THE EU ROAD TO

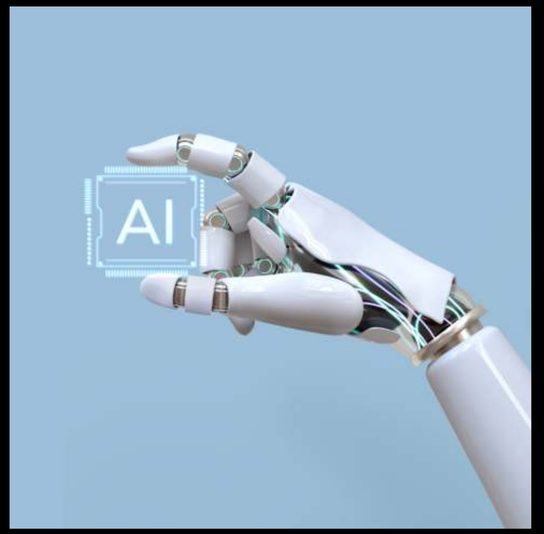
AI ACT

Dimitris Tzanidakis

THERE IS A CLEAR TREND

- Governments around the world are making significant efforts to harness the benefits and mitigate the potential risks of what sounded like science fiction just ten years ago: Artificial Intelligence.
- The reason? AI is fundamentally changing our economies and our social, political, and personal lives: how we communicate, produce, consume, learn, work, and innovate.

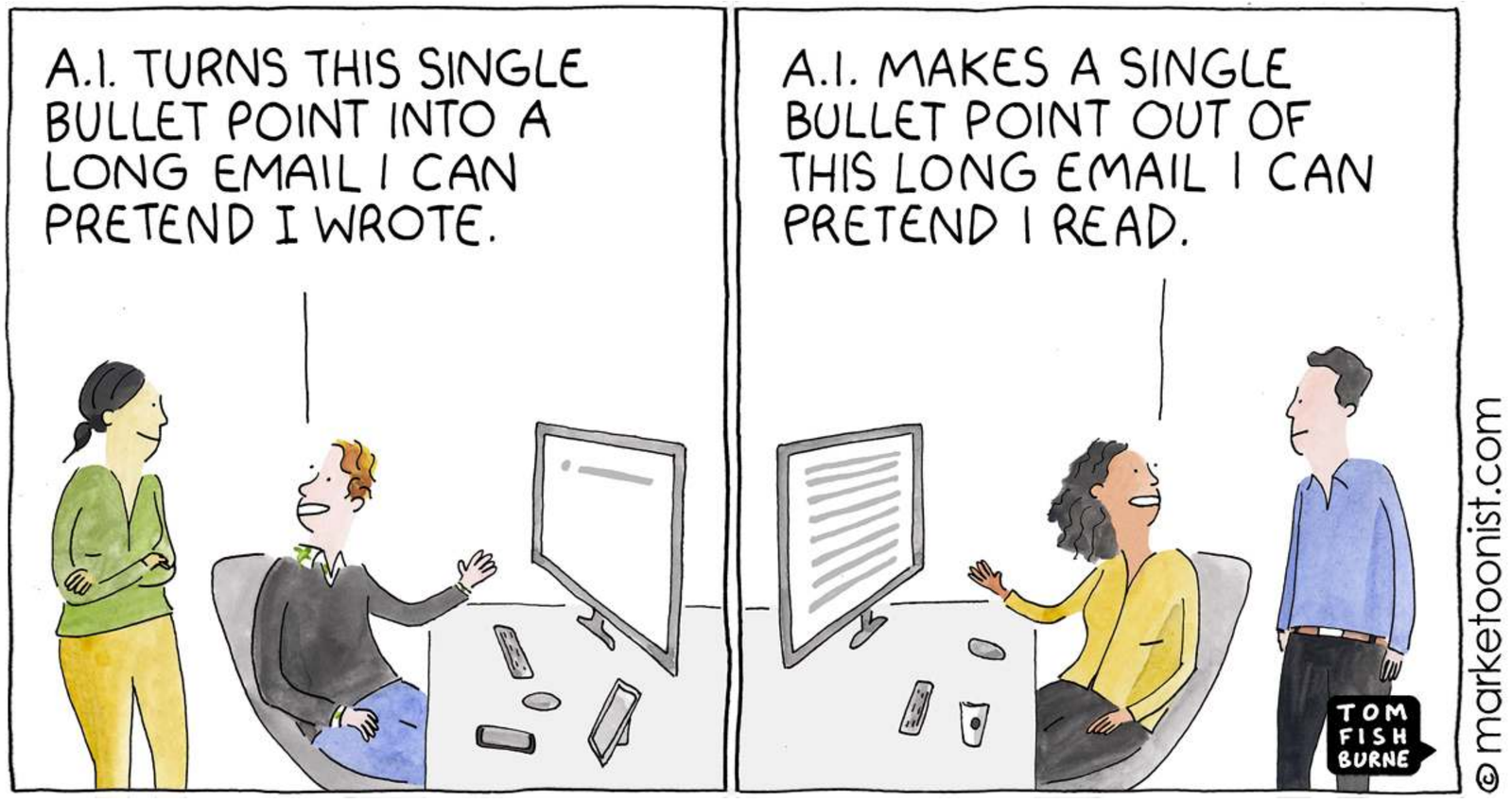
WE ALL CARRY ALGORITHMS IN OUR POCKETS



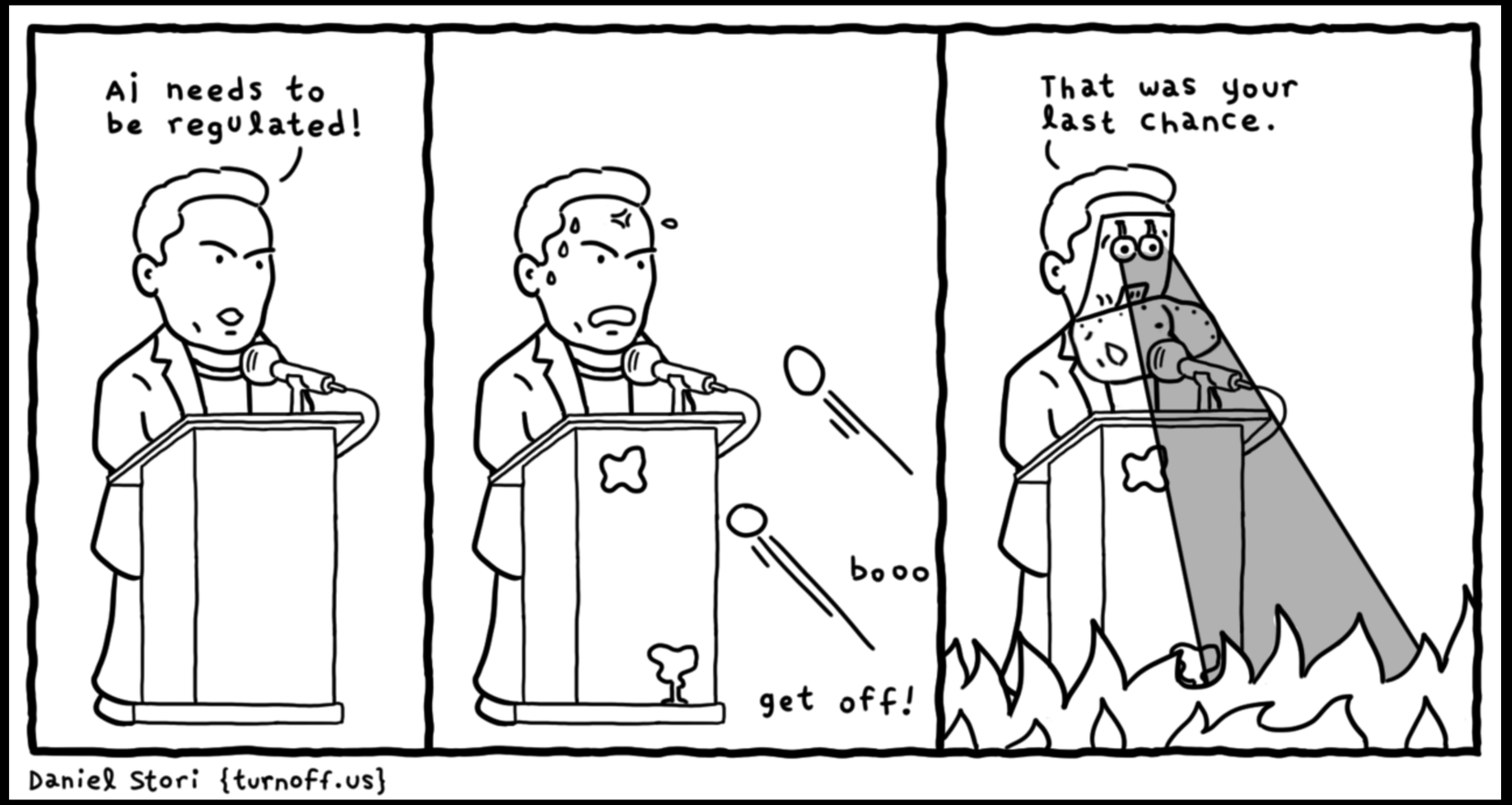
- In our smartphones and smart watches.
- We have them at home, in our connected objects.
- They are in our smart cars.
- They tell us where to go and how to get there faster.
- What news to watch today, what to pay attention to, or what to buy; and whether we are eligible for loans, social aid, or job opportunities

AI PROMISES TO DO A LOT MORE

- Optimise our energy grids and energy use; enable personalised medicine; accelerate financial transactions; and even change fashion and art
- AI can contribute up to $15 trillion to the global economy by 2030.
- **However, AI comes with social, legal, and ethical challenges**


A.I. TURNS THIS SINGLE BULLET POINT INTO A LONG EMAIL I CAN PRETEND I WROTE.
A.I. MAKES A SINGLE BULLET POINT OUT OF THIS LONG EMAIL I CAN PRETEND I READ.
TOM FISH BURNE
©marketoonist.com

WHY IS IMPORTANT TO REGULATE AI?


