LINKSFOUNDATION.COM

FONDAZIONE links
PASSION FOR INNOVATION

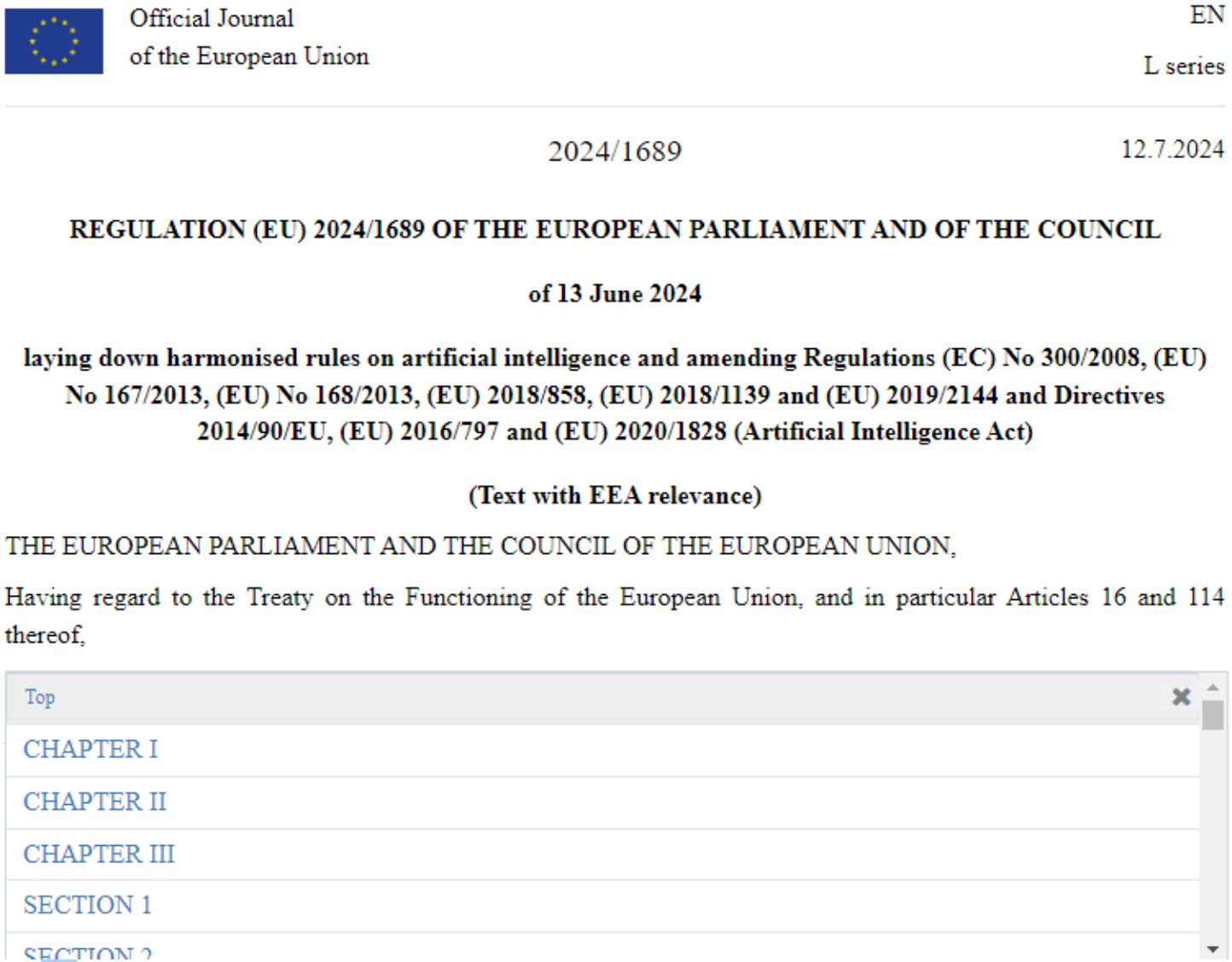
Applied Data Science Project

Politecnico di Torino

L7 – AI Ethics

ellis
European Laboratory for Learning and Intelligent Systems

The European Artificial Intelligence Act (AIA)



Official Journal
of the European Union

EN

L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Top

CHAPTER I

CHAPTER II

CHAPTER III

SECTION 1

SECTION 2

Regulatory framework:
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Why do we need an act to regulate AI in EU?

“Ensures that Europeans can trust what AI has to offer.

While most AI systems pose limited to no risk and can contribute to solving many societal challenges, **certain AI systems create risks that we must address to avoid undesirable outcomes”**

For instance, it’s not obvious tracking down how a decision has been made from a digital support.

It is necessary to preventing disadvantages, discrimination

A future-proof AI

according the EC

European Commission is working to promote a modern AI, able to respond and comply with **people-defined goals** (**Human Centred**) and is **aware of the impacts** on physical and digital environments.

