KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

Universiteit Leiden

imec

The AI Act – Where are we at?

dr. Jan De Bruyne
Research Expert KU Leuven CiTiP
Senior Researcher Knowledge Centre Data & Society
Assistant professor elaw – University Leiden
Maître de conference, ULiège

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

KU Leuven Centre for IT & IP Law (CiTiP)

- Focus on fundamental re-thinking current legal framework necessitated by rapid evolution of technology in various fields
- Over 95 researchers specialised in legal & ethical aspects of IT innovation and IP
- Currently involved in more than 30 research projects funded by EU (H2020), Belgian Research Council, FWO, Flemish Government (AI Centre), other
- Involved in teaching, e.g. LLM Intellectual Property Rights and ICT Law

data protection & privacy

eHealth & pharma

ethics & Law

intellectual property

media & telecommunications

(cyber)security

AI and data

Knowledge Centre Data & Society

Studies in Media, Innovation and Technology (VUB)

Research group for Media, Innovation and Communication Technologies Ghent University

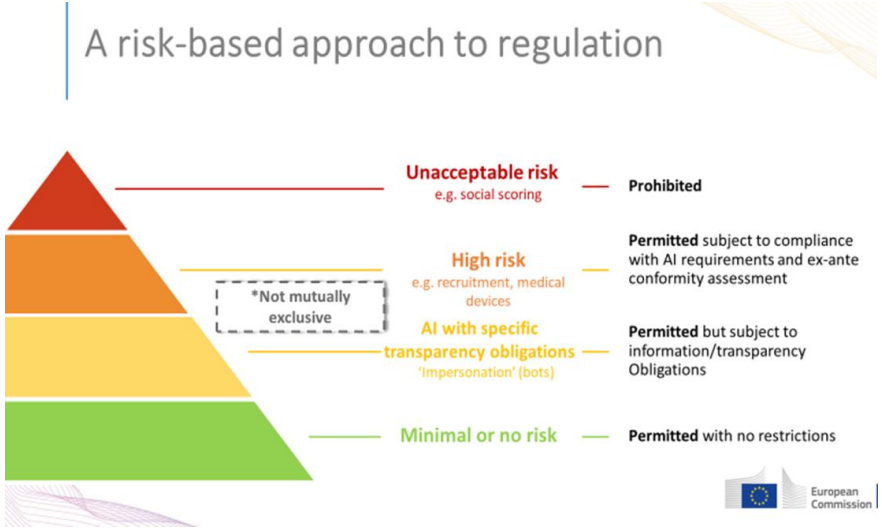
Centre for IT & IP Law

Organisational – general

- Established in 2019
- Funded by the Flemish Department of Science, Economy and Innovation (EWI)
- Yearly budget
- Part of Flemish AI Plan (three pillars)
  - strenghten basic strategic research
  - stimulate use of AI in companies
  - Raising awareness, training and ethical/legal framework

