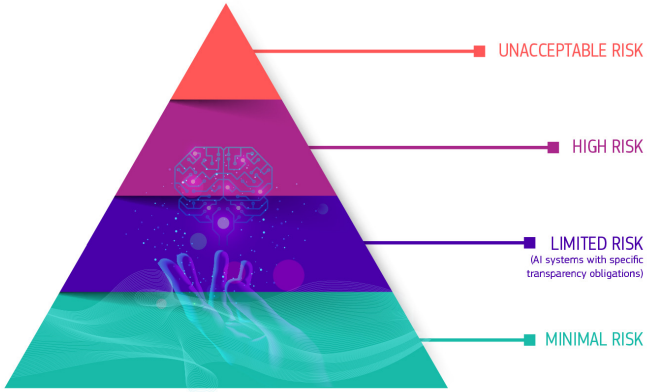
EU Artificial Intelligence Act
AIA
-rettsakten om kunstig intelligens

Tobias Mahler

Senter for rettsinformatikk, UiO

27. januar 2022



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

EU Commission:

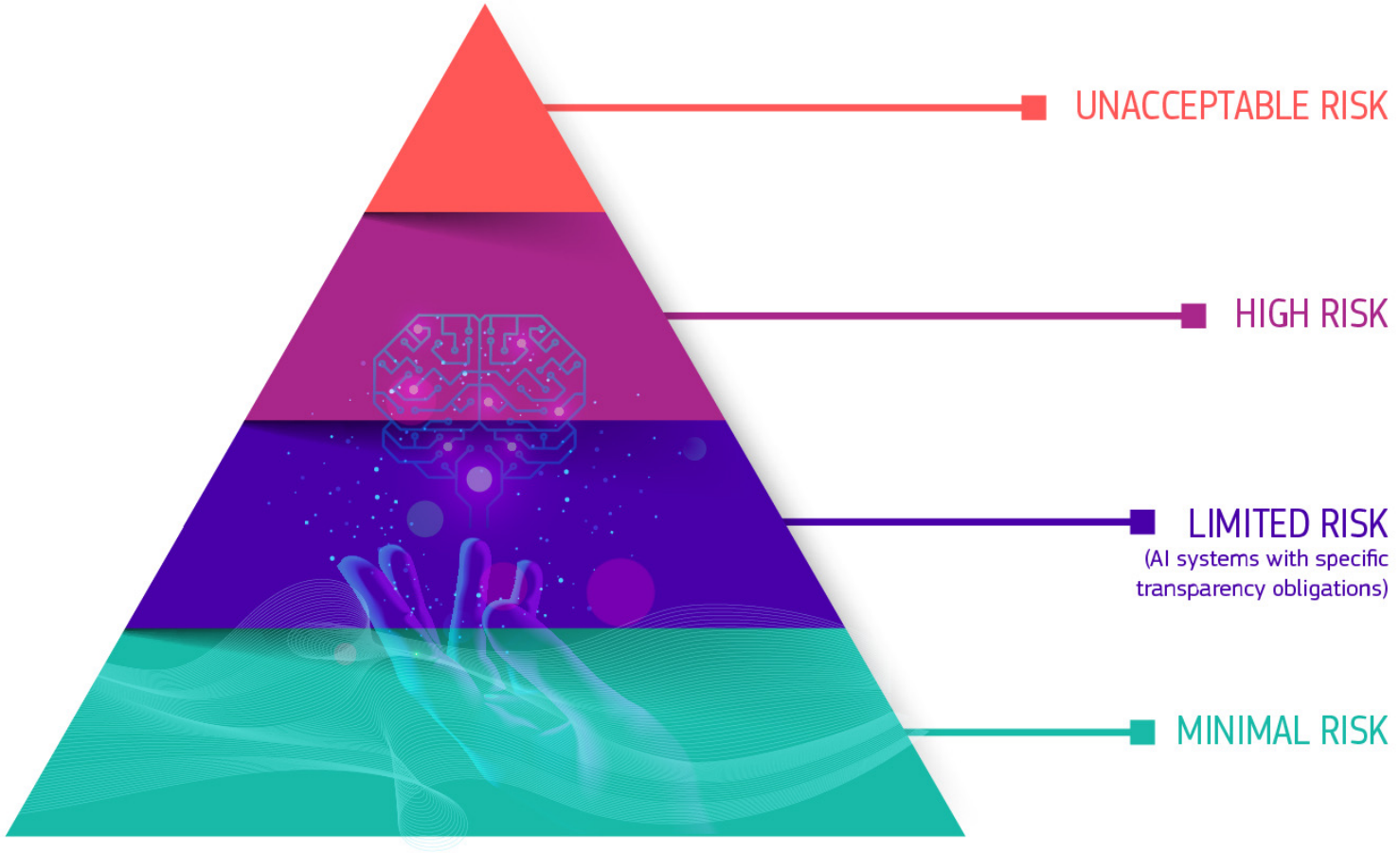
- ‘artificial intelligence system’ (AI system) means software
- that is developed with one or more of the techniques and approaches listed in Annex I and
- can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

Heislogikk?

