AI Risk

on the Regulatory Horizon

Tobias Mahler, Professor, University of Oslo, VIROS Project

XXXV Nordic Conference in Law and IT, 2020

2020

EU Commission

AI White Paper

Member states call for soft law approach

EU Parliament: Proposal for a REGULATION on ethical principles for the development, deployment and use of artificial intelligence, robotics and related technologies

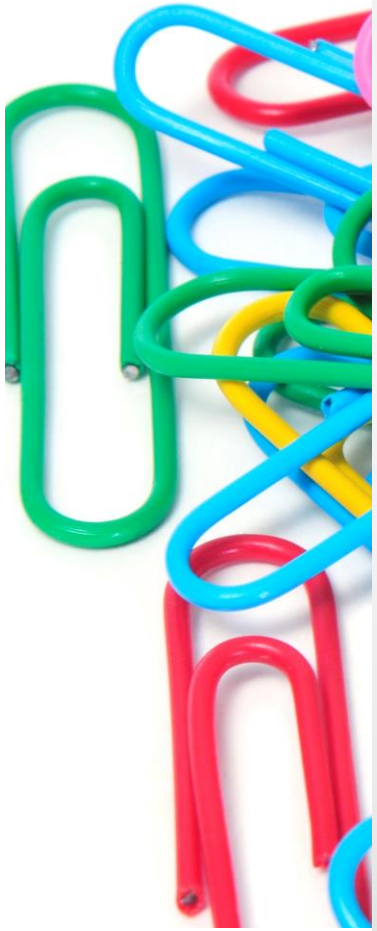
What are AI risks?

