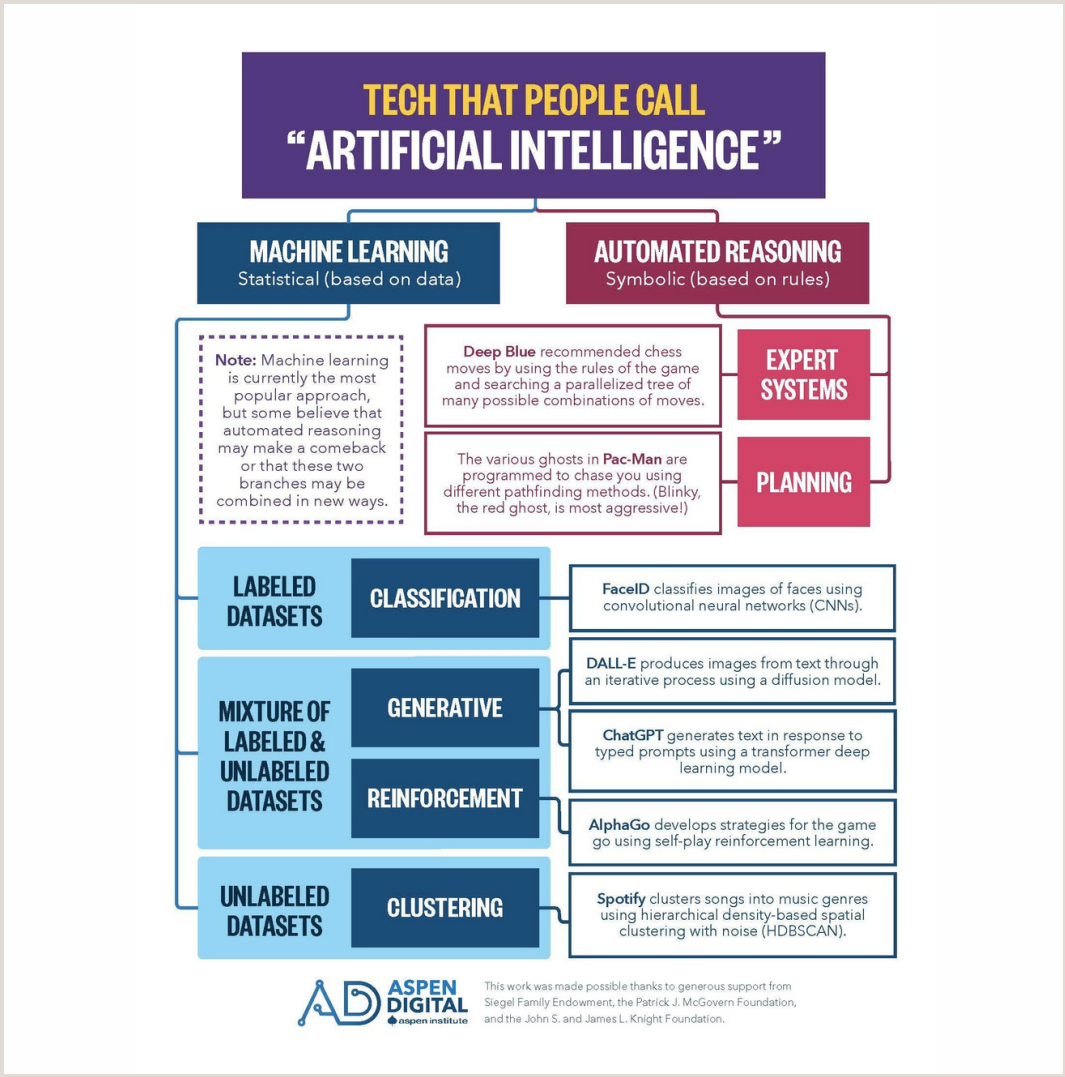
Comparing Regulatory Approaches to AI
The EU with the AI Act Regulation

Dr Begoña G. Otero

Senior Research Fellow at Max Planck Institute for Innovation and Competition, Munich