EU Council: ‘artificial intelligence system’ (AI system) means a system that

- **(i) receives machine and/or human-based data and inputs,**
- **(ii) infers how to achieve a given set of human-defined objectives using learning, reasoning or modelling implemented with the techniques and approaches listed in Annex I, and**
- **(iii) generates outputs in the form of**
  - **content (generative AI systems),**
  - **predictions,**
  - **recommendations or**
  - **decisions,**
  - **which influence the environments it interacts with;**

Risikobasert tilnærming

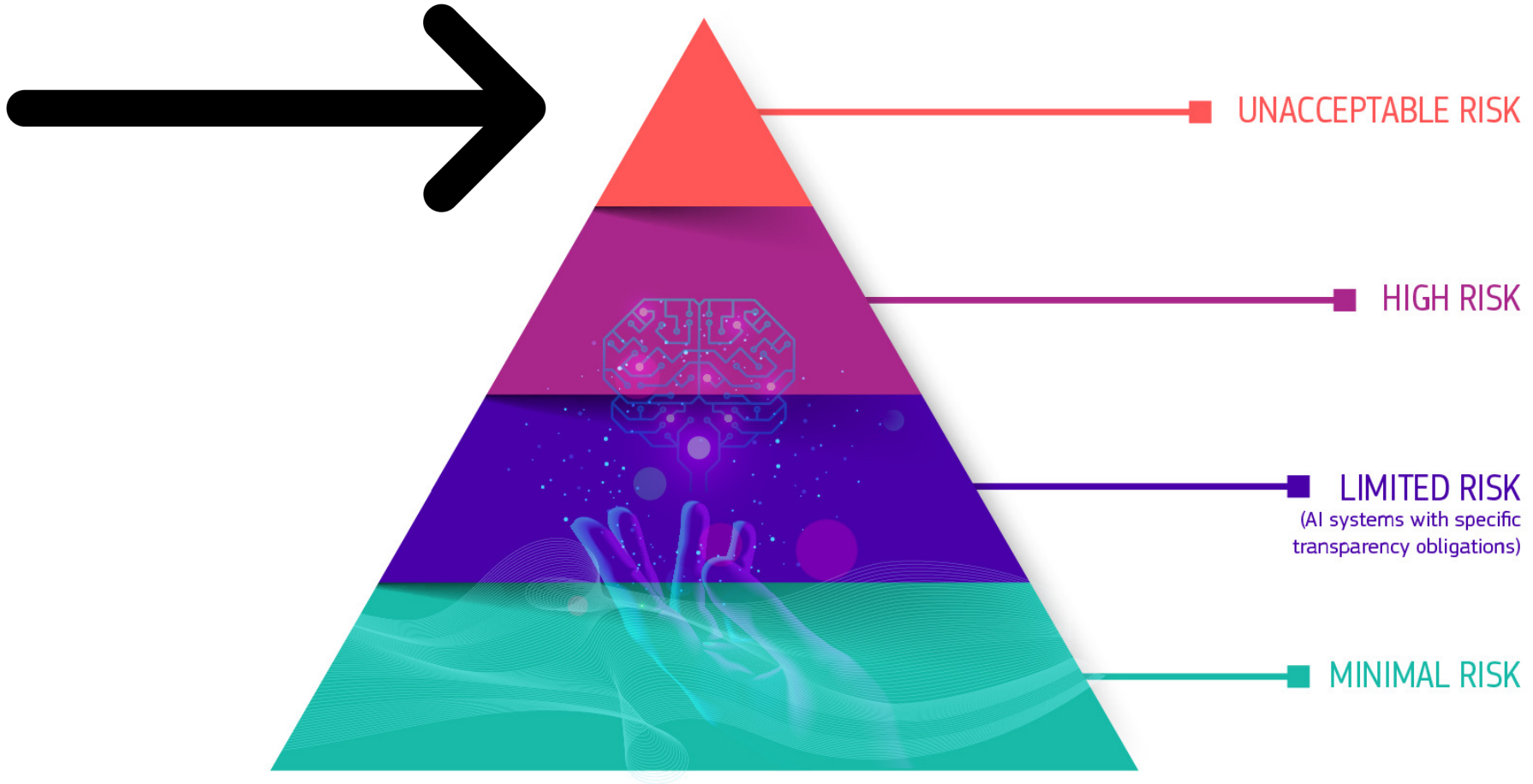


Source:
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en


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

Bøter

- The following infringements shall be subject to administrative fines of up to 30 000 000 EUR or, if the offender is company, up to 6 % of its total worldwide annual turnover for the preceding financial year, whichever is higher:
  - (a) non-compliance with the prohibition of the artificial intelligence practices referred to in Article 5;
  - (b) non-compliance of the AI system with the requirements laid down in Article 10.
- The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Articles 5 and 10, shall be subject to administrative fines of up to 20 000 000 EUR or, if the offender is a company, up to 4 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.


