ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

INTRODUCTION TO THE AI ACT

AI for Judges

Giulia Lasagni

Senior Assistant Professor in Criminal Procedure

Summary

1. General overview
2. Prohibitions
3. High-risk AI systems
4. Low-risk AI systems (relevant to the criminal matter)
5. Scope
6. Transparency Obligations
7. Institutional framework and organization
8. Remedies
9. A new punitive enforcement system?
10. Which way forward?

AI definition

Art. 3 (1)

‘AI system’ means a machine-based system that is designed to operate with varying levels of **autonomy** and that may exhibit **adaptiveness** after deployment, and that, for explicit or implicit objectives, **infers**, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

AI – General approach

Recital (6)

AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.

01.

Structure:
General Overview of the Regulation

A preliminary issue….

Recital (8)

A Union legal framework laying down ***harmonised rules on AI*** *is therefore needed to* ***foster the development, use and uptake of AI*** *in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, including democracy, the rule of law and environmental protection as recognised and protected by Union law.*

A piece of legislation to (potentially) regulate all AI technology

→ Does it make any sense?

General overview - Structure

- Definition (Chapter I)
- Scope (Chapter I)
- Prohibited AI systems (Chapter II)
- High-risk AI systems (Chapter III)
- Transparency Obligations (Chapter IV)
- General Purpose AI Models (Chapter V)
- Measures in Support of innovation (Chapter VI)
- Governance (Chapter VII)
- EU Database for High-risk Ai Systems (Chapter VIII)
- Post-market Monitoring, Information Sharing and Market Surveillance (Chapter IX)
- Codes of Conducts and Guidelines (Chapter X)
- Delegation of Power and Committee Procedure (Chapter XI)
- Penalties (Chapter XII)
- Final Provisions (Chapter XIII)

General overview - Entry into force

→ 2 AUGUST 2026, however…

- Definition (Chapter I)
- Scope (Chapter I)
- Prohibited AI systems (Chapter II)

2/02/25

- High-risk AI systems (Chapter III) – SECTION 4 (Notifying authorities and notified bodies)

Art 6(1) : AI system is intended to be used as a safety component of a product or as a product → 2/08/2027

- Transparency Obligations (Chapter IV)
- General Purpose AI Models (Chapter V)
- Measures in Support of innovation (Chapter VI)
- Governance (Chapter VII)
- EU Database for High-risk Ai Systems (Chapter VIII)
- Post-market Monitoring, Information Sharing and Market Surveillance (Chapter IX)
- Codes of Conducts and Guidelines (Chapter X)
- Delegation of Power and Committee Procedure (Chapter XI)
- Penalties (Chapter XII) - but not Art 101 (Fines for providers of general-purpose AI models)
- Final Provisions (Chapter XIII)

…and Art 78 (Confidentiality)→ 2/08/2025

General overview - Risk based approach

Recital (26)

In order to introduce a proportionate and effective set of binding rules for AI systems, **a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate.** It is therefore necessary to prohibit certain unacceptable AI practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.

2019 *Ethic guidelines for trustworthy AI*, AI HLEG

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity
6. Non-discrimination and fairness
7. Social and environmental well-being and accountability