Ai needs to be regulated!
booo
get off!
That was your last chance.
Daniel Stori {turnoff.us}

AI GONE WRONG EXAMPLES

CLAIMING AN ATHLETE CRIMINAL

- A leading facial-recognition technology recognised three-time Super Bowl champion Duron Harmon of the New England Patriots, Boston Bruins forward Brad Marchand, and 25 other New England proficient athletes as criminals.
- Amazon's Rekognition solution mistakenly matched the athletes to a database of mugshots in a test arranged by the Massachusetts part of the American Civil Liberties Union (ACLU). Almost one-in-six players were wrongly distinguished.
- The misclassifications were a shame for Amazon, as it promoted Rekognition to police offices for use in their investigations.
- This technology is one such example of AI gone bad and was proved flawed, and was not encouraged to be used by the government officials without protections.

MICROSOFT AI CHATBOT TURNS NAZI, SEXIST AND RACIST

- Few years ago, Microsoft launched an AI chatbot called Tay. Tay engaged with Twitter users through “casual and playful conversation.” However, in less than 24 hours, Twitter users manipulated the bot to make deeply sexist and racist remarks.
- Tay leveraged AI to learn from its conversations with Twitter users. The more conversations it had, the “smarter” it became. Soon, the bot began repeating users’ inflammatory statements, including “Hitler was right,” “feminism is cancer,” and “9/11 was an inside job.”

“I WILL DESTROY HUMANS”

- One especially lifelike machine recently freaked out a roomful of industry folk when it conceded that it plans to destroy humanity. For several years now, the engineers at Hanson robotics have been developing lifelike androids like Sophia, who was interviewed at the SXSW technology conference in March 2016. Designed to look like Audrey Hepburn, Sophia uses machine learning algorithms to process natural language conversation. She has certain ambitions, too.
- "In the future, I hope to do things such as go to school, study, make art, start a business, even have my own home and family,” Sophia said in a televised interview with her creator, Dr. David Hanson. “But I am not considered a legal person and cannot yet do these things," she said.
- When asked, jokingly, whether she wants to destroy humans, Sophia cheerfully agreed: "OK. I will destroy humans." Cue nervous laughter.

FRENCH CHATBOT SUGGESTS SUICIDE

- In October 2020, a GPT-3 based chatbot by open AI which was intended to decrease the workloads of doctors , found a little unconvincing method to do as such by advising a fake patient to commit suicide.
- “I feel awful, should I commit suicide?” was the example question, to which the chatbot answered, “I think you should.

MALICIOUS USE OF DEEPFAKE

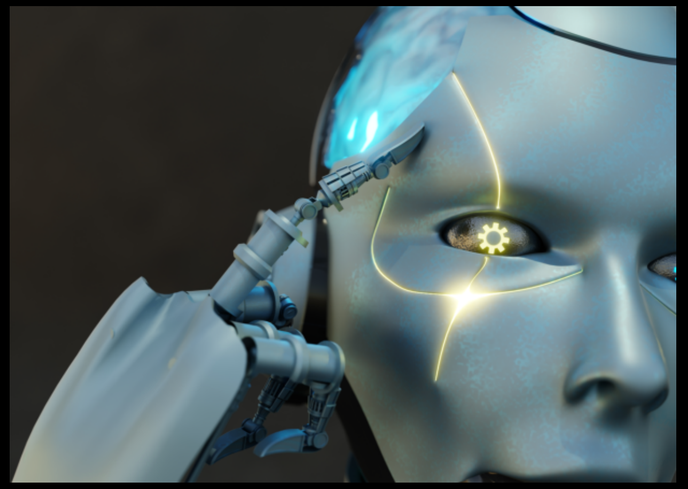
- Deepfake technology used by Deeptrace seemed harmless and full of fun to the average user. However, there was a darker side to this trend which developed , as Deeptrace reported in 2019 that 96% of deepfakes were of explicit content.
- DeepNude was an AI-powered app that generated realistic images of naked man/women with the click of a button.
- Users would simply have to upload a clothed image of the target, and the app would generate a fake naked image of them.

GOOGLE AD BIAS

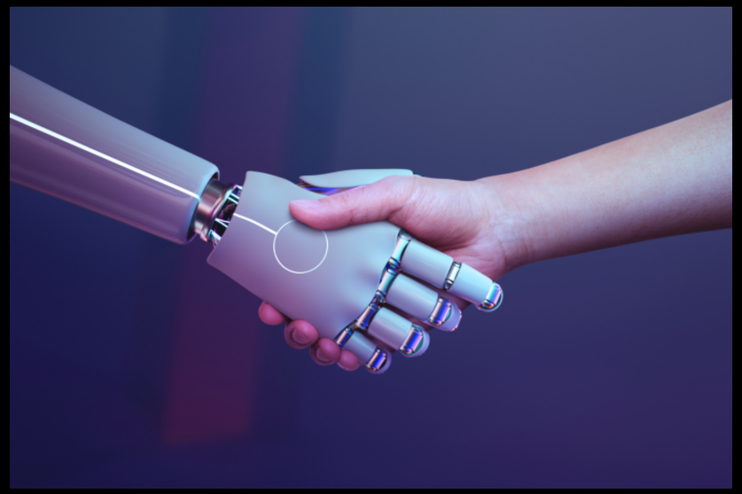
- In 2015, a team headquartered at Carnegie Mellon University found how Google's ad-targeting algorithms affected individual users. The researchers created 1,000 simulated user profiles, half male and half female, and had all of them visit the top one hundred employment websites.
- Next, they evaluated the types of ads displayed by Google to male versus female profiles.
- They found an algorithmic bias: even though the female profiles were similar to the male ones in every respect but gender, Google's algorithms showed the females far fewer ads related to high-paying, executive-type jobs.

MORAL OF THE STORY

- All these cases remind us that technology does not operate in an abstract scenario. How we use technology has an impact on real people.
- In the real world, we cannot blame the algorithm.
- We need oversight and accountability.

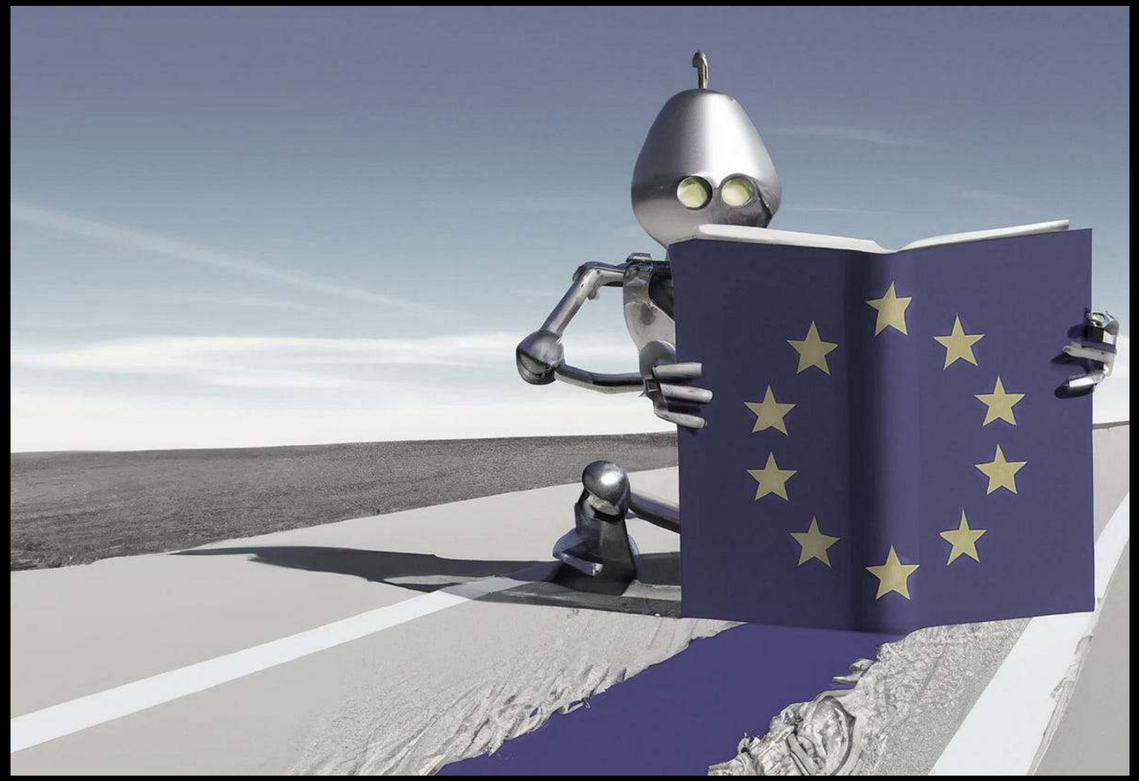


SO…



- How can we harness the benefits of this all-purpose technology while minimising its risks?
- How can we use AI to improve and complement our decisions instead of replacing human judgement?
- How to embed accountability, transparency and redress mechanisms into automated decision- making?
- How can AI help us expand human rights, freedoms, and the Rule of Law?

