk management system (Art. 9)

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:

Requirements for high risk AI systems

Risk management system (Art. 9)

2. 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.

Requirements for high risk AI systems

Risk management system (Art. 9)

3. The risk management measures referred to in paragraph 2, point (d)
 - shall give due consideration to the **effects and possible interactions**
 - resulting from the combined application of the requirements set out in this Chapter 2.
 - They shall take into account **the generally acknowledged state of the art**,
 - including as reflected in relevant harmonised standards or common specifications.

Requirements for high risk AI systems

Risk management system (Art. 9)

4. The risk management measures referred to in paragraph 2, point (d)
 - shall be such that any residual risk associated with each hazard
 - as well as the overall residual risk of the high-risk AI systems
 - is judged acceptable,
 - provided that the high-risk AI system is used in accordance with its intended purpose
 - or under conditions of reasonably foreseeable misuse.
 - Those residual risks shall be communicated to the user.

Requirements for high risk AI systems

Risk management system (Art. 9)

4. In identifying the most appropriate risk management measures, the following shall be ensured:
 - a) **elimination or reduction of risks as far as possible through adequate design and development;**
 - b) where appropriate, implementation of **adequate mitigation and control measures** in relation to risks that cannot be eliminated;
 - c) **provision of adequate information** pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

In eliminating or reducing risks related to the use of the high-risk AI system,

- due consideration shall be given to the **technical knowledge, experience, education, training**
- to be expected by the user and
- the environment in which the system is intended to be used.

Requirements for high risk AI systems

Risk management system (Art. 9)

5. High-risk AI systems shall be tested for the purposes of
 - identifying the most appropriate risk management measures.
 - Testing shall ensure that high-risk AI systems perform consistently
 - for their intended purpose and
 - they are in compliance with the requirements set out in this Chapter.
6. Testing procedures shall be suitable to achieve the intended purpose of the AI system
 - and do not need to go beyond what is necessary to achieve that purpose.

Requirements for high risk AI systems

Risk management system (Art. 9)

7. The testing of the high-risk AI systems shall be performed,
 - as appropriate,
 - at any point in time throughout the development process, and,
 - in any event,
 - prior to the placing on the market or the putting into service.
- Testing shall be made against preliminarily defined metrics
 - and probabilistic thresholds
 - that are appropriate to the intended purpose of the high-risk AI system.

Requirements for high risk AI systems

Risk management system (Art. 9)

8. When implementing the risk management system described in paragraphs 1 to 7,
 - specific consideration shall be given to whether the high-risk AI system
 - is likely to be accessed by or have an impact on children.
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.

Requirements for high risk AI systems

Data and data governance (Art. 10)

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.

Requirements for high risk AI systems

Data and data governance (Art. 10)

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.

Requirements for high risk AI systems

Data and data governance (Art. 10)

3. Training, validation and testing data sets shall be
 - relevant, representative, free of errors and complete.
- They shall have the appropriate statistical properties,
 - including, where applicable,
 - as regards the persons or groups of persons on which the high-risk AI system is intended to be used.
- These characteristics of the data sets may be met
 - at the level of individual data sets
 - or a combination thereof.

Requirements for high risk AI systems

Data and data governance (Art. 10)

4. Training, validation and testing data sets shall take into account,
 - to the extent required by the intended purpose,
 - the characteristics or elements that are particular to
 - the **specific geographical, behavioural or functional setting**
 - within which the high-risk AI system is **intended to be used**.

Requirements for high risk AI systems

Data and data governance (Art. 10)

5. To the extent that it is strictly necessary
 - for the purposes of **ensuring bias monitoring, detection and correction**
 - in relation to the high-risk AI systems,
 - the providers of such systems **may process special categories of personal data** referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725,
 - subject to appropriate safeguards for the fundamental rights and freedoms of natural persons,
 - including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures,
 - such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

Requirements for high risk AI systems

Data and data governance (Art. 10)

6. Appropriate data governance and management practices shall apply
 - for the development of high-risk AI systems
 - other than those which make use of techniques involving the training of models
 - in order to ensure that those high-risk AI systems comply with paragraph 2.

Requirements for high risk AI systems

Transparency and provision of information to users (Art. 13)

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.

An appropriate type and degree of transparency shall be ensured,

- with a view to achieving compliance with
- the **relevant obligations of the user and of the provider**
- set out in Chapter 3 of this Title.

Requirements for high risk AI systems

Transparency and provision of information to users (Art. 13)

2. High-risk AI systems shall be accompanied by
 - instructions for use
 - in an appropriate digital format or otherwise
 - that include concise, complete, correct and clear information
 - that is relevant, accessible and comprehensible to users.