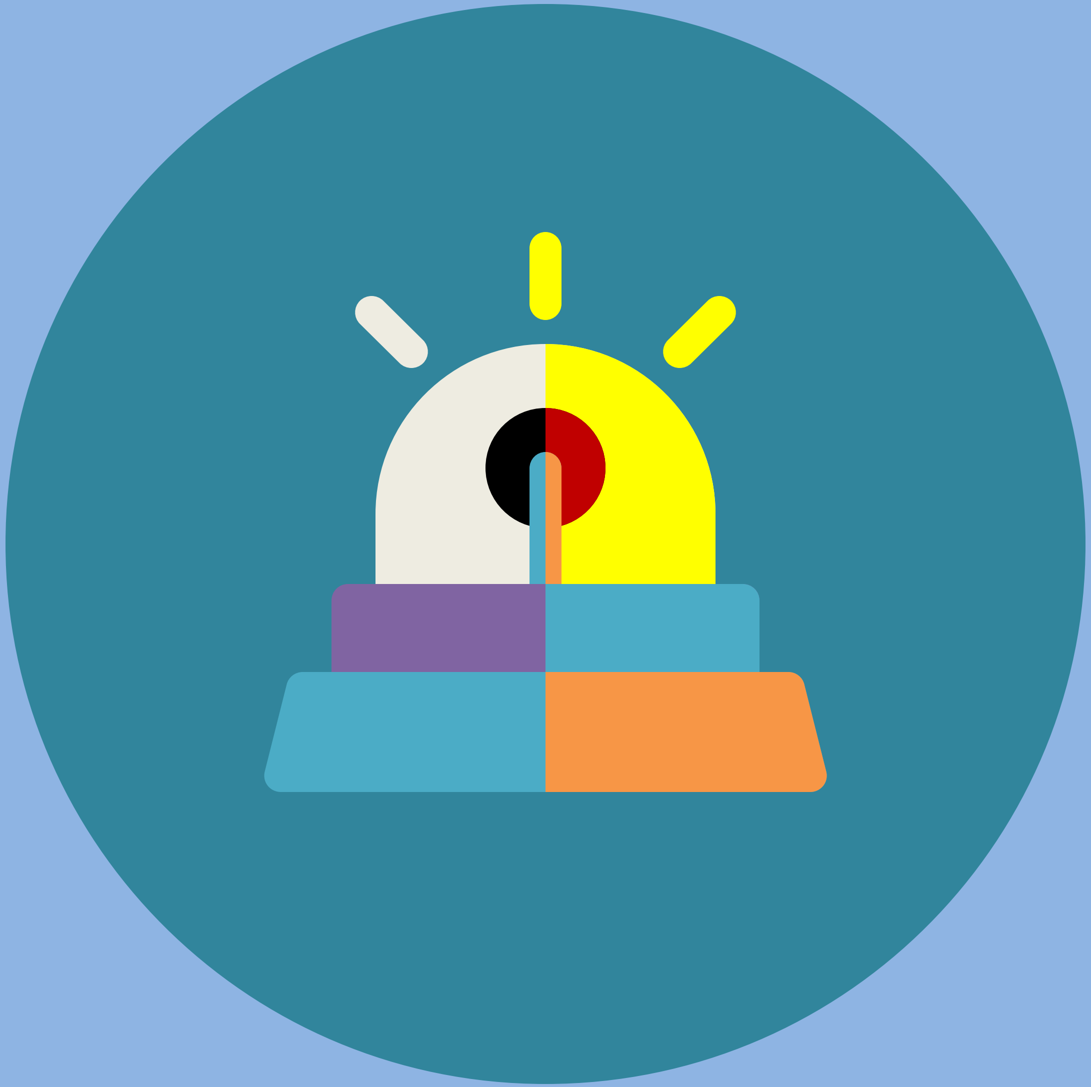
→ **No SOCIAL SCORING AND CONTROL** (Recitals 28-31)

General overview - Relation with LED Directive

Lex Specialis in respect to the rules on processing of biometric data in Article 10, LED

→The Regulation DOES NOT provide a legal basis for the processing of personal data ex art 8 LED (see also Recital (63))

→Need for national framework at MS level



02.

Prohibited AI systems

Prohibited AI Systems – Article 5

(a) the placing on the market, the putting into service or the use of an AI system that **deploys subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques**, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm; → deep fake?

(b) the placing on the market, the putting into service or the use of an AI system that **exploits any of the vulnerabilities of a natural person or a specific group of persons** due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

(c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, **with the social score** leading to either or both of the following: [...]

Prohibited AI Systems – Article 5 (continues)

(d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making **risk assessments** of natural persons in order to assess or predict the risk of a natural person **committing a criminal offence**, **based solely on the profiling** of a natural person **or on assessing their personality traits and characteristics**; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based **on objective and verifiable facts directly linked to a criminal activity;**

(e) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the **untargeted scraping of facial images from the internet or CCTV footage;** → *remembering Clearview…*

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to **infer emotions of a natural person in the areas of workplace and education institutions,** except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons; → *not as such, as in Recital (44)*

Prohibited AI Systems – Article 5 (continues)

(g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or **infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation**; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(h) the use of **'real-time' remote biometric identification systems in publicly accessible spaces** for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the objectives listed in the same provision.

Prohibited AI Systems – Some critical considerations

→ **By looking at the "specific" purpose**

What if the potential of the systems is however wider?

E.g. Facial recognition

(similar to Trojan viruses…)

→ Scope of the tools is not always so clear…

→ **Supporting human activity and taking an automated decision:** is it possible to really/always distinguish the two?

- Relevance of concrete circumstances (time, resources…)

→ **"objective and verifiable facts directly linked to a criminal activity"**

- Does "objective" make any sense in this context?
- Does it really matter, against the (usual) margin of discretion of the judge?

03.

High-risk AI systems

HIGH-RISK AI SYSTEMS – Article 6

For what concerns specifically the criminal matter → ANNEX 3

1. **Biometrics**, in so far as their use is permitted under relevant Union or national law:

(a) **remote biometric** identification systems.