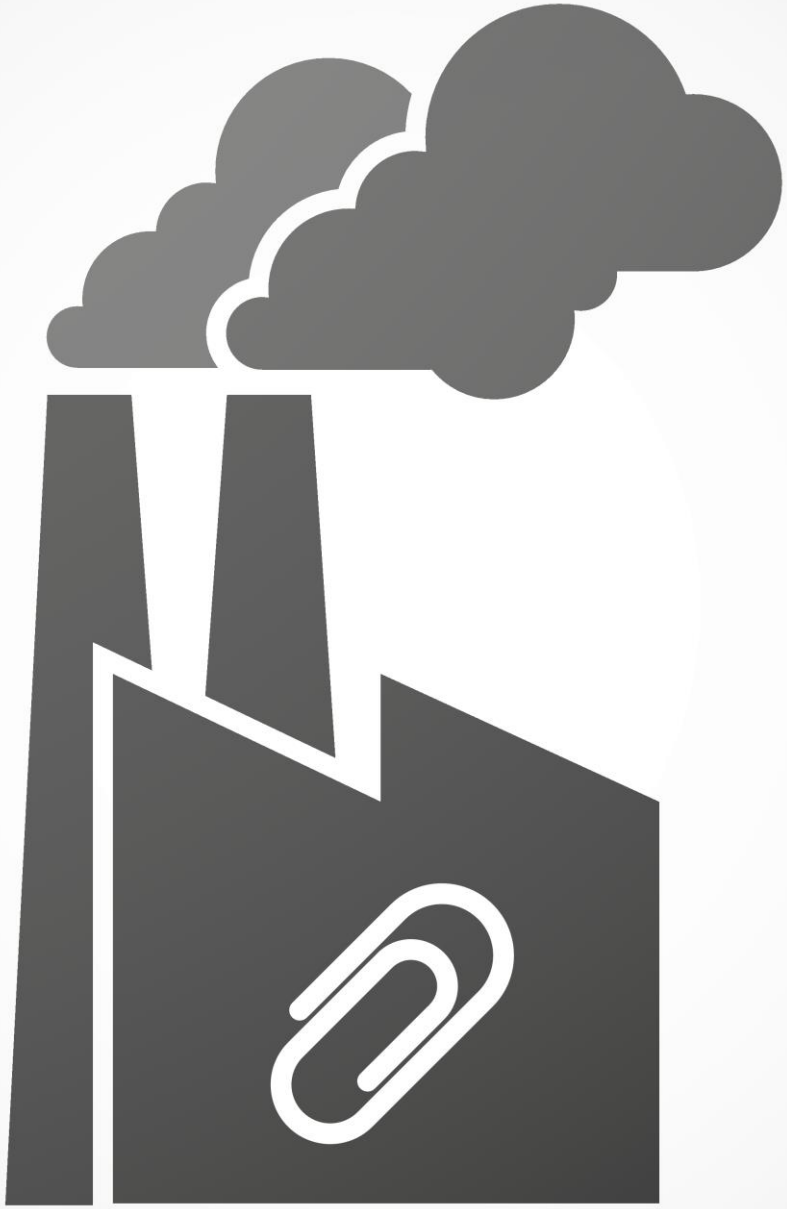
AI risks include

- Risks for fundamental rights, including personal data and privacy protection and non-discrimination
- Risks for safety and the effective functioning of the liability regime

(EU AI White Paper, pp 10-13)

Superintelligence (general AI): “maximise number of paperclips in the universe”





See further Nick Bostrom (2003). "Ethical Issues in Advanced Artificial Intelligence". *Cognitive, Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence*.

(How) should risk play a role for AI regulation?

AI risk = justification + focus for AI regulation

- A regulatory framework should concentrate on how to minimize (most significant) risks.

