Risk Categorization in the AI Act: Perspectives and Practical Approaches

Authors
Afra Ece Kaya
Luciano Martin Duarte Castineira
Maja Czarnecki
Szymon Piotr Vogiatzis

What Is the AI Act?

The AI Act, officially Regulation (EU) 2024/168, establishes a **risk-based framework** for the development, market entry, and use of artificial intelligence (AI) systems in the EU [1]. Its objective is to assure trustworthy AI that respects health, safety and fundamental human rights while promoting innovation and free market movements [2].

Why Does the AI Act Matter?

- In 2023, **industry produced 51** frontier AI models, compared to **15 from academia** [3].
- **52% of respondents** express **concern about AI** products and services, a 13-percentage-point rise from 2022 [4].
- Ipsos reports a rise in **people expecting AI to impact their lives** within 3–5 years, **from 60% to 66%** [4].
- **Generative AI** funding **reached $25.2 billion** in 2023, **an eightfold increase** despite declining overall AI investment [3].

How are AI Systems Classified in the AI Act [2]?

Unacceptable Risk	**Prohibited** AI systems that pose a **threat to fundamental rights**, **safety** or **EU values**
High-Risk	Systems with a significant impact on health, safety, or fundamental rights **if they fail or are misused**
Limited Risk	Systems with **transparency risks**, e.g., chatbots or AI-generated content, that **must disclose their artificial nature**
Minimal Risk	**Most AI systems**, e.g., AI-driven video games and spam filters, fall into this category **without specific regulations**

Our Methods

The approach used in this research consist of a narrative review to provide context and highlight major trends and gaps in the available literature.

Who Are the Key Stakeholders and Their Views on Classification Criteria?

POLICYMAKERS	Support risk-based safety [2] but **worry about clarity and competitiveness** [6].
BUSINESSES (PROVIDERS)	Large firms **fear burdensome rules** [7]; SMEs seek **fair competition** [8].
DEVELOPERS	Seek clarity and **view frameworks as steps toward** ethical **AI** [9].
USERS (CONSUMERS)	Emphasize the **need for democratic** oversight.
CIVIL SOCIETY	Support **ethical foundations**, **stricter oversight**, and **broader high-risk definitions** [7, 10].

Why Do Stakeholders' Perspectives Differ?

Policymakers: Focus on safety, ethics, and market competitiveness [2, 5, 11].
Businesses: Prioritize innovation, profitability, and minimal compliance obligations [7, 11].
Developers: Seek effective systems with fewer regulatory hurdles [9].
Users: Demand AI that is transparent and trustworthy.
Civil Society: Promote ethical AI and societal inclusion [10].

What Tensions Exist Among Stakeholders' Views?

MARKET ACCESS	↔	FAIR COMPETITION
TRANSPARENCY	↔	INTELLECTUAL PROPERTY
INNOVATION	↔	REGULATION
CLARITY	↔	FLEXIBILITY
PROFIT	↔	ETHICS
ENFORCEMENT	↔	FEASIBILITY

Why Are Classification Criteria Hard to Apply?

Ambiguity in Definitions and Scope [12,14]	Subjectivity in Risk Assessment [12]	Complexity of AI Systems	Regulatory Trade-Offs [13]
↓	↓	↓	↓
Unclear Terms	Varying Perspectives [15]	Dynamic Nature of AI [14]	Under-regulation
Broad AI System Definition	Sector-Specific Risks [13]	Varying Risk Profiles [12]	Over-regulation

What Are the Technical and Legal Challenges?

- Explainability and Transparency of AI Systems [16]
- Testing and Auditing AI Systems [13]
- Data Quality and Availability [12]

- Interpretation of Fundamental Rights [16]
- Lack of Legal Precedents [14]
- Harmonization Across Member States [13]

How Do These Challenges Impact Stakeholders?

AI Developers and Providers:
- Ambiguities in criteria complicate developers' obligations.
- High compliance costs may deter innovation or favor low-risk systems [12, 14].

End Users:
- Compliance costs may raise prices for AI products and services [13].
- Lengthy procedures may delay access to innovations [15].

Regulators:
- Limited resources and expertise may hinder regulators, leading to weak or inconsistent oversight [14].

SMEs and Startups:
- Smaller organizations may struggle to compete with larger corporations due to limited resources for compliance [13].

What Are the Solutions to These Challenges?

Clarify Classification Criteria: Provide detailed guidance and examples for classification and regularly update criteria to reflect AI advances and societal risks [16, 17].

Promote Technical Support and Education: Establish support centers for SMEs and startups and provide training for regulators to enhance compliance and expertise [13, 15].

Leverage Standards and Best Practices: Develop harmonized technical standards for transparency, data quality, and testing to reduce ambiguity and ensure consistent compliance across the EU [14].

Expand risk assessment frameworks to incorporate social and environmental impacts [18].

Replace or supplement self-assessment mechanisms with independent third-party audits [19].

Key Takeaways

While human oversight is emphasized in the AI Act, its implementation often lacks effectiveness due to insufficient training and guidance.

Static classification under the AI Act often misrepresents actual risks. This rigid approach can lead to both under- and over-regulation .

Open Questions

How can regulatory bodies maintain neutrality and avoid conflicts of interest while fostering innovation [19]?

Can general-purpose AI systems be effectively regulated without hindering innovation and flexibility [20]?

References

To view the references, scan the QR code or read the abstract. ☺