This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;

(b) AI systems intended to be used for **biometric categorisation**, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

(c) AI systems intended to be used for **emotion recognition**

HIGH RISK AI SYSTEMS/2

6. Law enforcement, in so far as their use is permitted under relevant Union or national law:

(a) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf ***to assess the risk of a natural person becoming the victim of criminal offences;***
(b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies ***in support of law enforcement authorities as polygraphs or similar tools;***
(c) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities ***to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;***
(d) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for ***assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling*** of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, ***or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;***
(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies ***in support*** of law enforcement authorities ***for the profiling of natural persons*** as referred to in Article 3(4) of Directive (EU) 2016/680 ***in the course of the detection, investigation or prosecution of criminal offences***

HIGH RISK AI SYSTEMS/3

7. Migration, asylum and border control management, in so far as their use is permitted under relevant Union or national law:

(a) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies ***as polygraphs or similar tools***;
(b) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess ***a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory*** of a Member State;
(c) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assist competent public authorities for ***the examination of applications for asylum, visa or residence permits*** and for associated complaints with regard to the eligibility of the natural persons applying for a status, including ***related assessments of the reliability of evidence***;
(d) AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, in the context of migration, asylum or border control management, for the purpose of ***detecting, recognising or identifying natural persons, with the exception of the verification of travel documents***.

→ Recital (23) This Regulation should also apply to Union institutions, bodies, offices and agencies when acting as a provider or deployer of an AI system.

HIGH RISK AI SYSTEMS/4

8. Administration of justice and democratic processes:

(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in ***researching and interpreting facts and the law and in applying the law to a concrete set of facts,*** or to be used in a similar way in alternative dispute resolution

HIGH RISK AI SYSTEMS/5

However → **Not high-risk where the system does not pose a significant risk** of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making, ie where (alternative options)

(a) the AI system is intended to perform a ***narrow procedural task***;

(b) the AI system is intended to ***improve the result of a previously completed human activity***;

(c) the AI system is intended to ***detect decision-making patterns or deviations from prior decision-making patterns*** and is not meant to replace or influence the previously completed human assessment, without proper human review; or

(d) the AI system is intended to perform a ***preparatory task to an assessment*** relevant for the purposes of the use cases

→ *always, if profiling is involved*

HIGH RISK AI SYSTEMS/6

→ If in the list of Annex 3: exclusion shall be documented by the provider

'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge (Article 3(3)).

→ The list can be amended by the Commission in light of the parameters listed in Article 7:

HIGH RISK AI SYSTEMS/7

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

*(b) the extent to which an AI system has been used or is **likely to be used;***

*(c) the **nature and amount of the data** processed and used by the AI system, in particular whether special categories of personal data are processed;*

*(d) the extent to which the AI system **acts autonomously** and the **possibility for a human to override** a decision or recommendations that may lead to potential harm;*

*(e) the extent to which the use of an AI system **has already caused harm** to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;*

*(f) the **potential extent of such harm** or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons;*

*(g) the extent to which persons who are potentially harmed or suffer an adverse impact **are dependent on the outcome produced with an AI system,** in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;*

*(h) the extent to which **there is an imbalance of power**, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age;*

*(i) the extent to which the **outcome produced involving an AI system is easily corrigible or reversible**, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;*

*(j) the **magnitude and likelihood of benefit** of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;*

*(k) the extent to which existing Union law provides for: (i) **effective measures of redress** in relation to the risks posed by an AI system, with the exclusion of claims for damages;*

*(ii) **effective measures to prevent** or substantially minimise those risks.*

HIGH RISK AI SYSTEMS/8

If the system is considered High-risk, ***a series of obligation applies:***

1. Risk management system, to be regularly updated, also including testing in real-world conditions
2. Data governance and management practices appropriate for the intended purpose

   Recital (67) The data sets should also have ***the appropriate statistical properties, including as regards the persons or groups*** *of persons in relation to whom the high-risk AI system is intended to be used, with specific attention to the mitigation of possible biases in the data sets, that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination*

3. Technical documentation, to demonstrate the system complies with the requirements of high-risk
4. Record keeping (automatic recording of events over the lifetime of the system)
5. Transparency on the functioning of the system
6. Human oversight (Article 14)
7. Appropriate levels of accuracy, robustness and cybersecurity (lifecyc
8. Retention of automated generated logs

HIGH RISK AI SYSTEMS/9

Human oversight

Art 14(2). Human oversight shall aim to **prevent or minimise 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 where such risks persist despite the application of other requirements set out in this Section

(5). Biometrics → no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification **has been separately verified** and confirmed by **at least two natural persons** with the necessary competence, training and authority

→ *Is that possible/effective? Eg. the FRONTEX case*

… The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems **used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.**

HIGH RISK AI SYSTEMS/10

Human oversight/2

→ Innovative approach: BY DESIGN

Recital (73) and Article 14

High-risk AI systems ***should be designed and developed in such a way that natural persons can oversee their functioning***, ensure that they are used as intended and that their impacts are addressed over the system's lifecycle. To that end, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service.