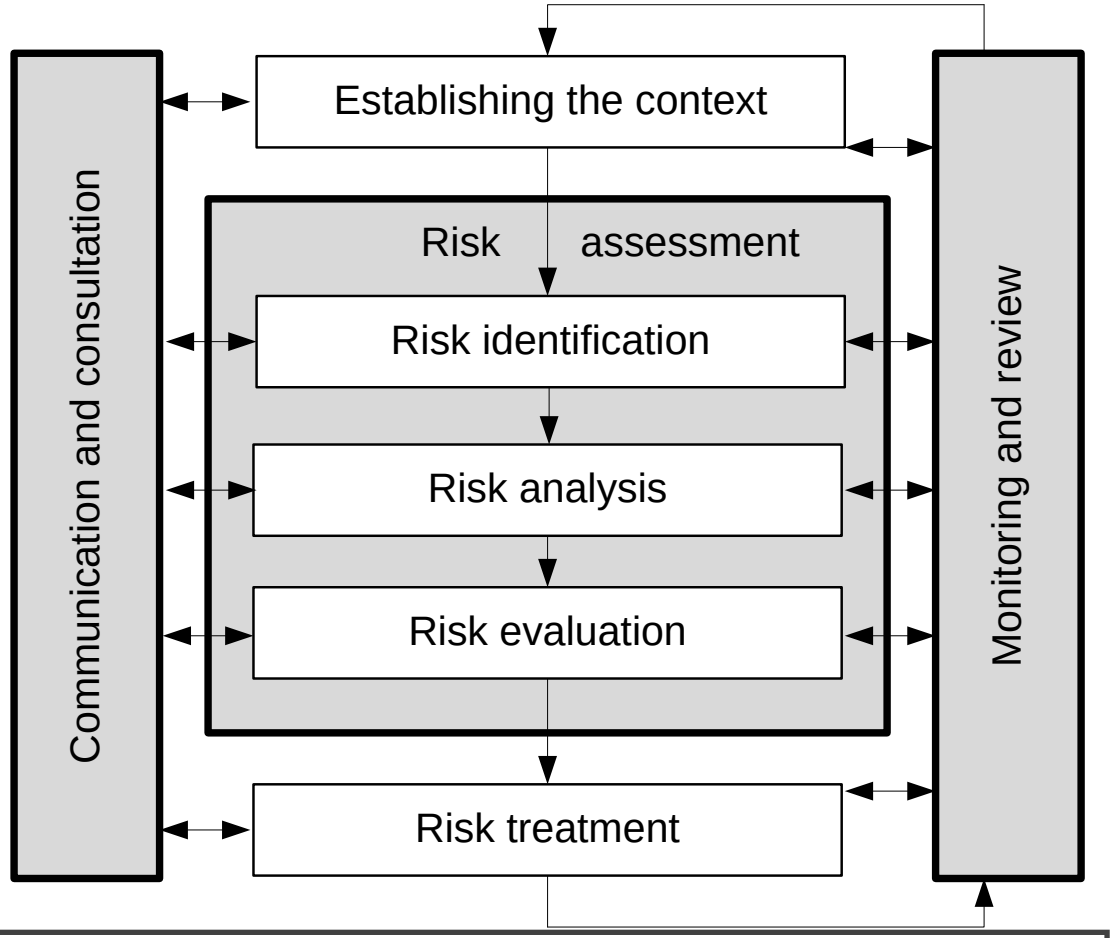
EU AI White Paper, p 10

Specific requirements for high-risk AI

TRANSPARENCY AND FAIRNESS

HUMAN CONTROL

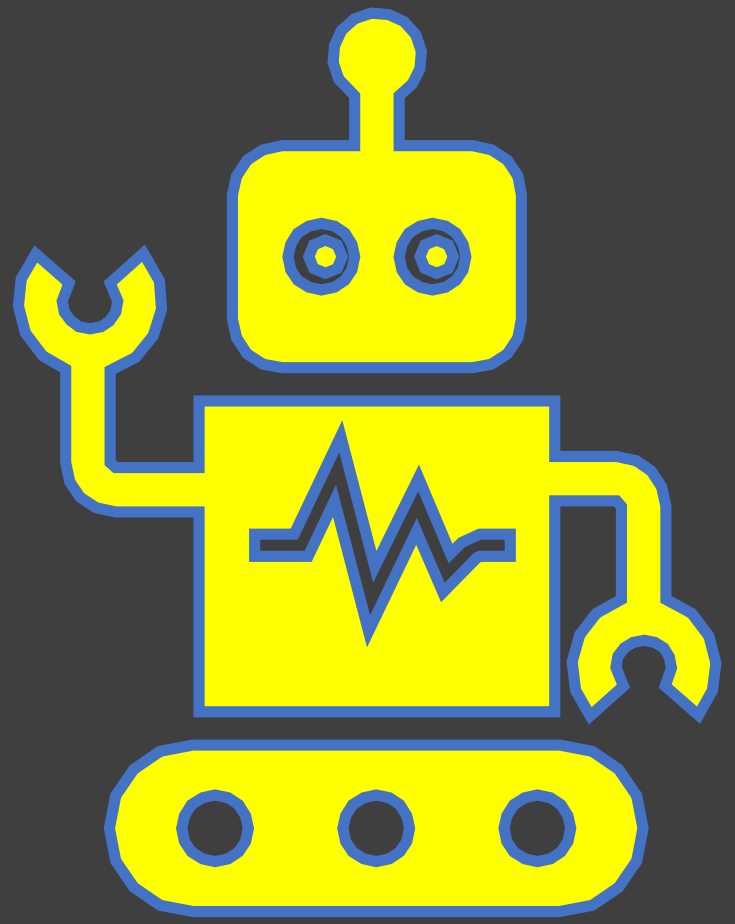
...



Risk = effect of uncertainty on objectives

ISO Guide 73, Risk management ISO 31000

A risk-based approach
OR
a rights-based approach
to AI regulation?



