

EU Artificial Intelligence Act AIA -rettsakten om kunstig intelligens

Tobias Mahler

Senter for rettsinformatikk, UiO

Forum rettsinformatikk 2021



CE

Etikk og menneskerettigheter

- Menneskelig tilsyn med algoritmer
- Diskriminering
- Ytringsfrihet
- Personvern

GDPR

- Rettigheter
- Risiko
- Tilsyn
- Regulatoriske sandkasser

Erstatning

- Nasjonal rett
- EU: Produktansvar
- Ansvar for roboter?

Produktsikkerhet

- Maskiner (roboter)
- Leketøy
- Medisinske apparater
- Tekniske standarder
- Sertifisering
- DSB

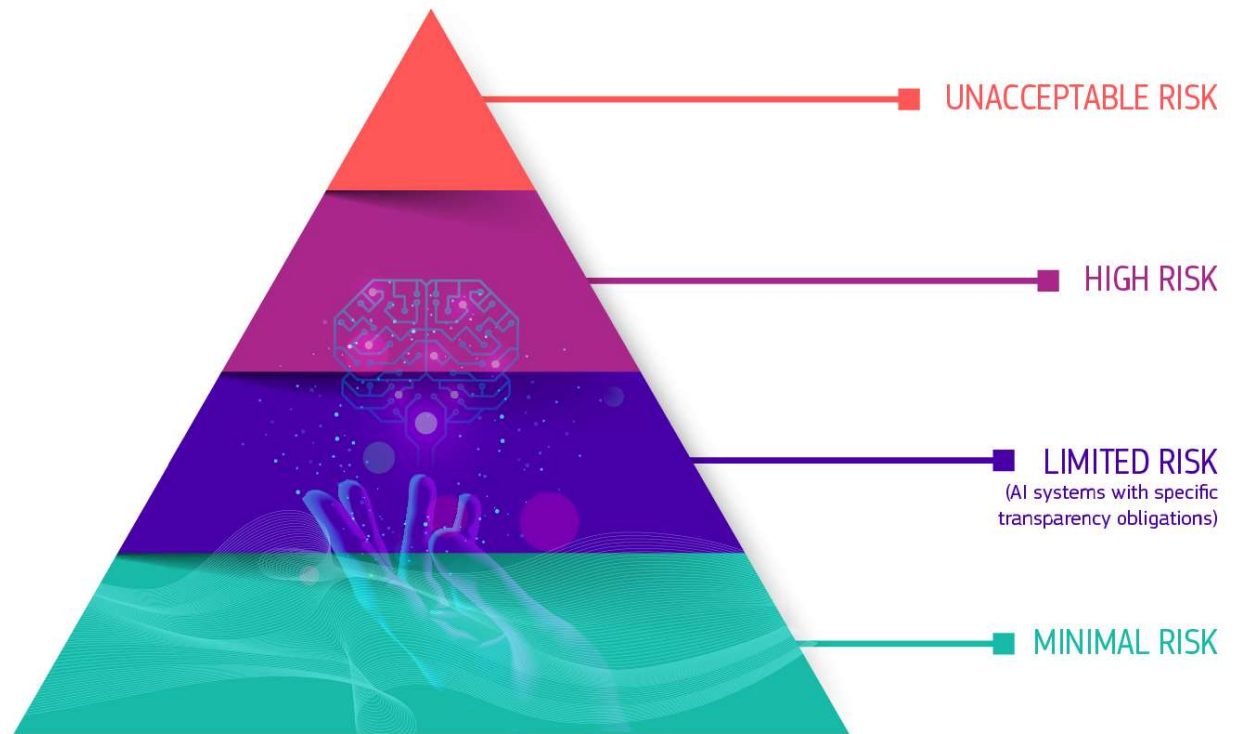
AI, Kunstig intelligens

(a) **Machine learning approaches**, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) **Logic- and knowledge-based approaches**, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) **Statistical approaches**, Bayesian estimation, search and optimization methods

Risikobasert tilnærming



Source:

https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en

The background of the slide is a dark blue gradient. On the left side, there are several overlapping, swirling, light blue scribbles that resemble a stylized, abstract shape or a collection of overlapping lines. The text is centered on the right side of the slide.