…and **the natural persons** to whom human oversight has been assigned **have the necessary competence, training and authority to carry out that role.**

HIGH RISK AI SYSTEMS/11

- Providers are obliged to ensure compliance with the above requirements
- Have quality management systems in place to ensure compliance with the regulation
- Documentation keeping
- Duty to put in place timely corrective actions
- Cooperation duties with competent authorities

  → sanctions…

- Duty to establish representatives/Obligations of importers/obligations of distributors and along the AI chain/deployers → even if public authorities
- Registration in the EU database

HIGH RISK AI SYSTEMS/12

FUNDAMENTAL RIGHTS IMPACT ASSESSMENT:

(a) a description of the **deployer's processes** in which the high-risk AI system will be used in line with its intended purpose;

(b) a description of the **period of time** within which, and the **frequency** with which, each high-risk AI system is intended to be used;

(c) **the categories of natural persons and groups** likely to be affected by its use in the specific context;

(d) **the specific risks of harm** likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13;

(e) **a description of the implementation of human oversight measures**, according to the instructions for use;

(f) **the measures to be taken in the case of the materialisation of those risks**, including the arrangements for internal governance and complaint mechanisms.

HIGH RISK AI SYSTEMS/13

FUNDAMENTAL RIGHTS IMPACT ASSESSMENT (2):

→Privates **and** public bodies

→To be notified to the MARKET SURVEILLANCE AUTHORITY

‘market surveillance authority’ means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020

→Prior to deployment

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

HIGH RISK AI SYSTEMS/14

→Could/should these requirements be considered by the judicial authority to assess the validity of the used AI tool?

…A sort of *Daubert* test?

04.

Low-risk AI systems (relevant to the criminal matter)

Low risk AI systems

1. AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns

Recital (53) *The third condition should be that the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns. The risk would be lowered because the use of the AI system* ***follows a previously completed human assessment which it is not meant to replace or influence,*** *without proper human review. Such AI systems include for instance those that, given a* ***certain grading pattern of a teacher,*** *can be used to check ex post whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies.*

→ The French case in the administration of justice
→What about case-law analysis? Borderline…

Low risk AI systems/2

2. AI system is intended to perform a task that is only preparatory to an assessment relevant for the purposes of the AI systems

Recital (53) *The fourth condition should be that the AI system is intended to perform a task that is only preparatory to an assessment relevant for the purposes of the AI systems listed in an annex to this Regulation, thus making the possible impact of the output of the system very low in terms of representing a risk for the assessment to follow. That condition covers, inter alia, smart solutions for file handling, which include various functions* ***from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents.***

→ What about the EncroChat/SKY ECC case?
→ Or Digital forensics in general?

Low risk AI systems/3

Obligation (?) → Recital (53)

To ensure traceability and transparency, a provider who considers that an AI system is not high-risk on the ***basis of the conditions referred to above should draw up documentation of the assessment before that system is placed on the market or put into service and should provide that documentation to national competent authorities upon request.*** *Such a provider should be obliged to register the AI system in the EU database established under this Regulation. With a view to providing further guidance for the practical implementation of the conditions under which the AI systems listed in an annex to this Regulation are, on an exceptional basis, non-high-risk, the Commission should, after consulting the Board, provide guidelines specifying that practical implementation, completed by a comprehensive list of practical examples of use cases of AI systems that are high-risk and use cases that are not*

Low risk AI systems/4

3. (Recital 58)
AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services **and for prudential purposes** to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation

Recital (59) **AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of prevention, detection, investigation and prosecution of criminal offence**

05.

Scope

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

SCOPE OF APPLICATION

- No research and development activity (Recital 25)
- No IRELAND and DENMARK

SCOPE OF APPLICATION/2

No National security → Article 2(3)

This Regulation does not apply to areas outside the scope of Union law, and **shall not, in any event, affect the competences of the Member States concerning national security**, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.

This Regulation does not apply to AI systems **where and in so far they are placed on the market, put into service, or used with or without modification exclusively** for military, defence or **national security purposes**, regardless of the type of entity carrying out those activities.

This Regulation does not apply to AI systems **which are not placed on the market** or put into service in the Union, **where the output is used in the Union exclusively** for military, defence **or national security purposes,** regardless of the type of entity carrying out those activities.

Hybrid systems: Recital (24)

AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, **and** one or more non-excluded purposes, such as civilian purposes or law enforcement, **fall within the scope** of this Regulation and providers of those systems **should ensure compliance with this Regulation**.