- AI regulatory framework should concentrate on how to minimize the various risks
- Risk assessment
  - High risk: specific regulation applies
  - Medium/low risk: voluntary labelling + general rules apply

(EU White Paper)

- Human rights impact assessment for AI in all domains
- Proponents e.g. Access Now

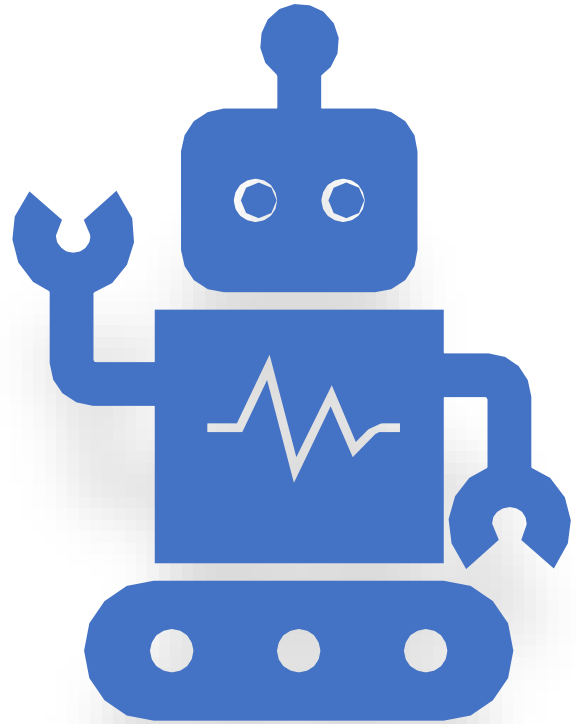
Risks to

A given AI application should generally be considered high-risk in light of what is at stake, considering whether

- both the sector and
- the intended use
- involve significant risks,
- in particular from the viewpoint of protection of safety, consumer rights and fundamental rights.

(White Paper, p 17)

IF (high) AI risk, THEN …?