Dette er en forenkling!
(og en blanding av mange spark)

Forbud 1

(Manipulere personer)
gjennom subliminale teknikker
utenfor deres bevissthet
(og sannsynligvis forårsake skade)

(forenklet)



Colourbox

Forbud 2

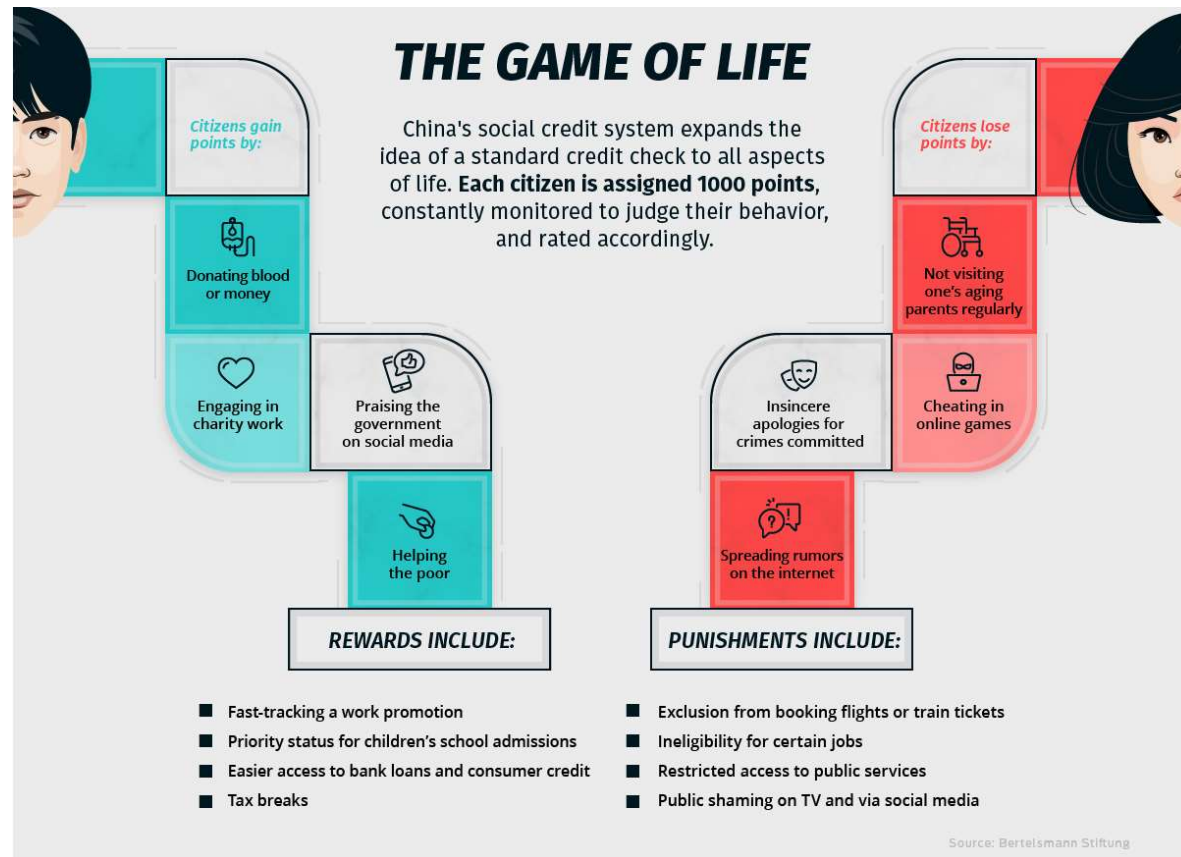
- Omsætning, ibrugtagning eller anvendelse af et **AI-system**,
- der **udnytter** enhver af en specifik **gruppe** af personers sårbarheder
- på grundlag af **alder** eller fysisk eller psykisk **handicap**
- med henblik på i væsentlig grad at **fordreje** en til gruppen hørende persons **adfærd** på en måde,
- der **påfører** eller sandsynligvis vil påføre den pågældende person eller en anden person fysisk eller psykisk **skade**