In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out national security, defence and military activities, regardless of the type of entity carrying out those activities, to use AI systems for national security, military and defence purposes, the use of which is excluded from the scope of this Regulation.

An AI system placed on the market for civilian or law enforcement purposes which is used with or without modification for military, defence or national security purposes should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities (???)

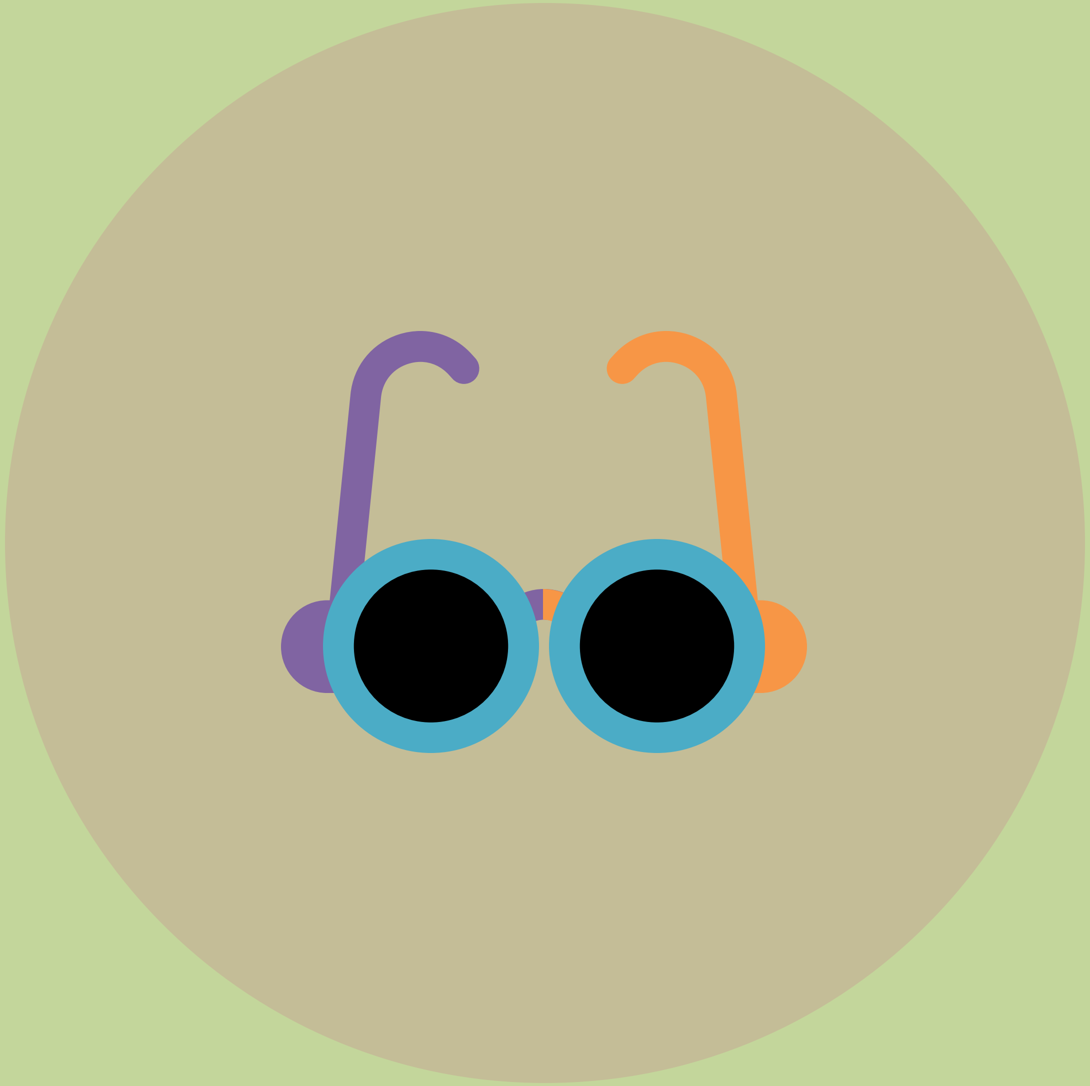
SCOPE OF APPLICATION/4

Article 3 (45) ‘law enforcement authority’ means:

(a) any public authority competent for the **prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties**, including the safeguarding against and the **prevention of threats to public security**; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the **prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security**

→ Overlapping and unclarity with regard to preventive “vs” repressive investigation
→ Need for Transnational Admissibility rules



06.