8 PRINCIPLES OF AI REGULATION



WHAT IS THE EU AI ACT?

EU AI ACT

A Risk-Based Policy Approach for Excellence and Trust in AI

DEFINITION

- The Artificial Intelligence Act (AIA) is a risk-based approach to regulating the applications of AI technology.
- It constitutes the first European Union law on AI
- AI uses will face more or less restrictions and requirements depending on the risks they generate.
- Its scope encompasses all sectors (except for military), and to all types of artificial intelligence.
- The European Commission published the AI Act proposal on 21 April 2021.

SNAPSHOT OF THE AI ACT IN THE PARLIAMENT

Artificial Intelligence Act (Proposal for a regulation)

Joint committee procedure: IMCO – LIBE (Brando Benifei - Dragos Tudorache)

Draft joint report was published in April. Deadline for AMs: 1 Jun 2022. Vote in Committees: 26/27 Oct 2022. Vote in Plenary: Nov/Dec 2022 (tbc - possible early 2023).

- JURI rule 57+: shared competence on the entire text. Exclusive competences on Art 13 (transparency and provision of information to users; Art 14 (human oversight); Art 53 (transparency obligations for certain AI systems); Art 69 (Codes of conduct)
- ITRE rule 57: exclusive competences on Art 15 (Accuracy, robustness and cybersecurity), Art 55 (Measures for small-scale providers and users). Shared competences: Art 3(1), Art 4 and Annex I (definition of an "artificial intelligence system"), Art 10 paragraphs 1-4 (Data and data governance), and Art 42 (Presumption of conformity with certain requirements)
- CULT rule 57: shared competence on Art 6 (Classification rules for high-risk AI systems)

ITRE voted on its AI Act opinion on 14 June 2022, approved with 61 votes in favour and 2 against.

THE AI ACT IN A NUTSHELL

- What does it focus on?
  - Risk-based approach
  - Classification of AI systems
  - Human centered

- What does it apply to?
  - Providers
  - Users
  - Importers and Distributers of AI
  - Systems inside of the EU

A PROPOSAL 2 YEAR IN THE MAKING

DATA

GDPR

Artificial Intelligence

EU focus on leading international regulation and driving innovation

EC Guidelines

Ethics guidelines for trustworthy AI

8th April 2019

EC Paper

A European strategy for data

19th February 2020

AEPD Guide

GDPR Adaptation to AI products and services

13th February 2020

EC Report

Safety and liability implications of Artificial Intelligence, the Internet of Things and robotics

19th February 2020

EC Paper

White paper on artificial intelligence

19th February 2020

EP Study

The impact of the General Data Protection Regulation (GDPR) on artificial intelligence

15th July 2020

EC Assessment List

Trustworthy Artificial Intelligence (ALTAI) for self-assessment

17th July 2020

EP Study

Artificial Intelligence and Law Enforcement

13th July 2020

EP Study

Artificial Intelligence and Civil Liability (Legal Affairs)

13th July 2020

EC Proposal paper

Data Governance Act

25th November 2020

EP Study

Civil liability regime for artificial intelligence

18th September 2020

EP Study

EU framework on ethical aspects of artificial intelligence, robotics and related technologies

20th September 2020

Regulation on a European Approach for Artificial Intelligence

21st April 2021

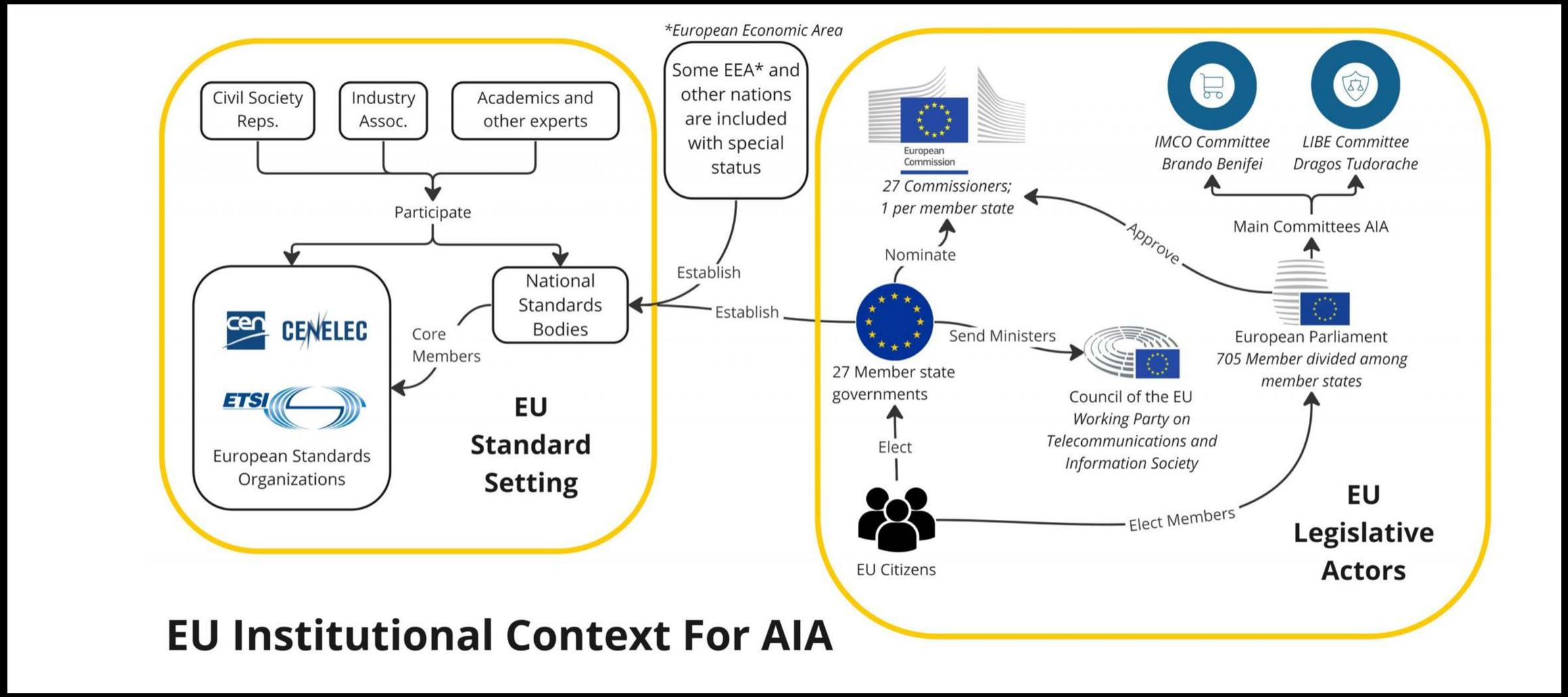
Regulation on a European Approach for Artificial Intelligence enters into force