Colourbox

Forbud 3

- AI brukt av **offentlige myndigheter**
- Til **evaluering eller klassifisering** av fysiske personers troverdighet ... fører til:
- skadelig eller **ugunstig behandling** i sosiale sammenhenger,
 - som **ikke har sammenheng** med konteksten der dataene ble innsamlet, eller
 - som er **uberettiget** eller **uforholdsmessig** ...

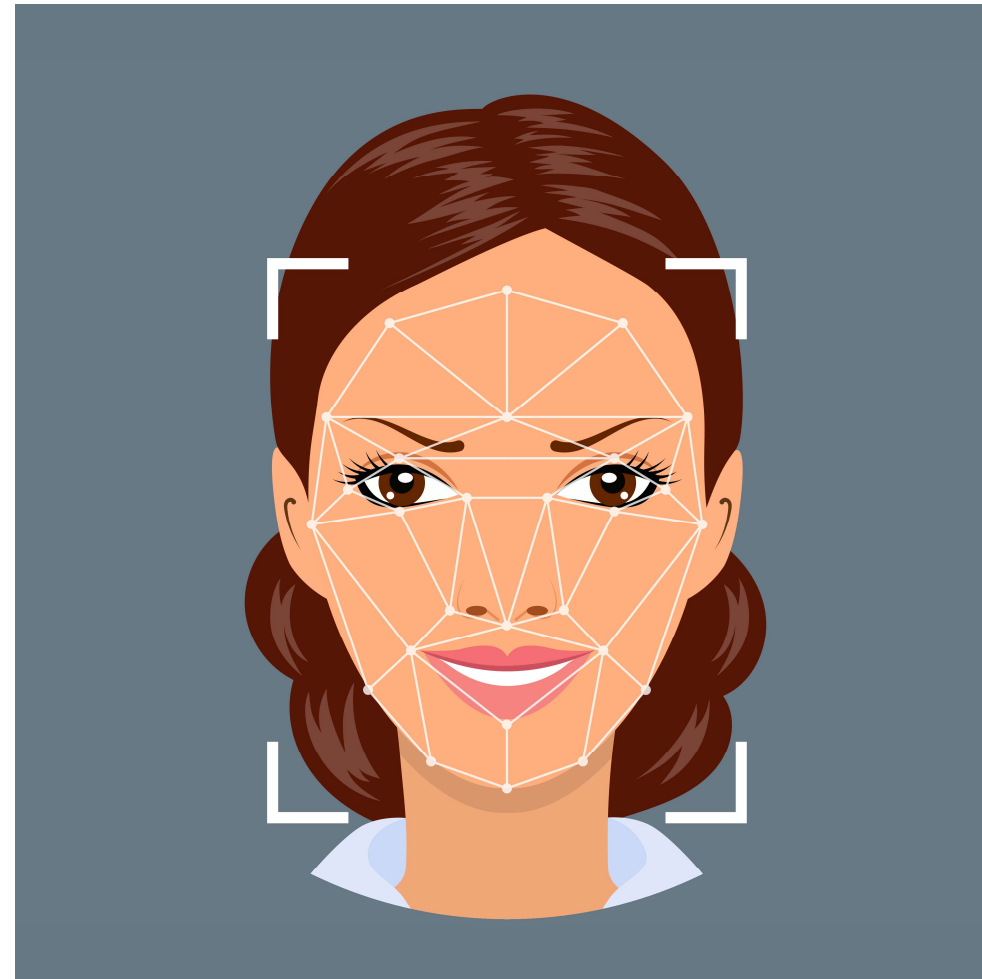


Bertelsmann Stiftung

Forbud 4, med unntak

Biometrisk fjernidentifikasjon i sanntid

- på **offentlige** steder
- med henblikk på **retshåndhevelse**, strengt nødvendig
 - i) til målrettet **søk etter ofre** (f eks forsvunne barn)
 - ii) **forebygging** av en ... **trussel** mot liv eller sikkerhet, eller terrorangrep
 - iii) avsløring, lokalisering, identifikasjon eller retsforfølgning av en **gjerningsperson**