Transparency Obligations

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Transparency obligations

Article 50 – DEEP FAKE

1. Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned **are informed that they are interacting with an AI system**, unless this is obvious from the point of view of a natural person who is reasonably well informed, observant and circumspect, taking into account the circumstances and the context of use
2. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, **shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable** as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible → realistic? Evidence problem! Code of practice by the Commission

4. Deployers of an AI system that generates or manipulates image, audio or video content constituting a **deep fake, shall disclose that the content has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence**

07.

Institutional framework and organization

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Institutional framework and organization

A composite and multi-level system:

- **Market Surveillance Authorities**
- **EU AI Office** (Article 64)
- **Civil society:** relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations in conducting such impact assessments and designing measures to be taken in the case of materialisation of the risks
- **European AI Board** (Article 65) → facilitate the Regulation application
- **Advisory forum** (Article 67) → technical expertise
- **Scientific panel of independent experts** (Article 68)

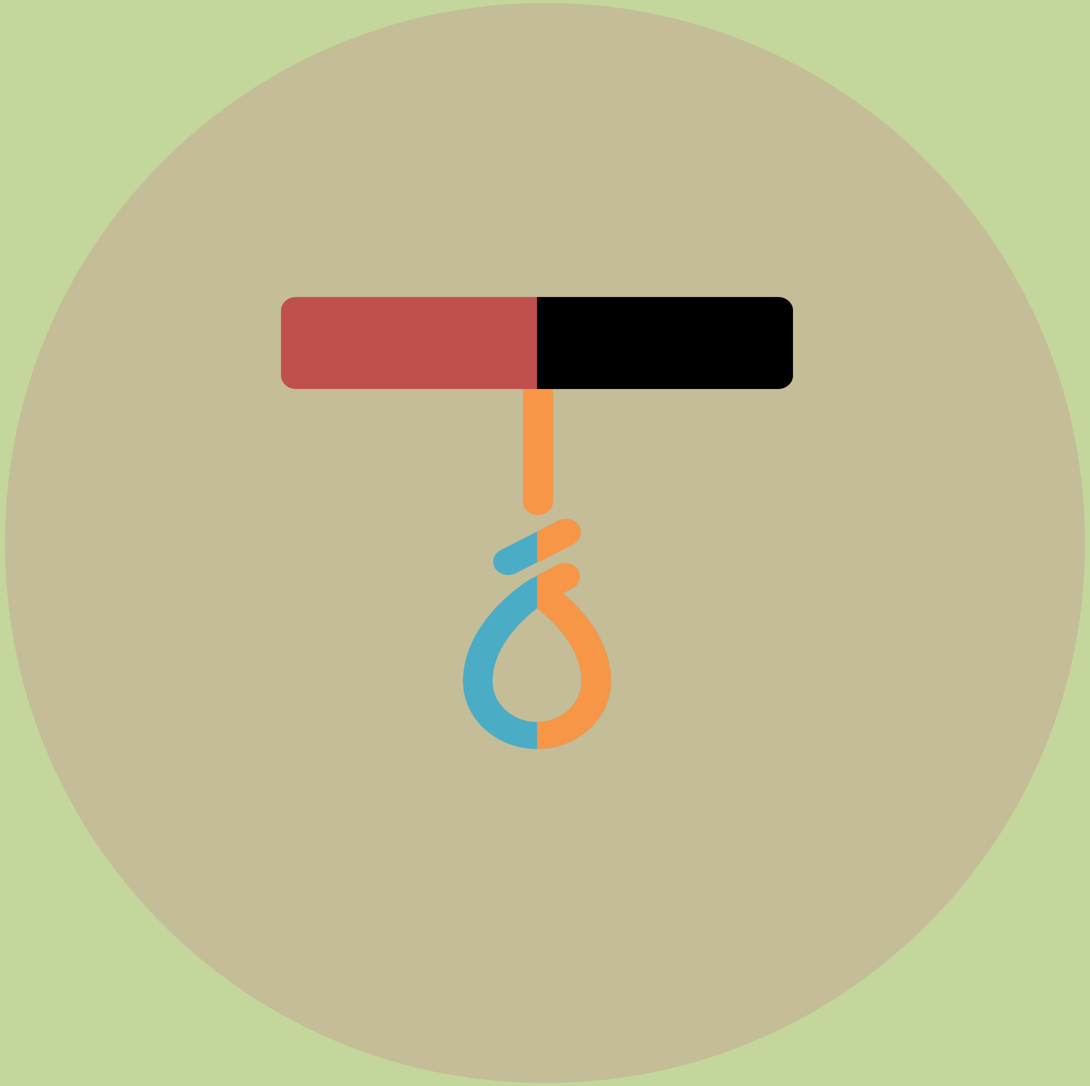
Institutional framework and organization/2

Each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of this Regulation (Recital (153)) → independent (Recital (159)).