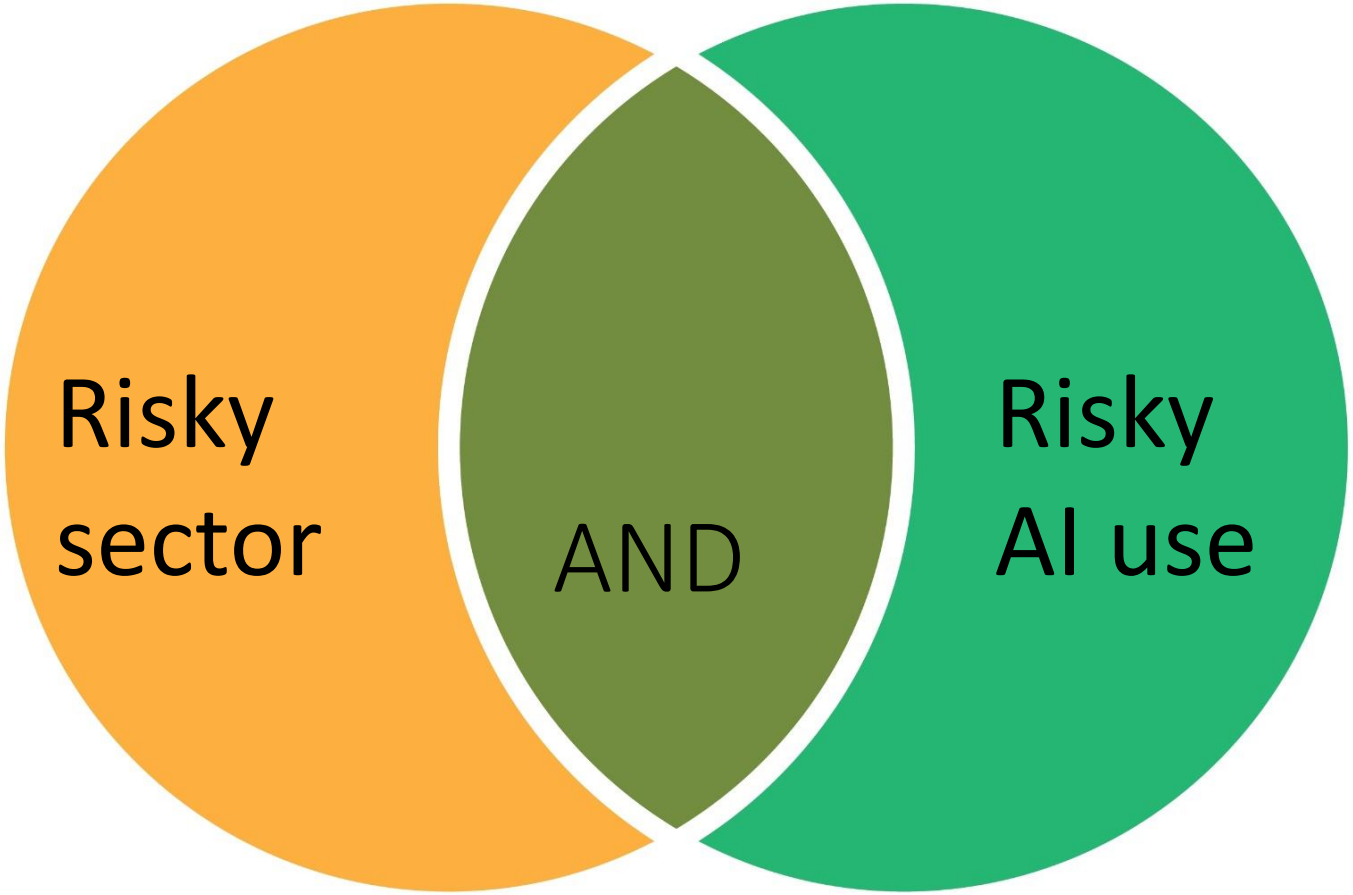


Specific obligations for high-risk AI

- Human control
- Safety, transparency and accountability
- Non-discrimination
- Social responsibility
- Environmental sustainability
- Privacy
- Redress for harm

