CELTIC-NEXT
eureka Cluster

The path to AI-Act

Diogo Gomes <dgomes@ua.pt>
Mário Antunes <mario.antunes@ua.pt>

Research Summit
Universidade de Aveiro, 2025

universidade de aveiro

instituto de telecomunicações

What is the EU AI Act ?

- First comprehensive **AI regulatory framework**
- Balances innovation with fundamental rights and safety

- Work started in 2020
- Approved 2024
- Fully applicable 2026

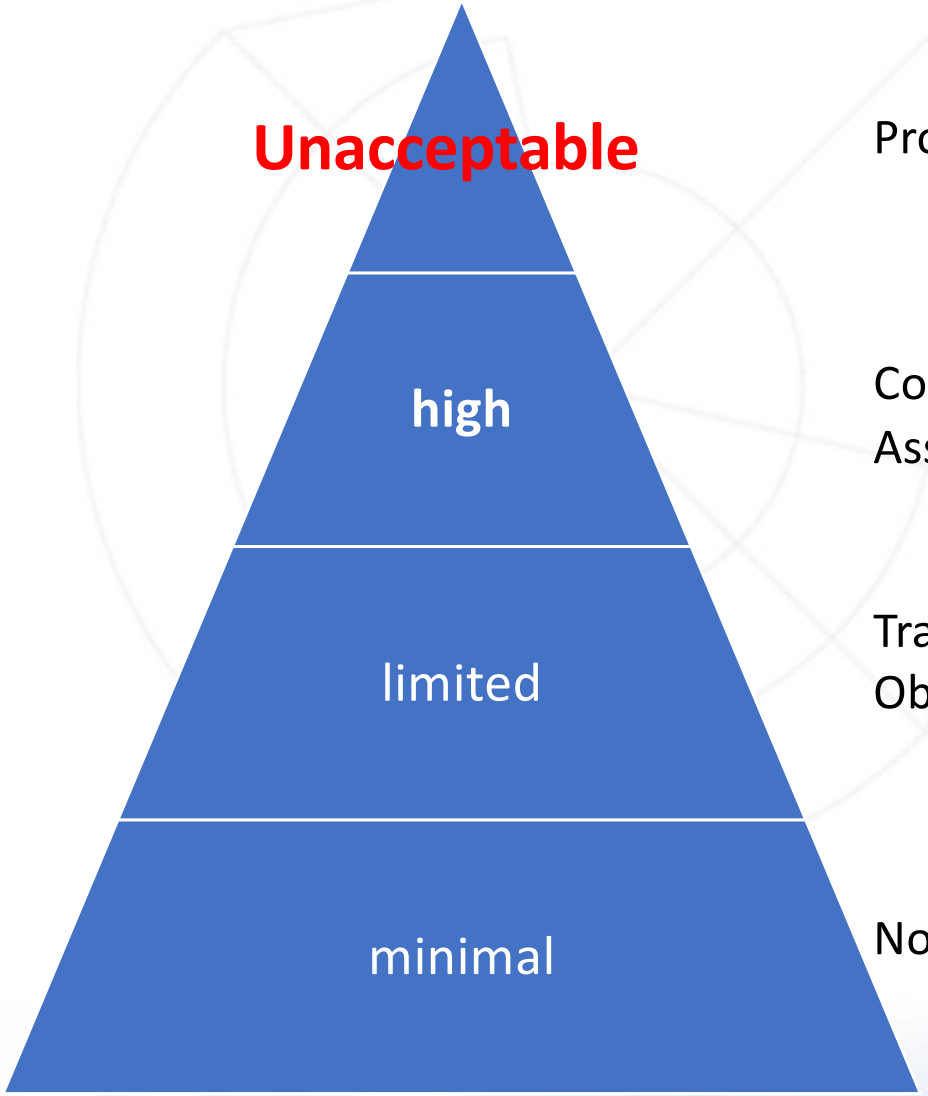
Risk-based framework

Unacceptable risk: Prohibited (e.g., social scoring).

High-risk: Strict obligations (e.g., medical devices, critical infrastructure).

Limited risk: Transparency obligations (e.g., chatbots).

Minimal risk: Free use (e.g., spam filters).



1. Biometrics and biometrics-based systems
2. Management of critical infrastructure, like road, water, gas, electricity and the internet
3. Educational and vocational training
4. Employment, workers management and access to self-employment tools
5. Access to public and private services, which include life and health insurance
6. Law enforcement
7. Migration, asylum and border control management tools, and
8. Administration of justice and democratic processes, which includes AI systems intended to be used for influencing elections, and recommendation engines of Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs), as defined by the Digital Services Act (DSA)

High-Risk AI

Key Requirements:

Transparency and Explainability: Providing clear insights into how AI models make decisions.