→ KCDS
→ Flemish AI Academy

Risk-Based Approach

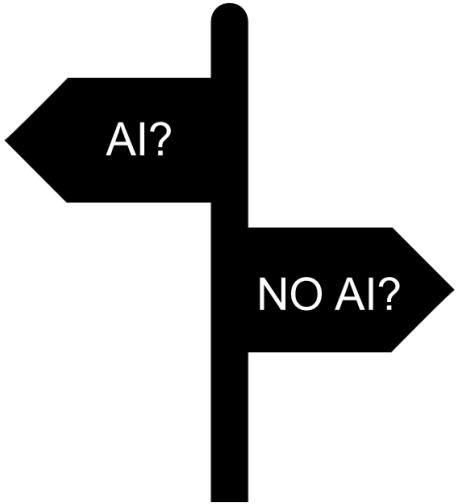


Council of the European Union

European Parliament

→ General principles for all AI operators
→ Environment

AI and Prohibited AIS



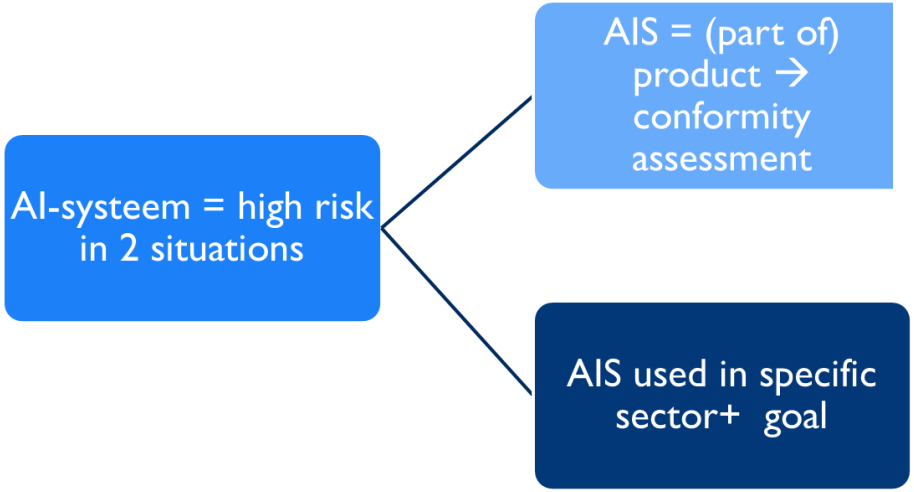
Council of the European Union

→ Notion AI (elements of autonomy)
→ Extended list proh. prac. (e.g. soc. scoring by private actors)

European Parliament

→ Notion AI (machine-based and varying levels autonomy)
→ Extended list proh. prac. (e.g. emo. recog. system in workplace,…)

High-risk AI



Council of the European Union

- Horizontal layer stand alone AIS

European Parliament

- More HR AIS (e.g. AI systems that influence voters)

Requirements high-risk AI (providers)

Risk management system

- periodical risk analysis
- iterative process entire lifecycle
- different measures
- Testing AI systems to identify most appropriate risk manag. measures

Data management and data governance

- appropriate data governance and management practices
- data quality measures (relevant, representative, free of errors and complete)

Technical documentation

- goal: facilitating control
- Annex IV (*process for development, design specifications of the system, testing procedures,…)*

Registration

- goal: traceability working AI system
- automatic recording of events: "logging"
- register stand alone AIS in EU database
- Minimal requirements for biometric identification

Requirements high-risk AI (providers)

Transparency and provision of information to users

- Goal: enable users to interpret the system's output and use it appropriately
- Instructions of use (with minimum information)
  - *Intended purpose, level of accuracy, robustness and cybersecurity, specifications for the input data,..*

Human oversight

- Goal: allow efficient oversight humans
- Built in system or by user
- Minimal requirements
  - *monitor working*
  - *automation bias*
  - *disregard, override or reverse the output*
  - *intervene on the operation*

Accuracy, robustness and cybersecurity

- **Accuracy**: included in IoU
- **Robustness**: through technical redundancy solutions,..
- **Cybersec.:** measures against data poisoning, adversarial examples

GPAI / foundation models / generative AI

- Not addressed in initial EC Proposal (2021)
- Text Council (December 2022)
  - → certain requirements HR AIS would apply
  - → via implementing act (missed chance?)
- Text Parliament (May/June 2023)
  - → requirements foundation models (e.g. guarantee protection of fundamental rights, registration database,…)
  - → additional provisions for generative AI (e.g. transparency requirements, publishing summaries of copyrighted data used for training,…)

Some other points of attention

- User rights: file complaints & right of explanation decision AIS affecting fundamental rights
- AI literacy
- Regulatory sandboxes: innovation (but role EC)
- AI Office
- Exemptions for (scientific) research activities and development and AI components provided under open-source licenses
- Different authorities with different roles
- ….

Points for discussion

- Definition AI?
- Do companies already adopt best practices? What should be done in light AI Act?
- Horizontal or sectoral legislation?
- Requirements for training data realistic?
- Coordination with other (legal) regimes?
- What issues do you think are missing in the legal framework?
- Exception for research/development: pro-active compliance?
- Who enforce?
- How to certify AI?
- ….

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

Universiteit Leiden

imec

Thank you!
Q&A

contact
jan.debruyne@kuleuven.be
j.de.bruyne@law.leidenuniv.nl