Those competent authorities **should have all powers** under this Regulation and Regulation (EU) 2019/1020 to enforce the requirements and obligations of this Regulation, including powers to carry our ex post market surveillance activities that can be integrated, as appropriate, into their existing supervisory mechanisms and procedures under the relevant Union financial services law (Recital (158)).

Institutional framework and organization/3

→ At the EU level: The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation (Recital (165) and Article 74(9))



08.

A new punitive enforcement system?

A new punitive enforcement system?

Article 99
In accordance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties and other enforcement measures, which may also include **warnings and non-monetary measures**, applicable to infringements of this Regulation by operators, and shall take all measures necessary to ensure that they are properly and effectively implemented, thereby taking into account the guidelines issued by the Commission pursuant to Article 96. The penalties provided for **shall be effective, proportionate and dissuasive**. They shall take into account the interests of SMEs, including start-ups, and their economic viability

→Formally administrative…however…Engel doctrine

A new punitive enforcement system?/2

3. Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 35 000 000 or, if the offender is an undertaking, **up to 7 % of its total worldwide annual turnover** for the preceding financial year, whichever is higher

4. Non-compliance with any of the following provisions related to operators or notified bodies, other than those laid down in Articles 5, shall be subject to administrative fines of up to **EUR 15 000 000 or, if the offender is an undertaking, up to 3 % of its total worldwide annual turnover** for the preceding financial year, whichever is higher

A new punitive enforcement system?/3

7. When deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and, as appropriate, regard shall be given to the following:

(a) **the nature, gravity and duration of the infringement and of its consequences**, taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

…

(e) **any other aggravating or mitigating factor** applicable to the circumstances of the case, such as financial benefits gained,
or losses avoided, directly or indirectly, from the infringement;

(f) **the degree of cooperation** with the national competent authorities, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

…

A new punitive enforcement system?/4

5. The **supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request** shall be subject to administrative fines of up to EUR 7 500 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

→ CJEU, *DB v Consob*...

And what about **UNLIMITED JURISDICTION**?

→ Provided only with regard to fines for providers of general-purpose AI models (Article 101): WHY?

09.

Remedies

Remedies

Recital (171): Affected persons should have the **right to obtain an explanation where a deployer's decision is based mainly upon the output from certain high-risk AI systems** that fall within the scope of this Regulation and where that decision produces legal effects or similarly significantly affects those persons in a way that they consider to have an adverse impact on their health, safety or fundamental rights. That explanation should be clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights. The right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions follow from Union or national law and should apply only to the extent this right is not already provided for under Union law

Remedies/2

Article 86

1. Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

2. Paragraph 1 shall not apply to the use of **AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law.**

3. This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for under Union law

Remedies/3

EU Database
Article 71(1). The Commission shall, in collaboration with the Member States, set up and maintain an EU database **containing information** referred to in paragraphs 2 and 3 of this Article **concerning high-risk AI systems**

The information contained in the EU database … shall be accessible and publicly available in a user-friendly manner. The information should be easily navigable and machine-readable→ **BUT: Exception for**
high-risk AI systems referred to in points 1, 6 and 7 of Annex III, in the areas of law enforcement, migration,
asylum and border control management

Remedies/4

→ the registration referred to … **shall be in a secure non-public section of the EU database …Only the Commission and national authorities** referred to in Article 74(8) shall have access to the respective restricted sections of the EU database

→ *What about defence lawyers?*

→ *Need for a new form of the RTBH? Mediated right?*

Remedies/5

Article 74(12)and (13)

Without prejudice to the powers provided for under Regulation (EU) 2019/1020, and where relevant and limited to
what is necessary to fulfil their tasks**, the market surveillance authorities shall be granted full access by providers to the documentation as well as the training, validation and testing data sets used for the development of high-risk AI sys**tems, including, where appropriate and subject to security safeguards, through application programming interfaces (API) or other relevant technical means and tools enabling remote access.