Record-keeping & Auditability: Maintaining detailed logs and documentation for regulatory compliance and post-market monitoring.

The Act is a catalyst for **embedding explainability and auditability** as core principles of AI development and deployment.

Infographic source: https://www.holisticai.com/blog/requirements-for-high-risk-ai-applications-overview-of-regulations

AI Act in Telecom

- Chatbot providing costumer support (**limited risk**)
  - Requires transparency

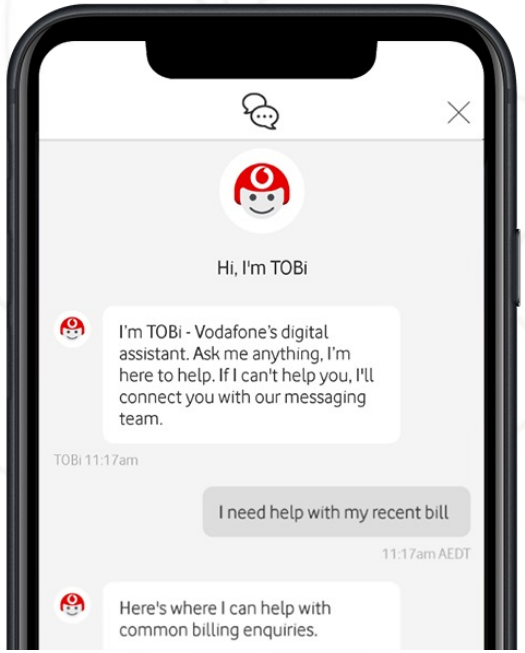
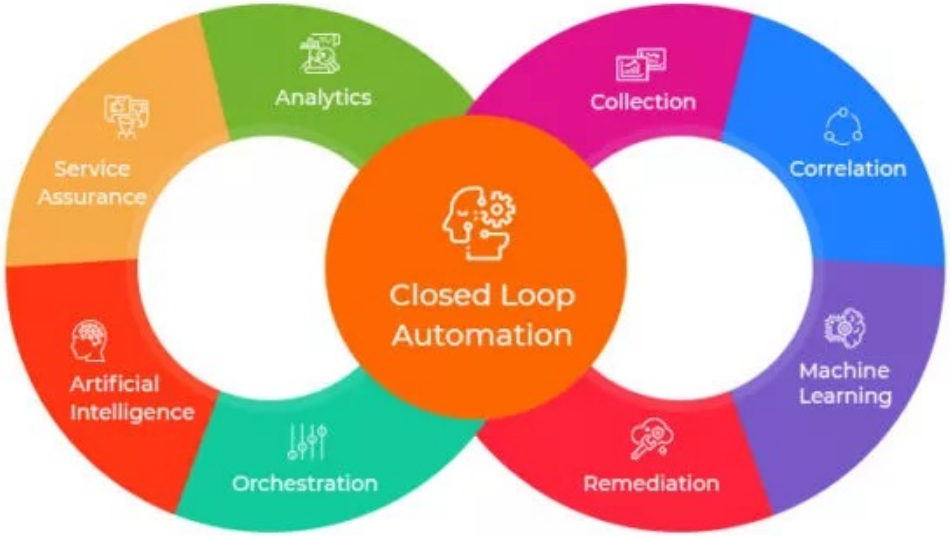


Image source: http://Vodafone.pt

AI Act in Telecom

- AI is used to manage the lifecycle of the network services (**high risk**)
- Communication Networks are **critical Infrastructures**