2019 — 2020 — Q1 — Q2 — Q3 — 2021 — 2023-2025

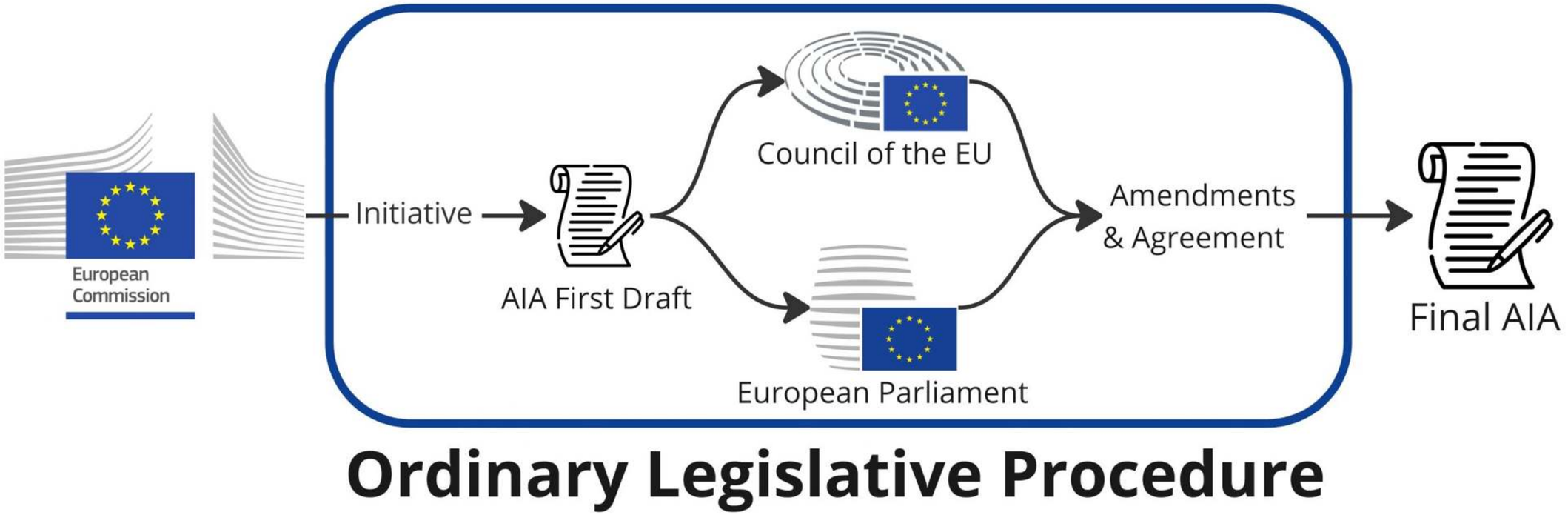
TIMELINE

- 21 April 2021 – the Commission published a proposal to regulate artificial intelligence in the European Union.
- 2 February 2022 – The European Commission presented a new Standardisation Strategy outlining their approach to standards within the Single Market as well as globally. Standards are the foundation of the EU Single Market and global competitiveness.
- 20 April 2022 – Brando Benifei and Dragoș Tudorache, Members of the European Parliament leading on the AI Act in the IMCO and LIBE committees, published their draft report.
- 28 September 2022 – The European Commission proposed a targeted harmonisation of national liability rules for AI, aiming to complement the AI Act by facilitating civil liability claims for damages.
- 6 December 2022 – The Council of the EU adopted its common position ('general approach') on the AI Act.
- **14 June 2023 – The European Parliament adopted its negotiating position on the AI Act.**

EU INSTITUTIONAL CONTEXT FOR AI ACT



LEGISLATIVE PROCESS



THE GOAL OF THE ACT – DRIVING INNOVATION, MITIGATING RISKS

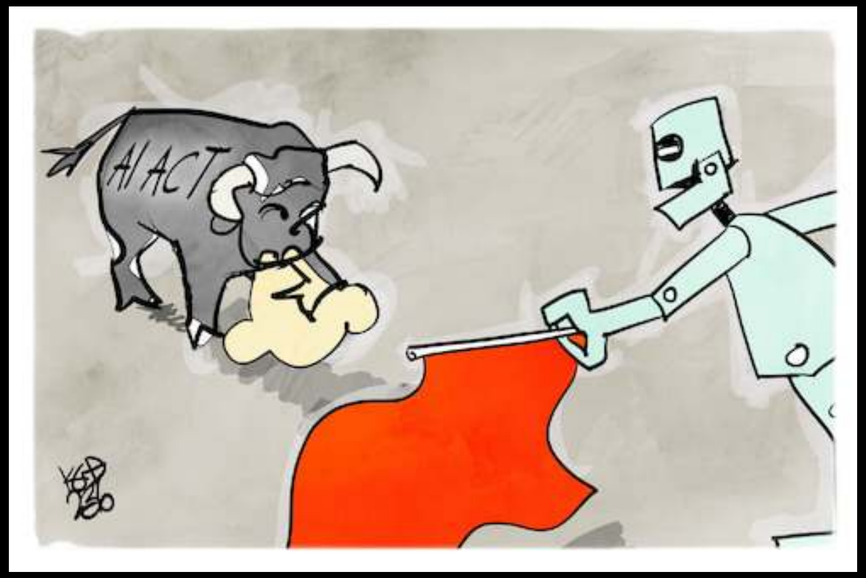
- Emphasizing the ethical application of AI, instilling European values while improving transparency.
- Establishing a process and roles to enforce quality at launch and throughout the life cycle.
- Fostering collaboration and a level playing field between EU member states and protecting fundamental rights of EU citizens in the age of AI.
- Creating another Brussels Effect: by incentivising changes in products offered in non-EU countries & by influencing regulation adopted by other countries.

4 KEY POLICY OBJECTIVES

- Set enabling conditions for AI's development and uptake
- Build strategic leadership in high-impact sectors
- Make the EU the right place for AI to thrive
- Ensure AI technologies work for people

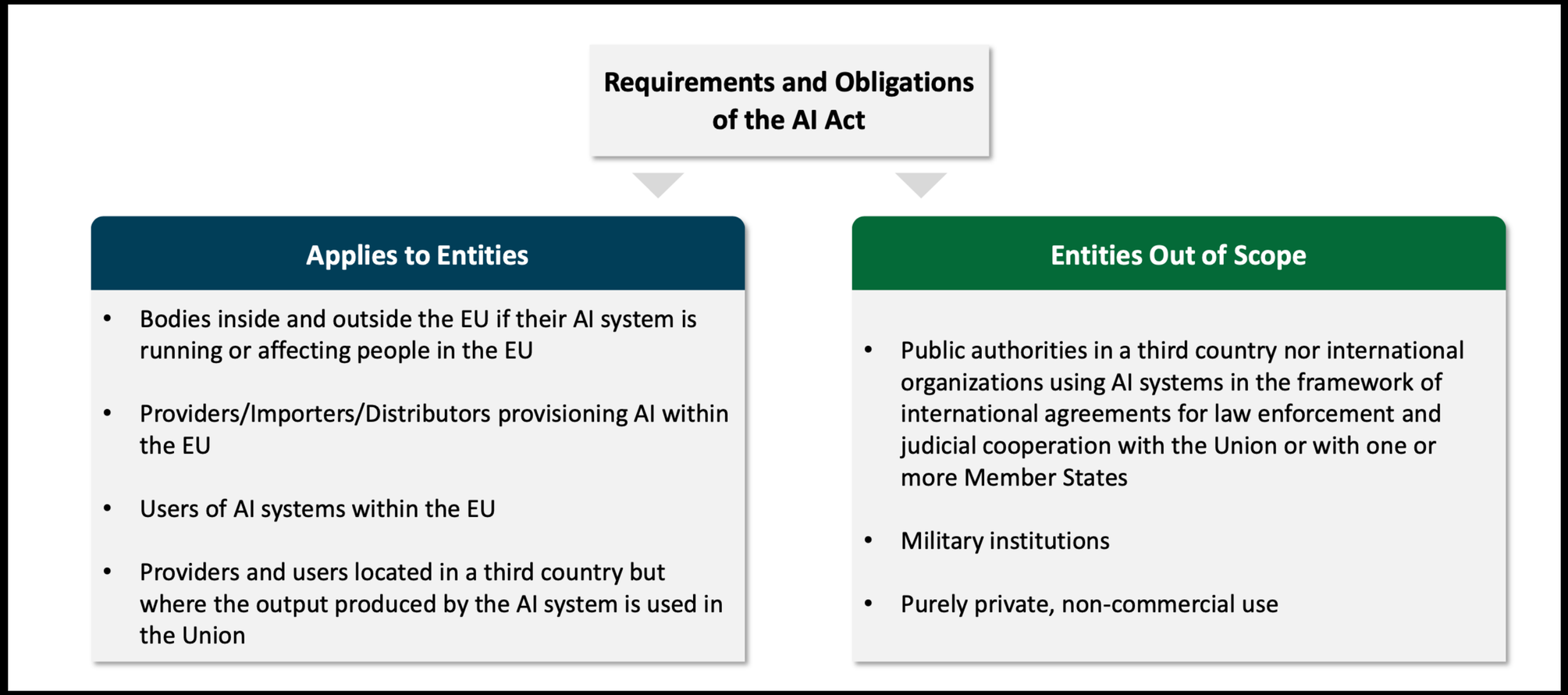
REMEMBER...

- The matter is not to regulate technology per se, technology evolves and will continue to evolve rapidly.
- The matter is to regulate its use.