Some **current** intrinsic features of AI systems are at the core of this goal:

OPACITY

- Of systems not providing users or affected parties any insight as to **how they came to produce the results**.
  AI algorithms can be opaque even when they are reliable

(Vaassen, B. 2022)

COMPLEXITY

- resulting from many different interacting aspects, parts, or functions, which cannot be easily described, analyzed, or predicted because of its intricacy and internal interactions. Over the “known unknows” (expected potential drawbacks), complexity implies the “**unknown unknowns”, challenges whose existence we are not aware of.**

(Pawson, Wong, and Owen 2011)

DATA DEPENDENCE

- Bias can be manifested in **multimodal data** through **sensitive features** and their **causal influences**, or through under/over-representation of certain groups.

AUTONOMY

- Of systems operating independently of human guidance, for a fixed goal (or “utility function”) with respect to which the appropriateness of actions will be evaluated.

(Ntouts, E et al. 2020)

The Artificial Intelligence Act (AIA)

The **first ever** legal framework on AI

The act expresses the **political commitment** to apply a **coordinated approach** to AI and **aware of the human and ethical implications**.

Four specific objectives:

- ensure that AI systems placed on the Union market and used are **safe** and respect existing **laws on fundamental rights** and **Union values**
- ensure **legal certainty to facilitate investment** and innovation in AI
- enhance governance and safety requirements applicable to AI systems
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and **prevent market fragmentation**.

https://artificialintelligenceact.eu/high-level-summary/

AI Act

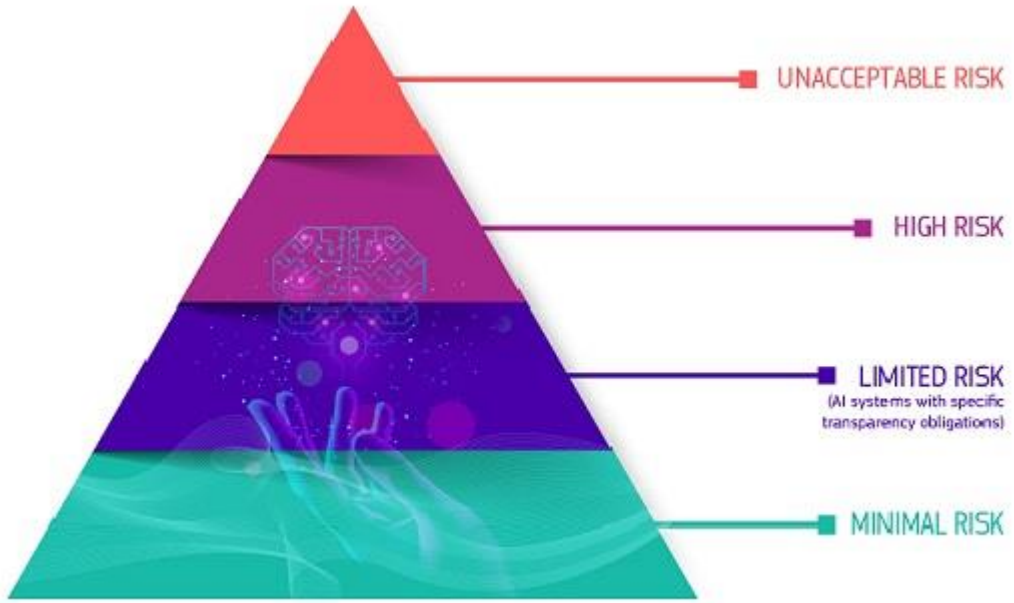
Key points:

- **Human** centric
- **Risk** based
- **EU Value** oriented

Considered risks:
Erroneous or distorted decisions suggested or supported by AI in critical areas, where there is a high risk to harm health, safety and human fundamental rights.

Risks: known, foreseeable, emerging, residual (associated with hazards)

Risks



Unacceptable applications

Systems violating human rights, persons assessment or classifications, subliminal techniques, real-time biometric identification systems)

High risk applications

- Systems for traffic and mobility control
- Water and electrical systems
- Education (evaluation of people)
- Work and access to work
- Access Systems to Public Services (credit score or creditworthiness)
- Law enforcement systems
- Migration and national borders
- Systems related to the administration of Justice
- Health-related applicatiosn
- Real-time and post-hoc remote biometric identification systems

Limited risk applications

Administrative proceedings

Minimal risk applications

AI-enabled games or spam filters

Requirements and obligations

Mandatory requirements for high-risk AI systems:

- High quality data (adequate statistical properties)
- **Documentation** (also for the end users)
- **Transparency** clear information for users
- **Human Oversight**
  - Interpretability
  - Minimize the risks of excessive trust (delegation)
- **Accuracy and robustness** (errors, defects, inconsistencies, unforeseen problems)

+ **cybersecurity** (addressing also the end users)

Obligations of providers

- Implement a **risk management system** that 1) identifies and analyses 2) estimates 3) manages known, foreseeable, emerging, residual risks
  - Guarantee an **effective communication** to the end-users
- Implementing a **quality management system**
  - **Data governance** including relevant, complete and free of errors training, validation and testing data sets (appropriate statistical properties)
  - **Bias monitoring**
- Provide **technical documentation**
- Automatically record the **logs**
- Carry out the **compliance assessment**
- Interface with **national authorities** and comply with legal obligations
- Should apply the **CE mark**