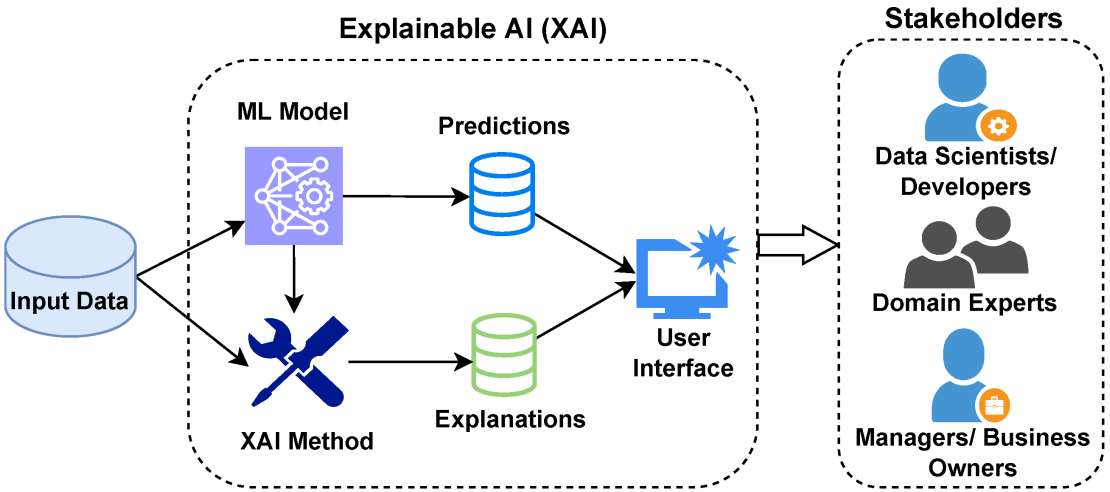


- **How to address AI-Act ?**

Image source: https://www.anutanetworks.com/5-real-world-use-cases-of-closed-loop-automation/

Explainable AI (XAI)

XAI are a collection of methods and techniques designed to make AI systems more comprehensible and interpretable to humans.



- **Transparency:** Revealing the internal logic and design of AI models.
- **Interpretability:** Explaining specific predictions or overall model behaviour in understandable terms.
- **Trust:** Building confidence among users, developers, and regulators.
- **Fairness:** Identifying and mitigating biases by understanding their origins.
- **Accountability:** Attributing AI decisions to their underlying reasons, enabling oversight.

Image Source: https://python.plainenglish.io/transform-your-world-with-8-revolutionary-types-of-ai-multimodal-agentic-shadow-ethical-8858e8764c5a

Federated Learning (FL)

AI Act Concern	FL Contribution
Data Governance & Privacy	Data remains local → reduces risk of data breaches and improves GDPR compliance.
Bias & Fairness	Local training can incorporate diverse contexts, reducing centralized data bias.
Transparency & Accountability	Training logs and model updates can be monitored at the edge → better traceability.
Security	Limits exposure of raw data → minimizes attack surface for adversarial threats.

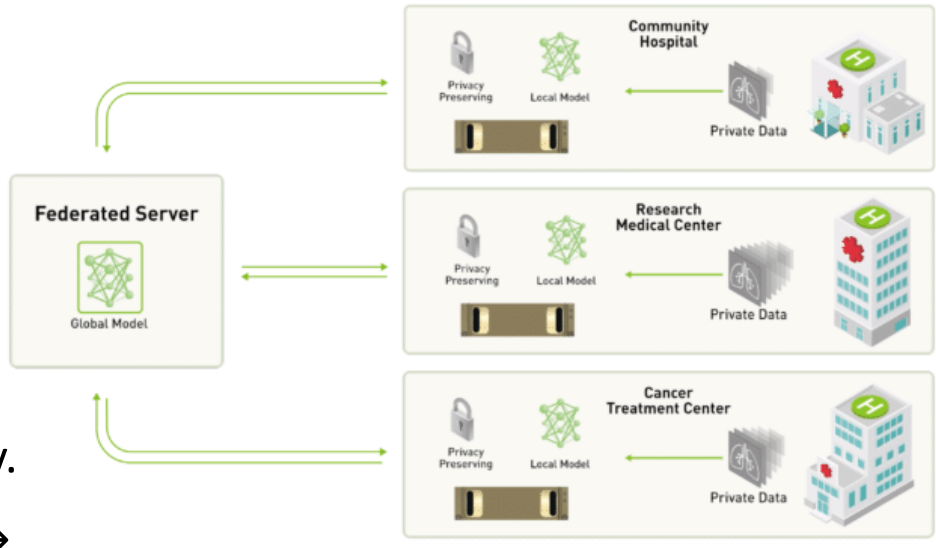


Image Source https://developer.download.nvidia.com/assets/Clara/flare/hroth_nvflare_webinar_Feb2025.pdf

Open Questions

- Ambiguity in definitions.
- Enforcement capacity and expertise.
- Global competitiveness vs. compliance burden.
- Impact on open research and open-source AI development.
- Risks of over-regulation vs. under-regulation.
- Need for adaptive, flexible rules in a fast-moving field.

Other legal frameworks

- Algorithmic Accountability Act, **United States**
- Stop Discrimination by Algorithms Act, **United States**
- Assembly Bill 331 on Automated Decision Tools, **California**
- Artificial Intelligence and Data Act (AIDA), **Canada**
- Basic Act on the Development of Artificial Intelligence and Establishment of Foundation for Trust, **Korea**
- Act on the Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies, **Japan**

Thank you!

Any Questions?

Drop me an email: dgomes@ua.pt