TECH THAT PEOPLE CALL
"ARTIFICIAL INTELLIGENCE"
MACHINE LEARNING
Statistical (based on data)
AUTOMATED REASONING
Symbolic (based on rules)
Note: Machine learning is currently the most popular approach, but some believe that automated reasoning may make a comeback or that these two branches may be combined in new ways.
Deep Blue recommended chess moves by using the rules of the game and searching a parallelized tree of many possible combinations of moves.
EXPERT SYSTEMS
The various ghosts in Pac-Man are programmed to chase you using different pathfinding methods. (Blinky, the red ghost, is most aggressive!)
PLANNING
LABELED DATASETS
CLASSIFICATION
FaceID classifies images of faces using convolutional neural networks (CNNs).
MIXTURE OF LABELED & UNLABELED DATASETS
GENERATIVE
DALL-E produces images from text through an iterative process using a diffusion model.
ChatGPT generates text in response to typed prompts using a transformer deep learning model.
REINFORCEMENT
AlphaGo develops strategies for the game go using self-play reinforcement learning.
UNLABELED DATASETS
CLUSTERING
Spotify clusters songs into music genres using hierarchical density-based spatial clustering with noise (HDBSCAN).
ASPEN DIGITAL
aspen institute
This work was made possible thanks to generous support from Siegel Family Endowment, the Patrick J. McGovern Foundation, and the John S. and James L. Knight Foundation.

AlphaGo

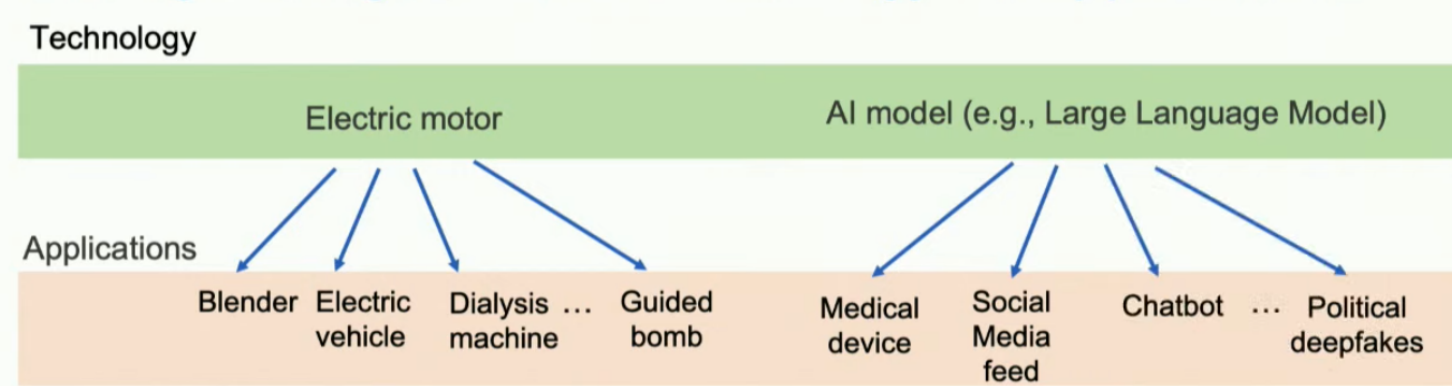
The AI Stack

Even though the media tends to focus on AI technology, most of the opportunities are in building AI applications.

To prevent chokepoints, promote (or at least don't stifle) open-source.

How to Regulate AI?

AI is a GPT: Differentiate Applications & the Technology



- **Technology** refers to tools that can be applied in many ways to solve problems.
  Applications are specific implementations of technologies designed to meet particular customer needs.

How to Regulate AI - Coglianese (2023)

Agility

- Legislator to build up their capacity and keep pace with changes in industry.
  - Yet, complex for civil law traditions
  - Is industry the best positioned to know the most about tech/risks of applications/interface with rights of others?
- Legislators should avoid embracing a perspective that values innovation for its own sake (?)

Flexibility

- Management-based approach of the legislator to require companies to engage in conversations to id and correct problems (**is it feasible in all jurisdictions?)**

Vigilance

- Legislators to build the capacity to assess the quality of the firms' management efforts and to sustain rigor in their oversight
- Legislators stay engaged with the industry due to rapid pace of change
- Responsible regulation requires vision, attentiveness and the capacity to learn and adapt

Key choices

Internal market legislation

- "Classic" internal market rules for the placing on the market and putting into service of AI systems (**CE mark**)
- **New Legislative Framework "philosophy"**: harmonized standards to operationalize legal requirements
- **Horizontal approach**: across sectors within EU competence. No national security, military, defense.
  - **Sectorial specificities/needs** considered (law enforcement, finance, product legislation acquis)
  - **Without prejudice to other relevant EU acquis** (e.g. data protection, consumer protection, equality law, platforms legislation): *AI Act is not the only EU law applicable to AI*