Roles and responsabilities: AI providers

Providers: developers and manufacturers

Main responsibility for ensuring their systems comply with the AI Act. Key checks:

- Conformity Assessment: to ensure that high-risk AI systems comply with all the legal requirements before they can be marketed or deployed. This includes conducting thorough testing and validation to meet safety, transparency, and robustness standards

- Documentation: to maintain technical documentation and records of the AI system. This includes providing details on how the system was trained, its intended uses, data governance policies, and compliance with risk mitigation measures

Roles and responsabilities: AI providers (II)

- Risk Management: to identify risks associated with their AI systems and taking steps to mitigate those risks throughout the lifecycle of the AI. This includes pre-market risk assessment and ongoing monitoring during deployment

- Transparency: for high-risk AI systems, to provide users with clear instructions, usage limitations, and warnings about the AI system's capabilities and risks. This is especially important in applications that can affect safety or fundamental rights

- Post-Market Monitoring: aven after an AI system is deployed, to establish systems for ongoing performance monitoring. They are required to report any malfunctions, unforeseen risks, or failures to comply with AI Act provisions to the authorities

- CE Marking: to ensure the AI system complies with the AI Act by undergoing a conformity assessment and obtaining CE marking, which certificate that the system adheres to EU standards

Roles and responsabilities: AI users (I)

Users: organizations using AI Systems

Participate in the responsibility of the value chain because they will have users of. Key checks:

- Ensure proper use: to operate AI within the prescribed safety and performance parameters as defined by the provider. Misuse or deviation from intended functionality could expose users to legal risks

- Human Oversight: humans should be able to intervene or override AI decisions in critical situations, especially in sectors like healthcare, justice, and transportation

Roles and responsabilities: AI users (II)

- Monitoring Performance: to monitor the performance of AI systems during operation and report any unexpected issues, errors, or risks that arise. This ensures that if problems occur after deployment, they are flagged for further action by providers or regulator

- Data Input Management: if requested, data fed into the AI system is accurate, unbiased, and appropriate for the intended purpose. The quality of data impacts the fairness and reliability of AI outputs, particularly in high-risk systems

Roles and responsabilities: Distributers and importers

To ensure that the systems they place on the market comply with the AI Act

- Verification of Compliance: verify that AI meet all conformity assessment requirements before they can be sold or distributed, and AI has the CE marking
- Record Keeping: keep records of the AI systems they distribute and assist in providing information to regulatory authorities
- Collaboration with providers: to ensure that any post-market monitoring data or issues raised by users are reported to the proper authorities

Roles and responsabilities: National Competent Authorities

Users: mainly regulators

To enforce the AI Act

- Monitoring Compliance: will monitor the market to ensure that AI systems meet the regulatory standards. Will conduct audits, inspections, and random checks on high-risk AI systems to verify compliance

- Handling Complaints: will enforce penalties for non-compliance. This can include fines and restrictions on the use or sale of non-compliant AI systems

- Collaboration with providers: will serve as points of contact for users, consumers, and third parties to report any concerns or grievances regarding AI systems. They will investigate complaints related to potential harms, malfunctions, or breaches of fundamental rights

- Market surveillance and auditing: will actively perform post-market surveillance and audits of AI systems, particularly those classified as high-risk. They will ensure that AI systems remain compliant with evolving standards and act when violations occur.

Roles and responsabilities: Notified bodies

Independent organizations designated by member states to assess conformity of AI systems, particularly for high-risk applications, usually auditors

- Conformity Assessments: will evaluate the safety and robustness of high-risk AI systems and ensure they comply with the technical and legal requirements outlined in the AI Act

- Handling Complaints: will provide certificates that enable AI providers to affix the CE marking to their products, indicating conformity with EU rules.

Roles and responsabilities: EU-level Oversight

The EU-wide oversight will be managed by a new European Artificial Intelligence Board (EAIB)

- Policy Harmonization: will coordinate and harmonize the implementation of the AI Act across member states to ensure a unified approach to regulation
- Advisory Role: will advise the European Commission on updates and adjustments to the AI Act to reflect technological advancements and societal impacts
- Cross-border Collaboration: will ensure cross-border enforcement of the AI Act, facilitating cooperation between national authorities for the handling of transnational AI issues

Impacts of the AI Act

DEVELOPERS Increased accountability, testing and documentation	BUSINESSES Challenges and opportunities in AI deployment
CONSUMERS Improved trust and protections	SOCIETY Balancing regulation with fostering a competitive AI ecosystem

Comparison with Global AI Regulations

Right now, US and China are discussing about AI regulations and developing ethical considerations

The EU AI Act, right now, is the first attempt worldwide to regulate the sector

This opens some opportunities for the Act to become a reference point for similar actions worldwide

FONDAZIONE links

PASSION FOR INNOVATION

Thank you for your attention.

Questions?

CONTACTS

Giuseppe Rizzo

Program Manager (LINKS Foundation) and
Adjunct Professor (Politecnico di Torino)

giuseppe.rizzo@polito.it

FONDAZIONE LINKS
Via Pier Carlo Boggio 61 | 10138 Torino
P. +39 011 22 76 150
LINKSFOUNDATION.COM