Proposed EU Regulation on Ethical Principles

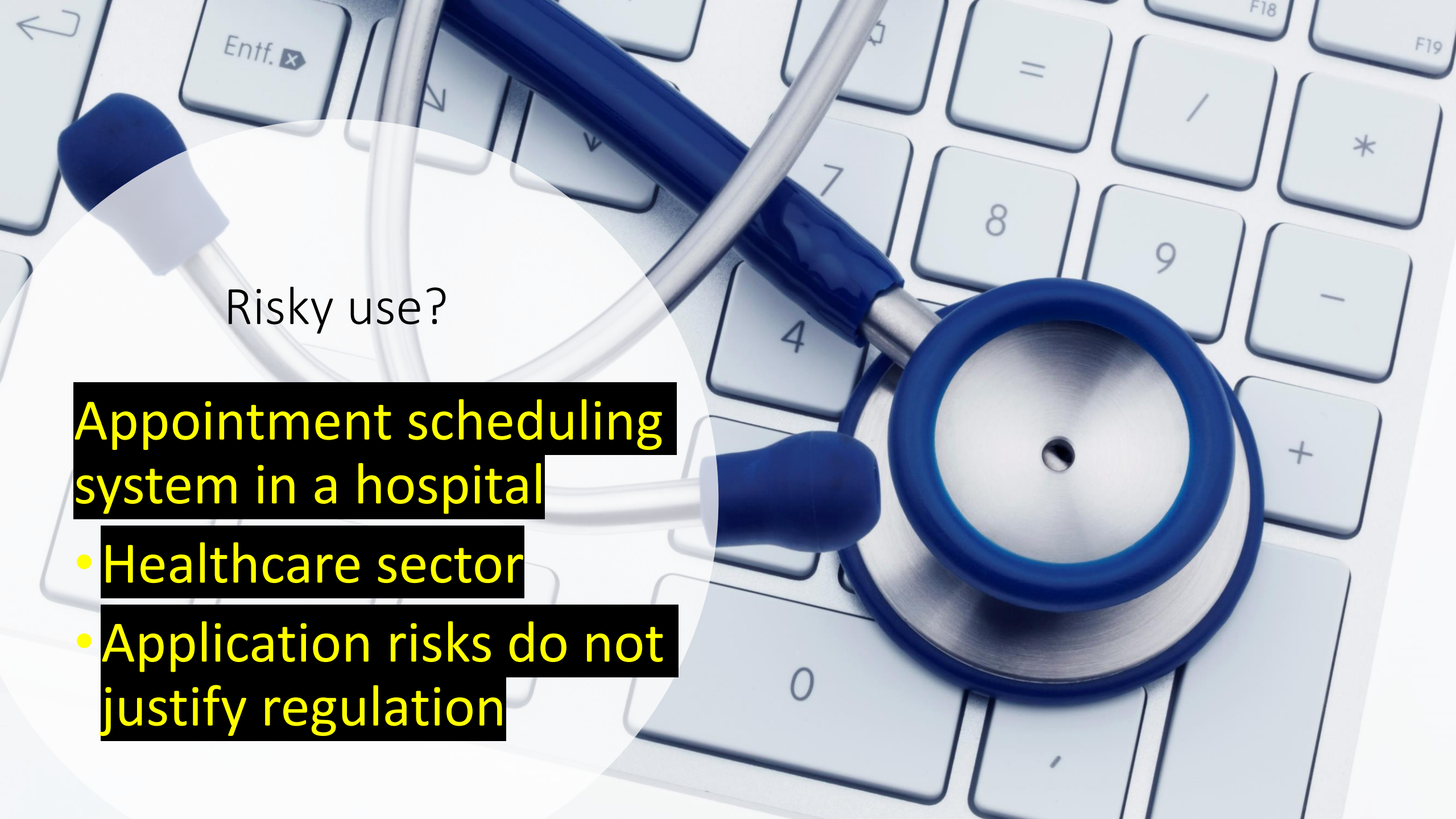
High risk AI



Cumulative criteria, Commission AI White Paper, p 17

High-risk sectors (EP)

- Employment
- Education
- Healthcare
- Transport
- Energy
- Public sector
  - asylum, migration, border controls,
  - judiciary and social security services
- Defence and security
- Finance, banking, insurance



Risky use?