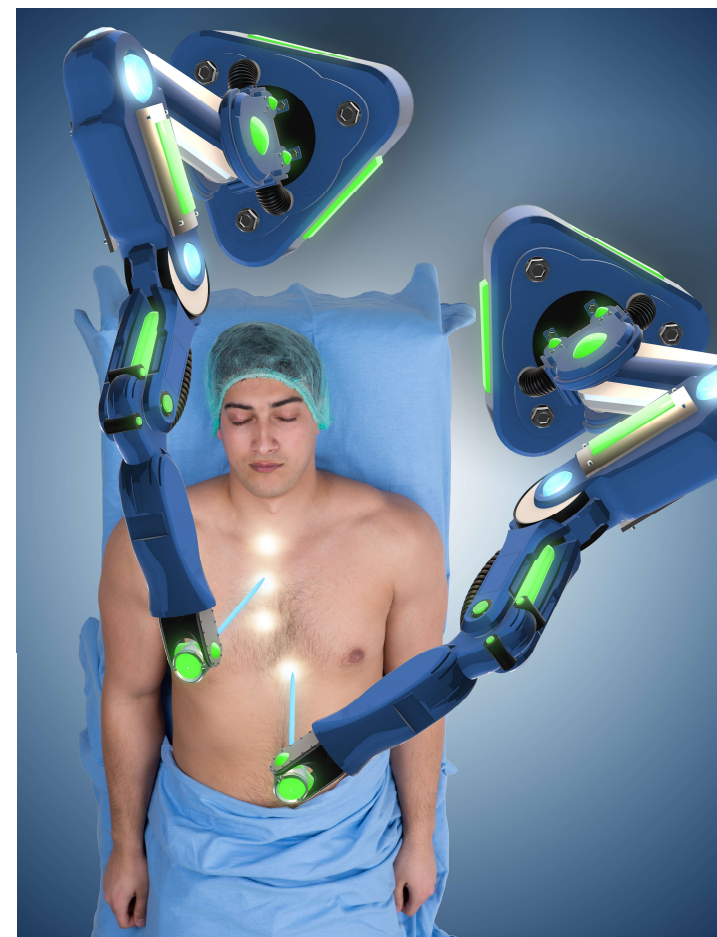
Source: Colourbox

Høyrisiko AI systemer 1

AI som sikkerhetskomponent for noen produkter

- underlagt tredjeparts forhåndsvurdering i henhold til EU-lov
- f.eks. maskiner, medisinsk utstyr

CE



Source: Colourbox

Frittstående høyrisiko AI systemer

1. Biometrisk identifikasjon og kategorisering
2. Forvaltning og drift av kritisk infrastruktur
3. Utdanning og yrkesopplæring
4. Ansettelse, arbeidsledelse & tilgang til selvstendig arbeid
5. Tilgang til essensielle private og offentlige tjenester
6. Lovhåndhevelse
7. Migrasjon, asyl og grensekontroll
8. Justisvesenet og demokratiske prosesser



Krav til høyrisiko AI systemer

- **Art. 9:** *Risikostyring*
- **Art. 10:** *Data & data governance*
- **Art. 11:** *Teknisk dokumentasjon*
- **Art. 12:** *Logfiler*
- **Art. 13:** *Transparens*
- **Art. 14:** *Menneskelig tilsyn*
- **Art. 15:** *Nøyaktighet, robusthet og cybersikkerhet*