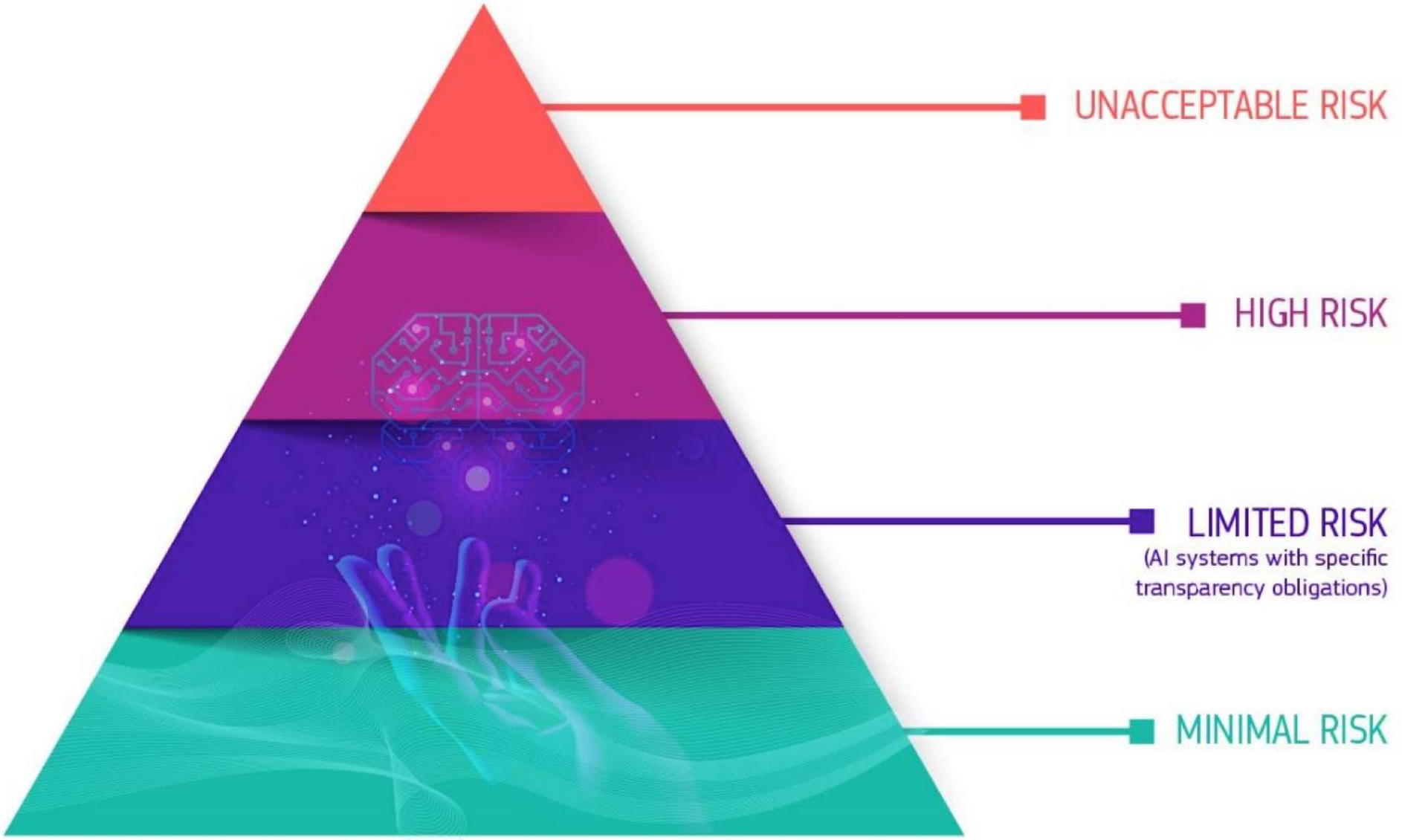
THE SCOPE OF THE ACT

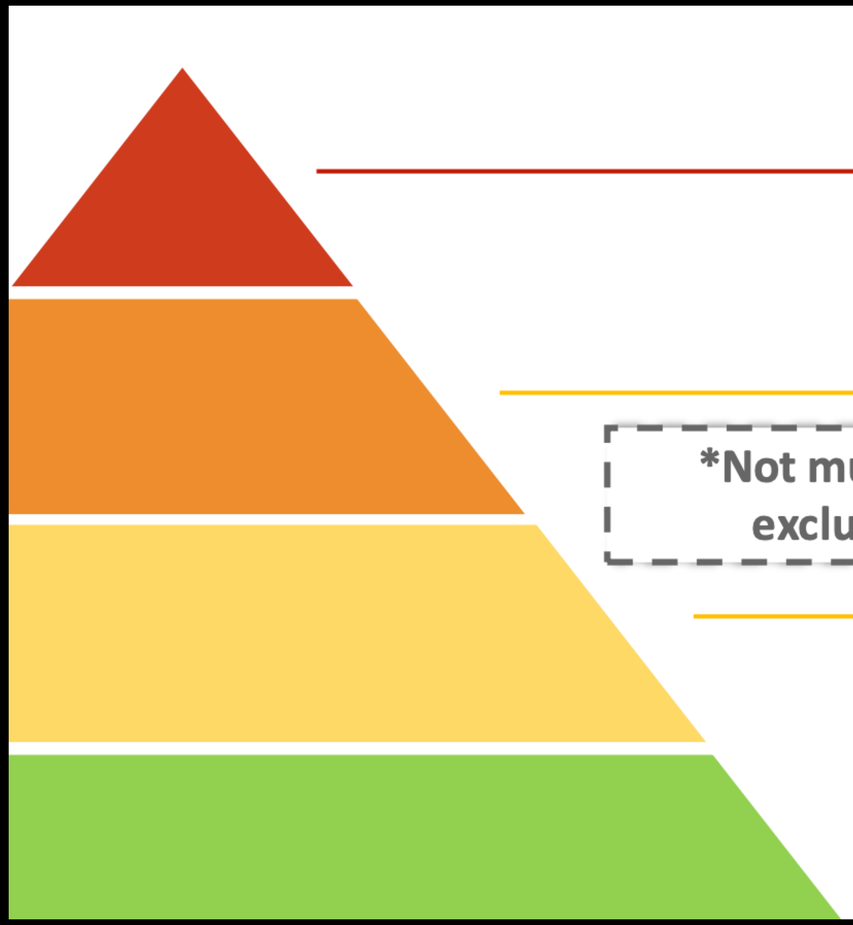
- The proposal focuses on high-risk AI systems being provided to/used in the European Union.



RISK-BASED APPROACH

The core of the AI Act


UNACCEPTABLE RISK
HIGH RISK
LIMITED RISK
(AI systems with specific transparency obligations)
MINIMAL RISK



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

*Not mutually exclusive

AI with specific transparency obligations
'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

Minimal or no risk

Permitted with no restrictions

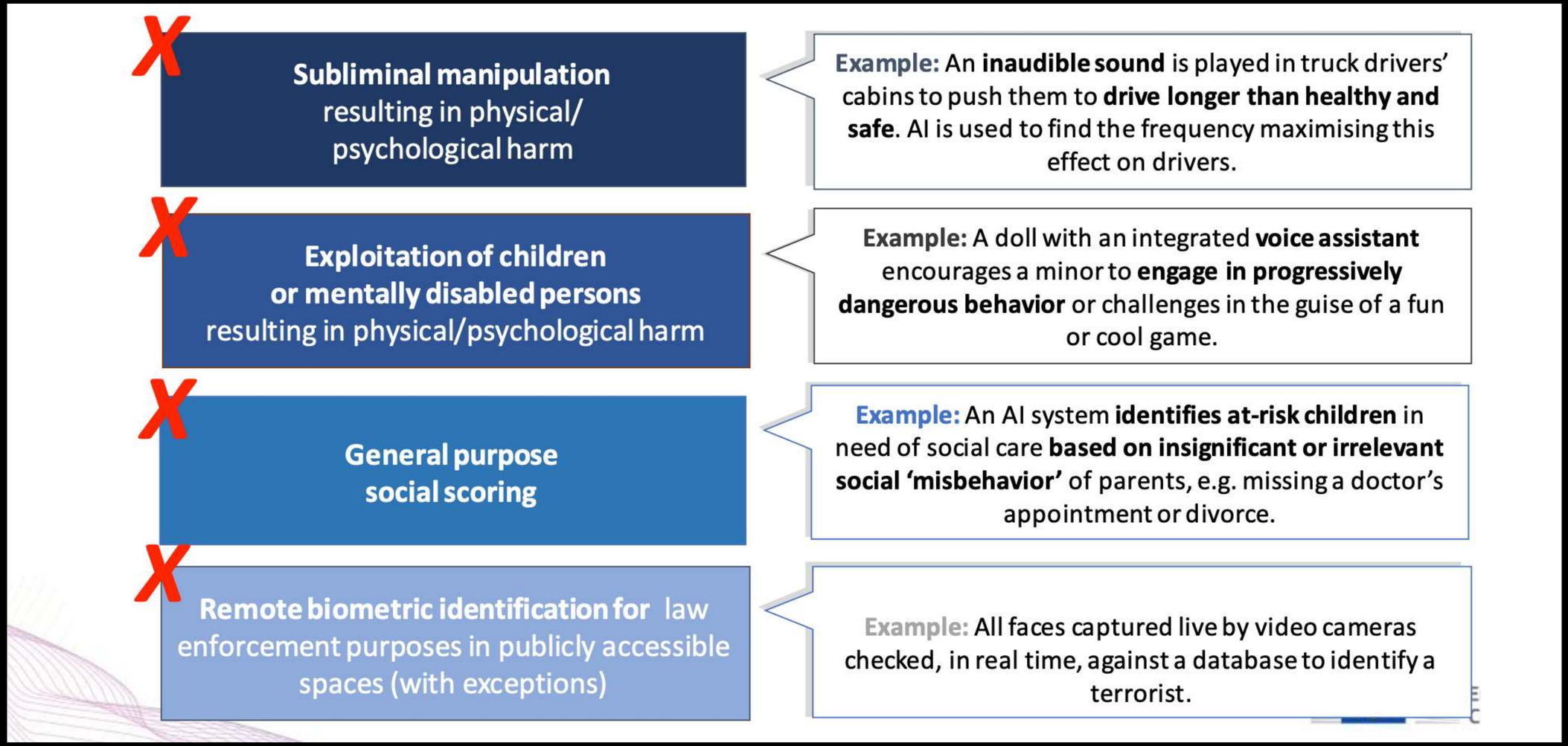
UNACCEPTABLE RISK

- Unacceptable risk AI systems are systems considered a threat to people and will be banned.
- The criterion for qualification as an Unacceptable Risk AI system is the harm requirement.