Risk-based approach

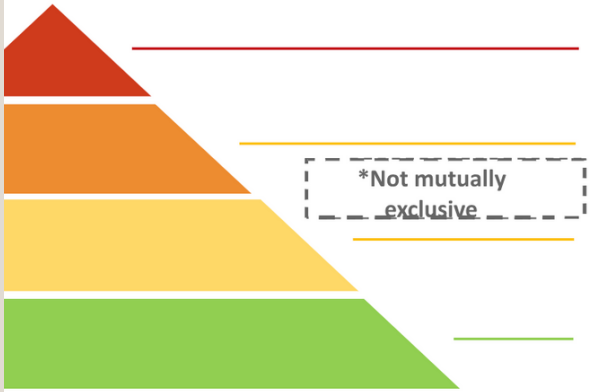
Level playing field for EU and non-EU players

- When AI is used in the EU market, same rules apply *(Brussels' effect?)*

Risk-based approach

The higher the risk the stricter the rules

No regulation of the technology as such



Unacceptable risk
e.g. social scoring
— **Prohibited**

High risk
e.g. recruitment, medical devices
Permitted subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk
'Impersonation' (bots), deep fake
— **Permitted** but subject to information/transparency obligations

Minimal or no risk
— **Permitted** with no restrictions

European Commission

High-risk AI systems

ANNEX II

New Legislative Framework - Section A

'Old Approach'- Section B

1 SAFETY COMPONENTS OF REGULATED PRODUCTS

(e.g. medical devices, machinery) which are subject to third-party assessment under the relevant sectorial legislation

2 CERTAIN (STAND-ALONE) AI SYSTEMS IN THE FOLLOWING AREAS

ANNEX III

- ✔ Biometric systems
- ✔ Management and operation of critical infrastructure
- ✔ Education and vocational training
- ✔ Employment and workers management, access to self-employment
- ✔ Access to and enjoyment of essential private services and public services and benefits
- ✔ Law enforcement
- ✔ Migration, asylum and border control management
- ✔ Administration of justice and democratic processes

European Commission

AI Act Art 3(66) 'general-purpose AI system' means an AI system which is based on a **general-purpose AI model** and which has the capability to **serve a variety of purposes**, both for direct use as well as for integration in other AI systems'.

WHAT IS A FOUNDATION MODEL?

In recent years, a new successful paradigm for building AI systems has emerged: **Train one model on a huge amount of data and adapt it to many applications**. We call such a model a foundation model.

WHY DO WE CARE?

Foundation models (e.g., GPT-3) have demonstrated impressive behavior, but can fail unexpectedly, harbor biases, and are poorly understood. Nonetheless, they are being **deployed at scale**.

(CRFM, Standford)

General Purpose AI models

All GPAI (lower tier)

- Technical documentation (incl. computational resources & energy consumption)
- Information downstream
- Copyright (policy & detailed summary of content)

GPAI with systemic risks (higher tier)

- Evaluation of high-impact capabilities
  - at least 10^25 FLOPs
  - designated by the AI Office (e.g. based on certain criteria)
- All obligations from the lower tier PLUS
  - risk assessment and mitigation
  - incident reporting
  - adequate level of cybersecurity

- **Open-source models** in scope, except technical documentation and transparency as regards lower tier
- **Codes of Practice** for demonstrating compliance

European Commission

The clock is ticking

May - August 2024

The EU AI Act is published in the Official Journal of the EU and enters into force after 20 days.

December 2024

According to Art 113(a), the prohibitions in Article 5 become applicable within the EU.

Summer 2025

According to Art 113(b), the GPAI provisions in Art 51 ff become applicable within the EU.

Summer 2026

According to Art 113, the vast majority of all Articles of the AI Act, in particular the rules for high-risk AI systems listed in ANNEX III, become applicable within the EU.

Summer 2027

According to Art 113(c), the provisions for high-risk AI systems listed in ANNEX I become applicable within the EU.

kaizenner.eu

Stakeholders: call to action!

Engage in Standardization Bodies

Help CEN/CENELEC to develop horizontal as well as vertical harmonized technical standards in time.

Join Regulatory Sandboxes

Enter in a close dialogue with national authorities, make the AI Act compliance easier and benefit both from regulatory learning.

Share your expertise

The Commission relies on your input for guidelines (Art 96), the code of practice (Art 56), and DA/IAs. You could also join the Scientific Panel (Art 68) or Advisory Forum (Art 67).

Identify & motivate AI talent

European and national governance bodies need to attract AI experts but those persons can often earn much more in large Tech companies.

kaizenner.eu


Gracias por su atención
Thanks for your attention!