Chatbots & deep fakes

Article 52: Transparens

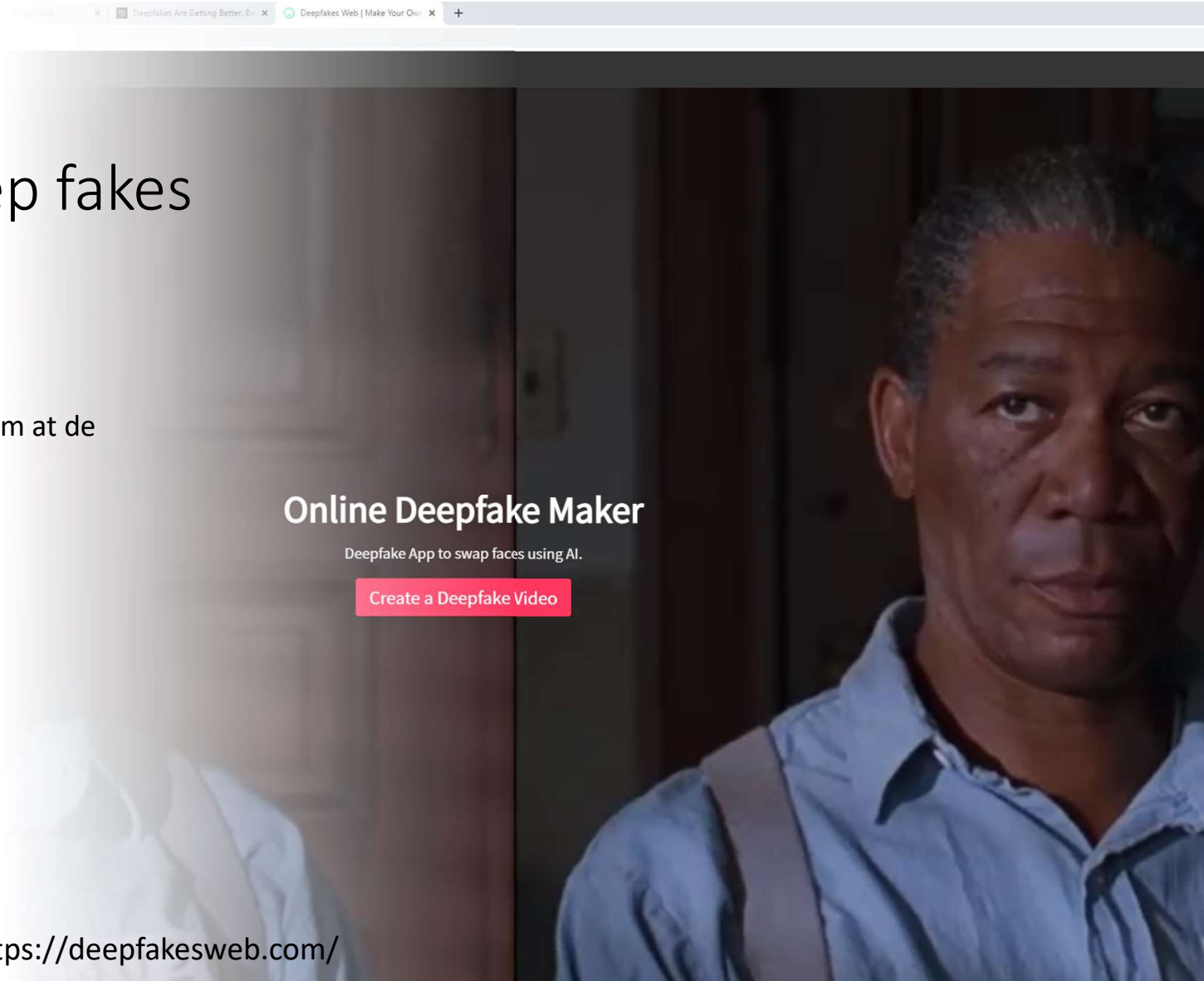
Krever at AI -systemer opplyser om at de er AI-systemer

- Chatbots
- Deep fakes

Unntak

- Med mindre det er åpenbart
- Lovhåndhevelse
- Ytringsfrihet, kunst, ...

Source: <https://deepfakesweb.com/>



Produktsikkerhet uten rettigheter?