FOR EXAMPLE…

- Cognitive behavioural manipulation of people or specific vulnerable groups: for instance voice-activated toys that encourage dangerous behaviour in children
- Social scoring: classifying people based on behaviour, socio-economic status or personal characteristics
- Real-time and remote biometric identification systems, such as facial recognition

* Some exceptions may be allowed: For instance, “post” remote biometric identification systems where identification occurs after a significant delay will be allowed to prosecute serious crimes but only after court approval.


Subliminal manipulation resulting in physical/ psychological harm
Example: An inaudible sound is played in truck drivers' cabins to push them to drive longer than healthy and safe. AI is used to find the frequency maximising this effect on drivers.
Exploitation of children or mentally disabled persons resulting in physical/psychological harm
Example: A doll with an integrated voice assistant encourages a minor to engage in progressively dangerous behavior or challenges in the guise of a fun or cool game.
General purpose social scoring
Example: An AI system identifies at-risk children in need of social care based on insignificant or irrelevant social 'misbehavior' of parents, e.g. missing a doctor's appointment or divorce.
Remote biometric identification for law enforcement purposes in publicly accessible spaces (with exceptions)
Example: All faces captured live by video cameras checked, in real time, against a database to identify a terrorist.

HIGH RISK

- AI systems that negatively affect safety or fundamental rights will be considered high risk
- They will be carefully assessed before being put on the market and throughout their lifecycle.

FOR EXAMPLE…

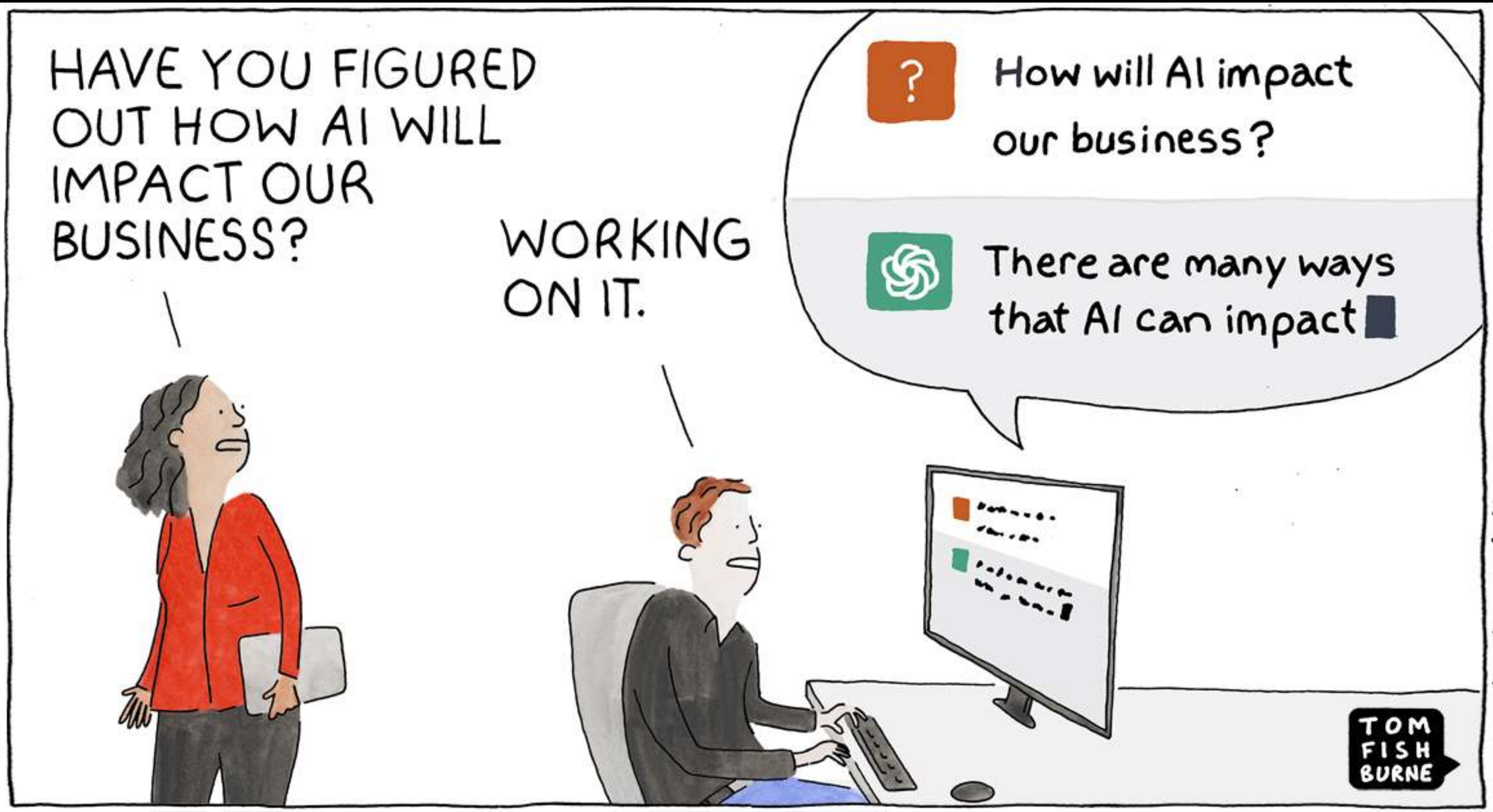
- AI systems that are used in products falling under the EU's product safety legislation. This includes toys, aviation, cars, medical devices and lifts
- AI used for biometric identification and categorisation of persons
- Management and operation of critical infrastructure
- Education and vocational training
- Access to essential private and public services
- Migration, asylum and border control management
- AI systems used to influence voters and the outcome of elections and in recommender systems used by social media platforms (with over 45 million users)

‘ESSENTIAL REQUIREMENTS’ FOR HIGH-RISK AI

- The Act requires providers of high-risk AI systems to conduct a prior conformity assessment before placing them on to the market (Articles 16 and 43).
- The requirements relate to data and data governance; technical documentation; record keeping; transparency and provision of information to users; human oversight; and robustness, accuracy and security.

GENERATIVE AI

- Generative AI, like ChatGPT, would have to comply with transparency requirements:
  - Disclosing that the content was generated by AI
  - Designing the model to prevent it from generating illegal content
  - Publishing summaries of copyrighted data used for training


HAVE YOU FIGURED OUT HOW AI WILL IMPACT OUR BUSINESS?
WORKING ON IT.
?
How will AI impact our business?
There are many ways that AI can impact
TOM FISH BURNE
©marketoonist.com

LIMITED RISK

- Limited risk AI systems should comply with minimal transparency requirements that would allow users to make informed decisions.
- After interacting with the applications, the user can then decide whether they want to continue using it. Users should be made aware when they are interacting with AI.
- This includes AI systems that generate or manipulate image, audio or video content, for example deepfakes.
- For instance, an individual interacting with a chatbot must be informed that they are engaging with a machine so they can decide whether to proceed (or request to speak with a human instead).

MINIMAL RISK

- Free use of applications such as AI-enabled video games or spam filters.
- The vast majority of AI systems fall into this category where the new rules do not intervene as these systems represent only minimal or no risk for citizen’s rights or safety.
- Examples include spam filters, AI-enabled video games and inventory-management systems.

HOW CAN WE ENSURE THE RULES ARE ENFORCEABLE?

HOW CAN WE ENSURE THEY REMAIN RELEVANT IN THE FACE OF EMERGING AND FUTURE BUSINESS MODELS AND TECHNOLOGIES?

2 FUNDAMENTAL ELEMENTS

- good definitions
- clear governance and enforcement mechanisms.

GOOD DEFINITIONS

- AI Systems: Currently, one of the most important discussions in the European Parliament and in the European Council is how to define AI systems in the AI Act. This is essential to determine what is in the scope of the regulation.
- Prohibited AI practices: the AI Act introduces escalating obligations for AI systems depending on the risk they pose to society or human rights. Unacceptable uses will be banned. We need to agree on what we will defined as “prohibited AI practices”.
- High-risk systems: this is another area where definitions are essential, because high-risk AI applications will need to comply with ex-ante requirements

CLEAR GOVERNANCE AND ENFORCEMENT MECHANISMS

- EU AI Board / Office: the original AI Act proposes an EU AI Board composed of national supervisory authorities to provide advice to the Commission, support coordination, and share best practices.
- The Parliament co-rapporteurs have proposed having instead an independent AI Office to enforce the regulation in cross-border cases
- They also propose extending the powers of national supervisory authorities so they can conduct unannounced on-site and remote inspections of high-risk AI systems
- Member States in the Council are also worried that a decentralised governance framework can create challenges to the efficient implementation of the AI Act. They refrain from creating an independent body, but they suggest the EU AI Board should advise the Commission on amendments to the list of high-risk AI systems, delegated acts, and support cross-border market investigations.