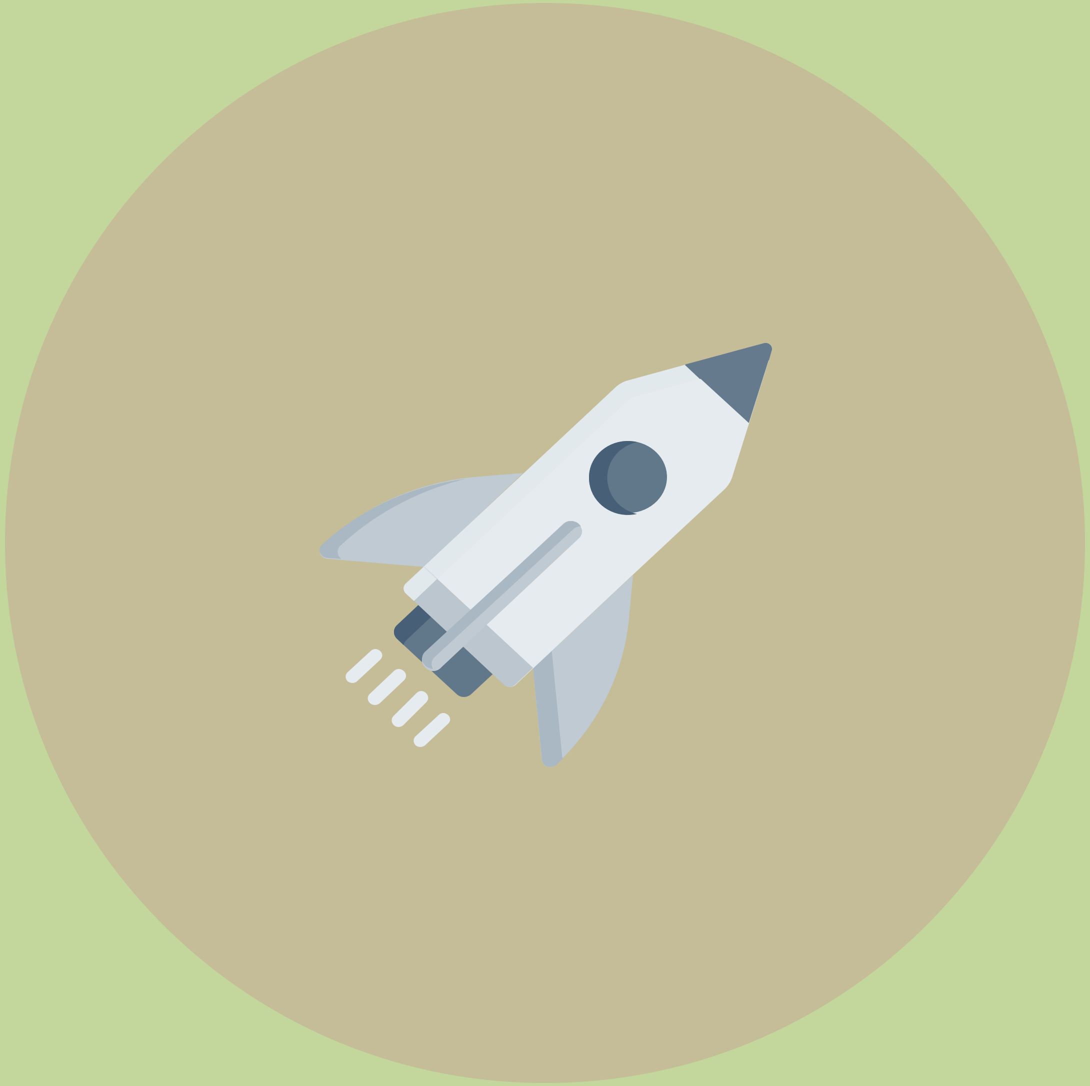
13. Market surveillance authorities shall be granted access **to the source code of the high-risk AI system** upon a reasoned request and only when both of the following conditions are fulfilled:
(a) access to source code **is necessary to assess the conformity of a high-risk AI system** with the requirements set out in Chapter III, Section 2; and (b) testing or auditing procedures and verifications based on the data and documentation provided by the provider **have been exhausted or proved insufficient.**

→ Eg EncroChat case?

Remedies

Article 78 (3)
When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in point 1, 6 or 7 of Annex III, the technical documentation referred to in Annex IV **shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities** referred to in Article 74(8) and (9), as applicable, can, **upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed** to access that documentation or any copy thereof.

Article 79(9)
The market surveillance authorities shall ensure that **appropriate restrictive measures** are taken in respect of the product or the AI system concerned, such as withdrawal of the product or the AI system from their market, without undue delay.



10.

Which way forward?

WHICH WAY FORWARD?

1. *As usual, much will depend on its practical implementation, however…*

→ *Most systems in place are not looking like they are in compliance with the procedural requirements: Positive aspect*

Although: **Article 111(2)**

In any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps to comply with the requirements and obligations of this Regulation by **2 August 2030.**

WHICH WAY FORWARD?

2. A new (?) model of RTBH

Using independent authorities as a neutral intermediate

Already emerging in other fields of law, where link with privacy rights is at stake

WHICH WAY FORWARD?

3. Training, training, training…!!!

Recital (20)
In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI system

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Thank you for the attention!

Giulia Lasagni

giulia.lasagni6@unibo.it