Requirements for high risk AI systems

Transparency and provision of information to users (Art. 13)

The information referred to in paragraph 2 shall specify:

- a. the **identity and the contact details of the provider** and, where applicable, of its authorised representative;
- b. the **characteristics, capabilities and limitations of performance** of the high-risk AI system, including: (...)
- c. the **changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment**, if any;
- d. the **human oversight measures referred to in Article 14**, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users;
- e. the **expected lifetime of the high-risk AI system and any necessary maintenance and care measures to ensure the proper functioning** of that AI system, including as regards software updates.

Requirements for high risk AI systems

Accuracy, robustness and cybersecurity (Art. 15)

1. High-risk AI systems shall be **designed and developed** in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and **perform consistently** in those respects throughout their lifecycle.
2. The **levels of accuracy and the relevant accuracy metrics** of high-risk AI systems shall be declared in the accompanying instructions of use.

Requirements for high risk AI systems

Accuracy, robustness and cybersecurity (Art. 15)

3. High-risk AI systems shall be **resilient** as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.

The **robustness** of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations (**'feedback loops'**) are duly addressed with appropriate mitigation measures.

Requirements for high risk AI systems

Accuracy, robustness and cybersecurity (Art. 15)

4. High-risk AI systems shall be **resilient** as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset (**'data poisoning'**), inputs designed to cause the model to make a mistake (**'adversarial examples'**), or model flaws.

In case of high risk systems

Obligations for providers (Art. 16)

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;

In case of high risk systems

Obligations for providers (Art. 16)

Providers of high-risk AI systems shall:

- 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.

In case of high risk systems

Quality management system (Art. 17)

1. Providers of high-risk AI systems shall put **a quality management system** in place **that ensures compliance with this Regulation**. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:
 - a. **a strategy for regulatory compliance**, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;
 - b. **techniques, procedures and systematic actions to be used for the design, design control and design verification** of the high-risk AI system;
 - c. **techniques, procedures and systematic actions to be used for the development, quality control and quality assurance** of the high-risk AI system;

In case of high risk systems

Quality management system (Art. 17)

- d. **examination, test and validation procedures** to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;
- e. **technical specifications, including standards**, to be applied and, where the relevant **harmonised standards** are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;
- f. **systems and procedures for data management**, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;

In case of high risk systems

Quality management system (Art. 17)

- g. the **risk management system** referred to in Article 9;
- h. the setting-up, implementation and maintenance of a **post-market monitoring system**, in accordance with Article 61;
- i. procedures related to the **reporting of serious incidents and of malfunctioning** in accordance with Article 62;
- j. **the handling of communication with national competent authorities, competent authorities**, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

In case of high risk systems Quality management system (Art. 17)

- k. **systems and procedures for record keeping** of all relevant documentation and information;
- l. **resource management**, including security of supply related measures;
- m. **an accountability framework** setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.

Obligations of users of high-risk systems (Art. 29)

1. Users of high-risk AI systems shall use such systems **in accordance with the instructions of use accompanying the systems**, pursuant to paragraphs 2 and 5.
2. The obligations in paragraph 1 are **without prejudice to** other user obligations under Union or national law and to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.
3. Without prejudice to paragraph 1, **to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.**

Obligations of users of high-risk systems (Art. 29)

4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system. They shall also inform the provider or distributor when they have identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system. In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.

For users that are credit institutions regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Obligations of users of high-risk systems (Art. 29)

5. Users of high-risk AI systems shall **keep the logs automatically generated by that high-risk AI system**, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law.

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

Obligations of users of high-risk systems (Art. 29)

6. Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.

What's up?

- The architecture of the Act
- Defining AI in the AI Act
- Details
- Connection with the GDPR

Connections with GDPR

- Often, ‘users’ of the AIA will be the ‘controllers’ of the GDPR
- Qualification of high risk systems under the AIA is predefined in the AIA
- Qualification as high risk to fundamental rights under the GDPR depends on an impact assessment (DPIA): more granular and flexible
 - Systems qualified as high risk in Annex III should be considered high risk in a DPIA?
- Qualification as high risk in AIA does not imply lawfulness, this will also depend on compliance with other legislation such as GDPR (recital 41 AIA)

Connections with GDPR

- The GDPR provides for a 'the **right to obtain human intervention** on the part of the controller, to express his or her point of view and to contest the decision' in the case of 'a decision based solely on **automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.
 - Only relevant for 'decisions'
- The AIA requires that 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'.
 - Also relevant for 'behaviour'

- See my feedback to the European Commission on the Act:

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662611_en