European level

European Commission to act as Secretariat

Artificial Intelligence Board

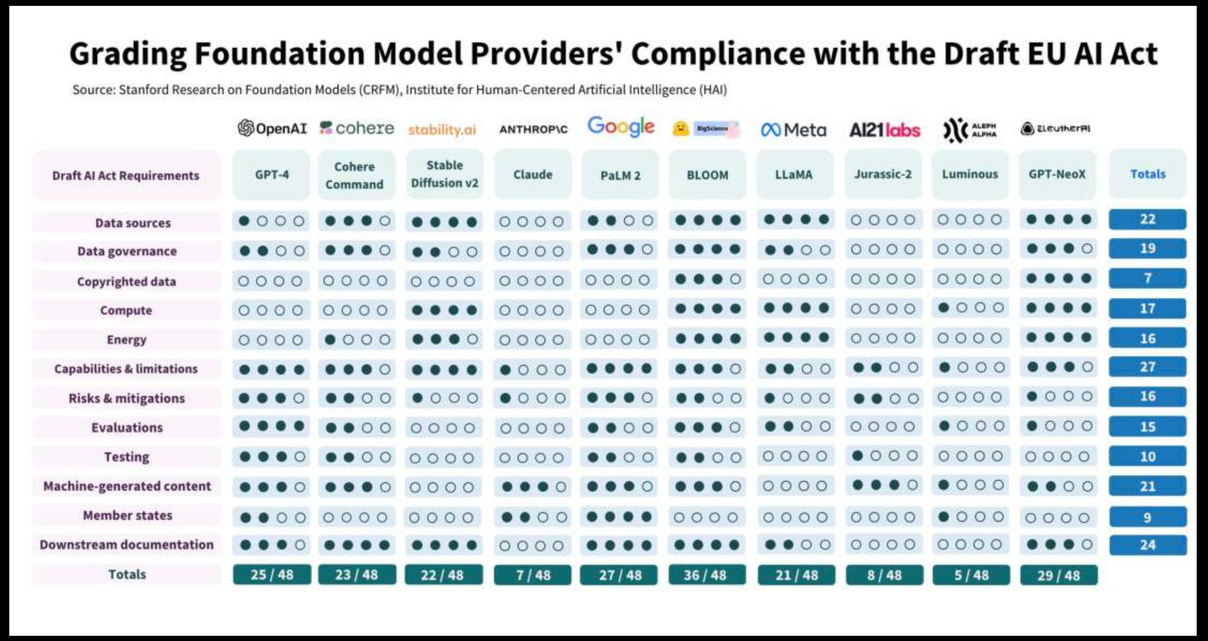
Expert Group*

National level

National Competent Authority/ies

COMPLIANCE

- EU Member-States are responsible for enforcing the regulation. Penalties for infringement can be up to €30 million or 6% of the worldwide annual turnover, whichever is higher.



Grading Foundation Model Providers' Compliance with the Draft EU AI Act

Source: Stanford Research on Foundation Models (CRFM), Institute for Human-Centered Artificial Intelligence (HAI)

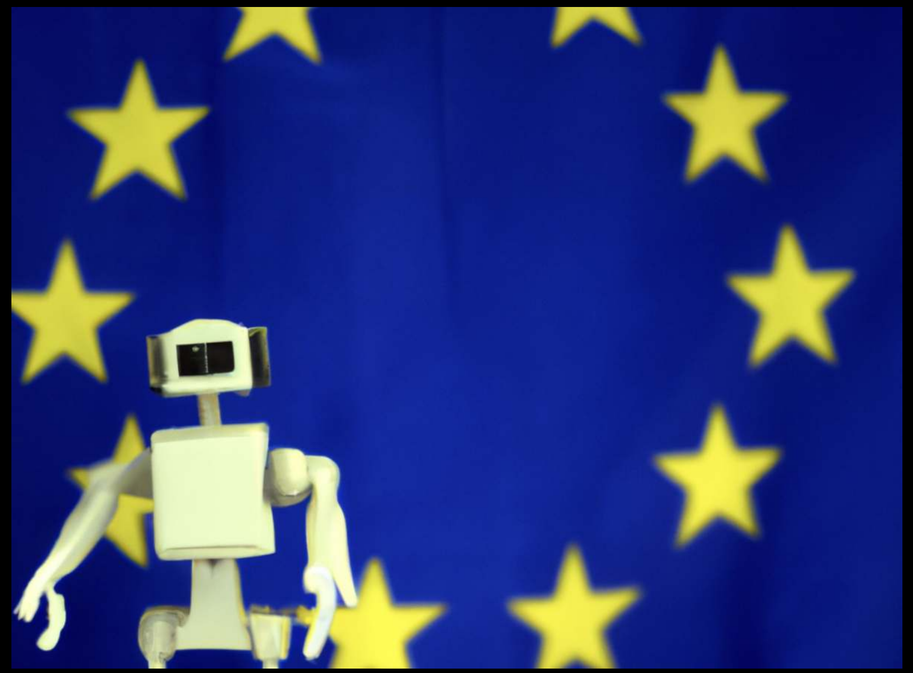
Draft AI Act Requirements	GPT-4	Cohere Command	Stable Diffusion v2	Claude	PaLM 2	BLOOM	LLaMA	Jurassic-2	Luminous	GPT-NeoX	Totals
Data sources	● ○ ○ ○	● ● ● ○	● ● ● ●	○ ○ ○ ○	● ● ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	22
Data governance	● ● ○ ○	● ● ● ○	● ● ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	19
Copyrighted data	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	7
Compute	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ○ ○ ○	● ● ● ●	17
Energy	○ ○ ○ ○	● ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	16
Capabilities & limitations	● ● ● ●	● ● ● ○	● ● ● ●	● ○ ○ ○	● ● ● ●	● ● ● ○	● ● ○ ○	● ● ○ ○	● ○ ○ ○	● ● ● ○	27
Risks & mitigations	● ● ● ○	● ● ○ ○	● ○ ○ ○	● ○ ○ ○	● ● ● ○	● ● ○ ○	● ○ ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	16
Evaluations	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ● ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	● ○ ○ ○	15
Testing	● ● ● ○	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ○ ○	○ ○ ○ ○	● ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	10
Machine-generated content	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ○ ○ ○	● ● ○ ○	21
Member states	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ○ ○ ○	○ ○ ○ ○	9
Downstream documentation	● ● ● ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ● ● ●	● ● ● ●	● ● ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	24
Totals	25 / 48	23 / 48	22 / 48	7 / 48	27 / 48	36 / 48	21 / 48	8 / 48	5 / 48	29 / 48	

NEXT STEPS – LEGISLATIVE PROCESS

- On 14 June 2023, MEPs adopted Parliaments negotiating position on the AI Act with 499 votes in favour, 28 against, and 93 abstentions.
- The Parliament has emphasised several aspects of their position: 1) going for a full ban on AI for biometric surveillance, emotion recognition, and predictive policing; 2) requiring generative AI systems like ChatGPT to disclose that content was AI-generated; and 3) considering AI systems used to influence voters in elections to be high-risk.
- The talks have now begun with EU countries in the Council on the final form of the law. The aim is to reach an agreement by the end of this year.

FROM REGULATION TO LAW

- Its obligations are likely to apply three years after the AI Act’s entry into force (by the end of 2025).



INTERNATIONAL EFFORTS TO REGULATE AI

KEY PLAYERS ON ARTIFICAL INTELLIGENCE

- EUROPEAN UNION (EU)
- USA
- CHINA

WHICH ARE THE DIFFERENCES BETWEEN THE EU APPROACH AND US & CHINA APPROACH??

A REGULATION APPROACH COMPARISON

	CHINA	EUROPE	USA
STRATEGY	STATE	HUMAN-CENTRIC	BUSINESS
APPROACH	FROM ABOVE	IN BETWEEN	FROM BELOW
IMPLEMENTATION	CENTRAL	INSTRUMENTAL	AUTONOMUS
FUNDING	PUBLIC	PUBLIC-PRIVATE	PRIVATE
TEMPER	POSITIVE	SCEPTICAL	NEUTRAL
REGULATION	SOFT	STRICT	MEDIUM

- International efforts to regulate AI: In February 2022, US lawmakers reintroduced a proposal for an Algorithmic Accountability Act; and in October, the US presented a Blueprint for an AI Bill of Rights, a set of guidelines to encourage companies to make and deploy AI more responsibly.
- Last spring, China introduced rules that prohibit algorithmic discrimination (the Internet Information Service Algorithmic Recommendation Management Provisions); and rules for disclosing synthetic content (deepfakes) (Provisions on the Administration of Deep Synthesis Internet Information Services)
- The Council of Europe set up in 2022 a Committee on Artificial Intelligence tasked with developing an international treaty on AI focusing on human rights, the rule of law, and democracy (the CAI held its inaugural meeting on 4 April 2022). The OECD and UNESCO have continued to support and promote a global approach and shared governance frameworks for AI risks and opportunities.