Appointment scheduling system in a hospital

- **Healthcare sector**
- **Application risks do not justify regulation**

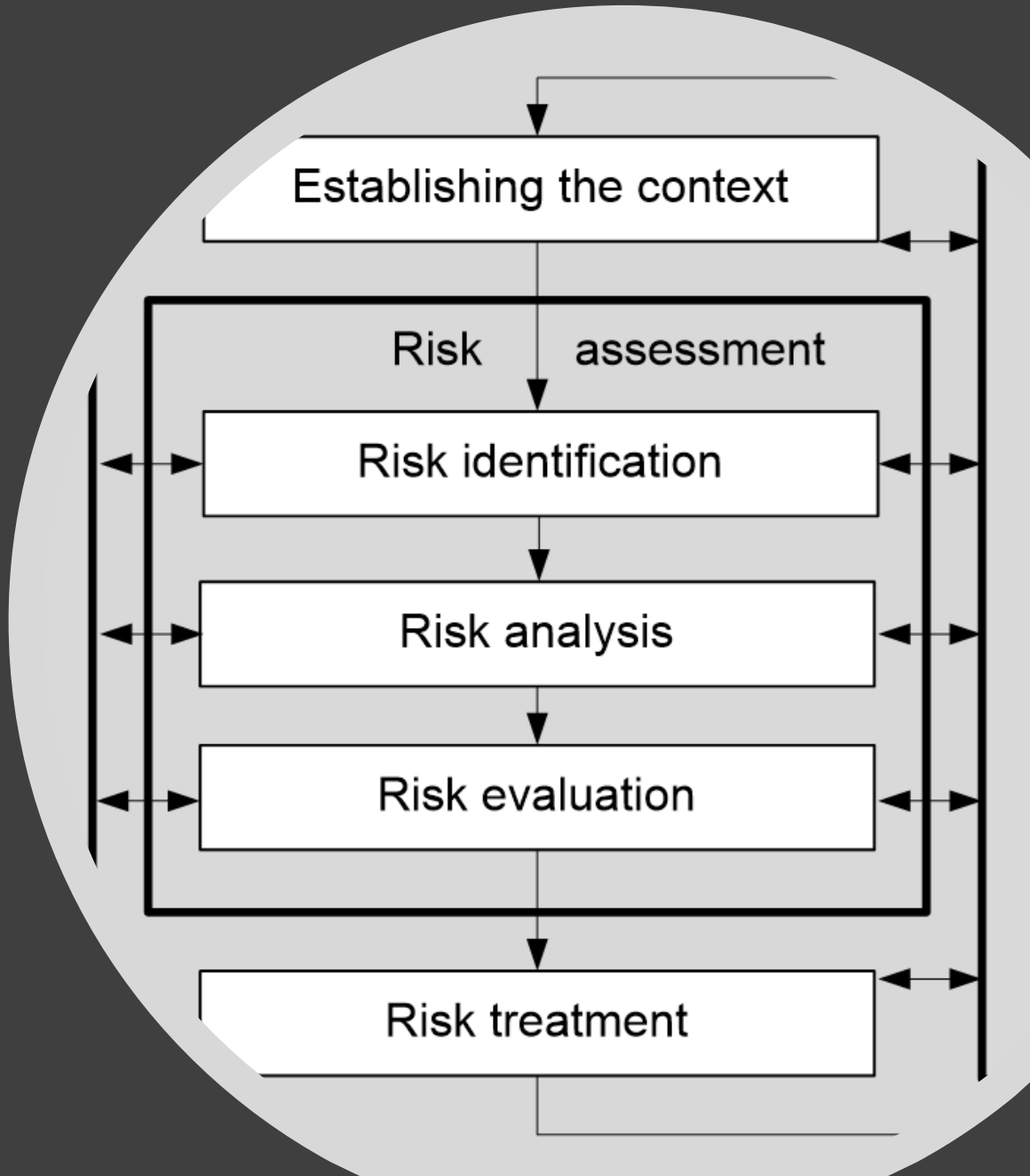
High-risk uses or purposes (EP)

- Recruitment
- Grading and assessment of students
- Allocation of public funds
- Granting loans
- Trading, brokering, taxation, etc.
- Medical treatments and procedures
- Electoral processes and political campaigns
- Public sector decisions (significant & direct impact)
- Automated driving
- Traffic management
- Autonomous military systems
- Energy production and distribution
- Waste management
- Emissions control
- AND?

Article 14, **Risk assessment** Proposed AI Regulation (EP)

AI high-risk:

- Risk assessment with objective criteria such as
  - sector
  - and severity of possible injury
- AI development, deployment or use entail a significant risk
- In breach of fundamental rights and safety rules as laid down in Union law



AI risk may be a key parameter for AI regulation

- ✓ AI risk *may* justify AI regulation
- ✓ EU AI regulation *will likely* be risk-based
- ✓ If high AI risk is the threshold, regulatory over-reach *may* be avoided
- ✓ Medium/low risk AI applications are *not necessarily* unregulated
- ✓ Risk-based AI regulation is *not necessarily* in conflict with rights-based regulation

Picture credits: Colourbox and private

VIROS Project Webinar - Challenges and Emerging Patterns of Robot Regulation

- The implementation of smart robotics in a growing number of areas of society raises various concerns to the industry, users, and regulators.
- Nov. 19, 2020 1:00 PM–4:00 PM, Webinar - Zoom
- This webinar explores the security, privacy, and safety dimensions of smart robotics. Three panels will address issues such as the use of smart robots in elderly care systems, robot impact assessment and risk management, as well as the privacy and safety dimensions in human-robot interaction.
- For full program click here
- Link to Zoom - click here
- https://www.jus.uio.no/ifp/english/research/projects/nrccl/viros/events/seminars/webinar-november-2020.html