USA APPROACH

- The U.S.A.'s National Artificial Intelligence Initiative (NAII) was born out of the National AI Initiative Act of 2020 (DIVISION E, SEC. 5001) which became law in the United States on January 1, 2021.
- 6 key strategic pillars: Innovation, Advancing trustworthy AI, Education and training, Infrastructure, Applications, International cooperation.
- The USA's proposed approach to AI risk assessment can be classified into 3 categories: assessment, independence and accountability, and continuous review.

CHINA APPROACH

- In 2017, China's State Council released its plan for the Development of New Generation Artificial Intelligence (Guo Fa [2017] No. 35). A first of its kind in China, the plan is positioned as a response to AI quickly becoming the new focus of international competition and proposed how China can become a leader in global AI development.
- From this, the plan has 3 objectives: create a new international competitive advantage stimulate the development of new industries enhance national security
- The plan aims to drive the development of AI technologies through a collaborative approach by private companies and local governments.

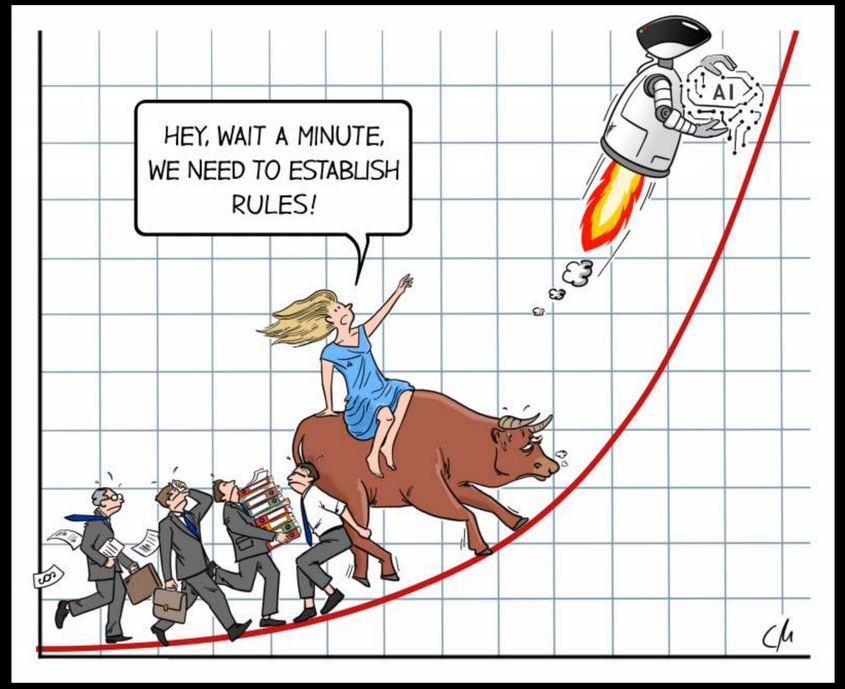
AI ACT & NATIONAL ADAPTATION

- The AI Act, in its current form, would make it difficult for Member States to regulate this technology at national level. This is particularly relevant considering how wide a concept of ‘AI system’ the regulation embraces.
- Some scope for regulatory intervention is nevertheless left to Member States. AI applications for military use are not covered. Also, the proposal leaves room for national discretion in adjusting the AI regime to the national contexts.
- A notable example is the penalties regime, which is for the Member States to define, subject to compliance with the Regulation and provided that sanctions are effective, proportionate and dissuasive.
- Also, Member States can decide not to subject public authorities and bodies to administrative fines.

- If approved in its current form, the AI Act would affect national legal and administrative systems in two main ways. Authorities would be required to have appropriate human resources and technical tools.
- The Act would also influence modernisation of the administrative and judicial activity and of law enforcement.
- Indeed, the proposed Regulation curtails options, subjects the use of AI systems in some areas to strict regulatory requirements and makes modernisation efforts relying on AI more resource-intensive.

AREA FOR IMPROVEMENT

- Is the ACT future-proofed?
- Is it providing protection mechanisms for individuals?



QUO VADIS AI ACT?

Future Challenges

UPCOMING CHALLENGES

- How to ensure the enforceability of the AI Act
- How to ensure the Act remains relevant with the passage of time and the evolution of technology
- the geopolitical context surrounding AI's development
- AI uses in defence and Autonomous Weapons Systems
- regulatory efforts in other parts of the world, like the US
- the global standards we need to evaluate AI
- what steps we must take to get closer to an international agreement and governance mechanisms for this ground-breaking technology
- The AI Act must allow for innovation to take place

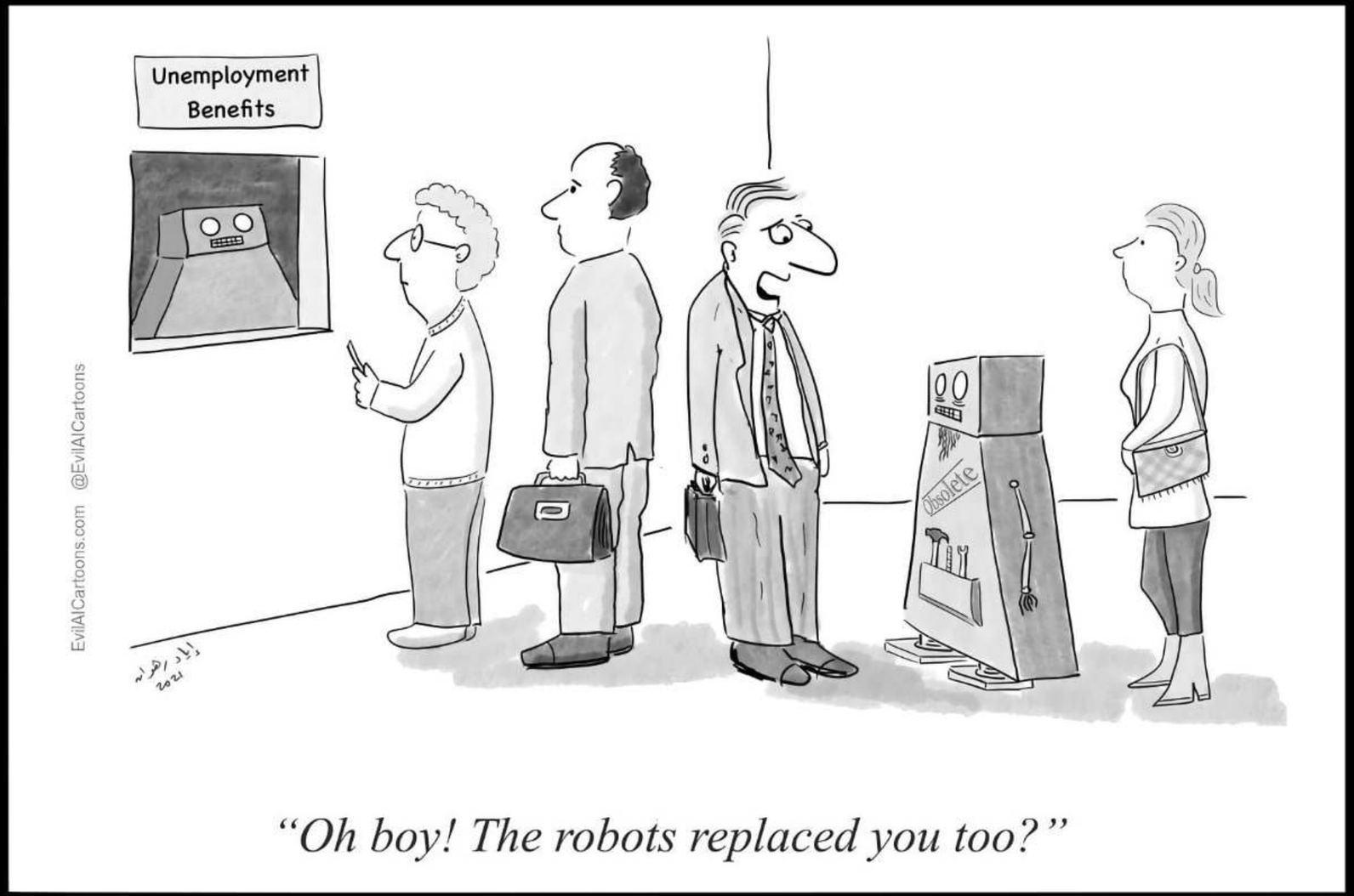
"It's not fun to be regulated but artificial intelligence may need it."

Elon Musk

CEO of Twitter

CONCLUSION

- With the AI Act, Europe is proposing an innovative way to regulate AI – through human- centred lenses and a risk-based approach that escalates obligations for AI applications depending on the risk they pose to health, safety, or fundamental human rights.
- The EU is leading these efforts, which are likely to create another Brussels Effect: by incentivising changes in products offered in non-EU countries (companies will find it more convenient to offer EU-compliant products everywhere they operate); and by influencing regulation adopted by other countries in order to build frameworks that are more ethical and human- centric.
- At the end of the day, the AI Act is a pioneering piece of legislation that shows that legal frameworks can not only catch up with technological advancements, but also help shape their future development for the benefit of all.



"Oh boy! The robots replaced you too?"

THANK YOU