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

Forbud 1

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

(forenklet)

Colourbox

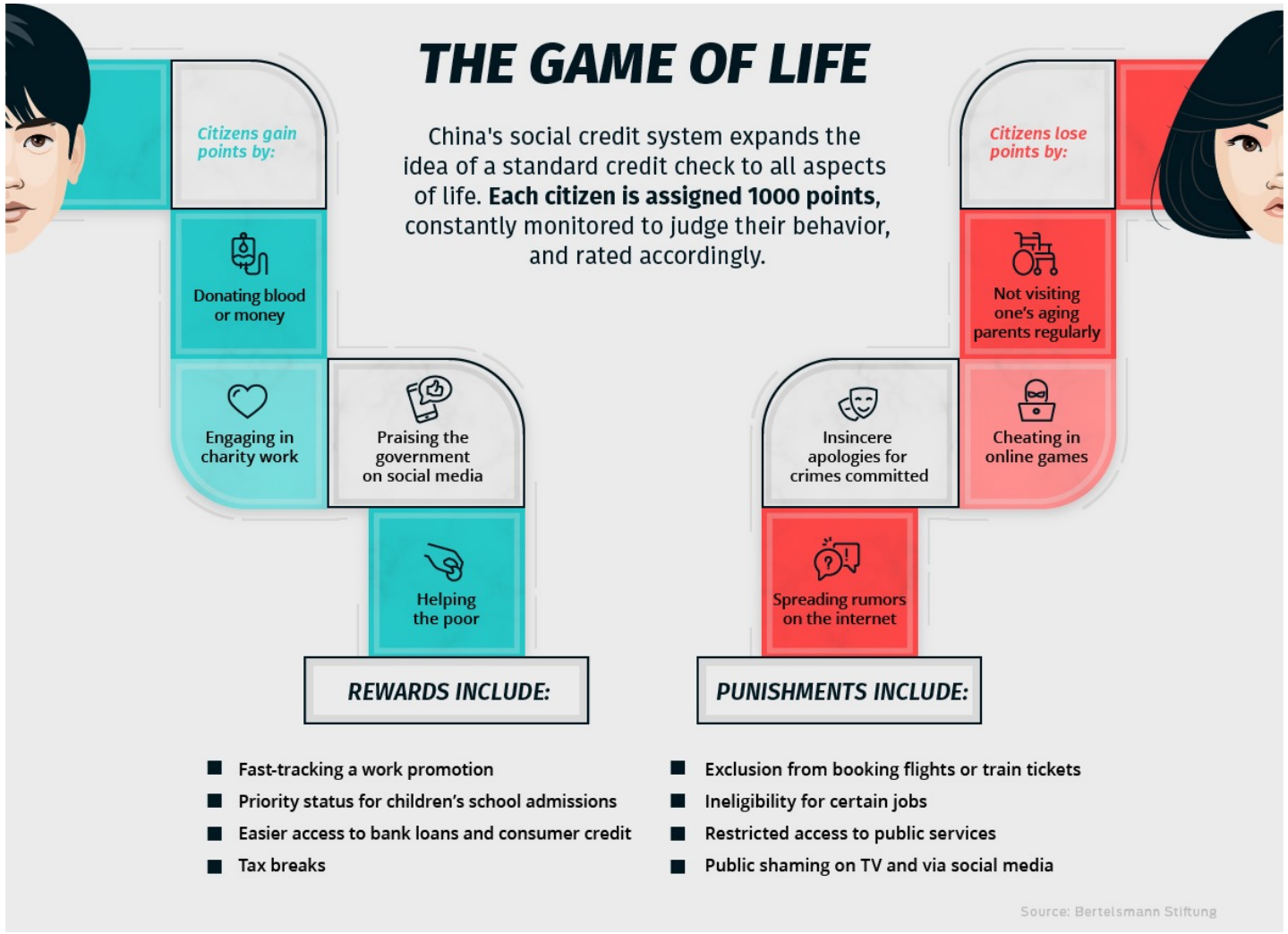
Forbud 2

- 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 sys. 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** ...

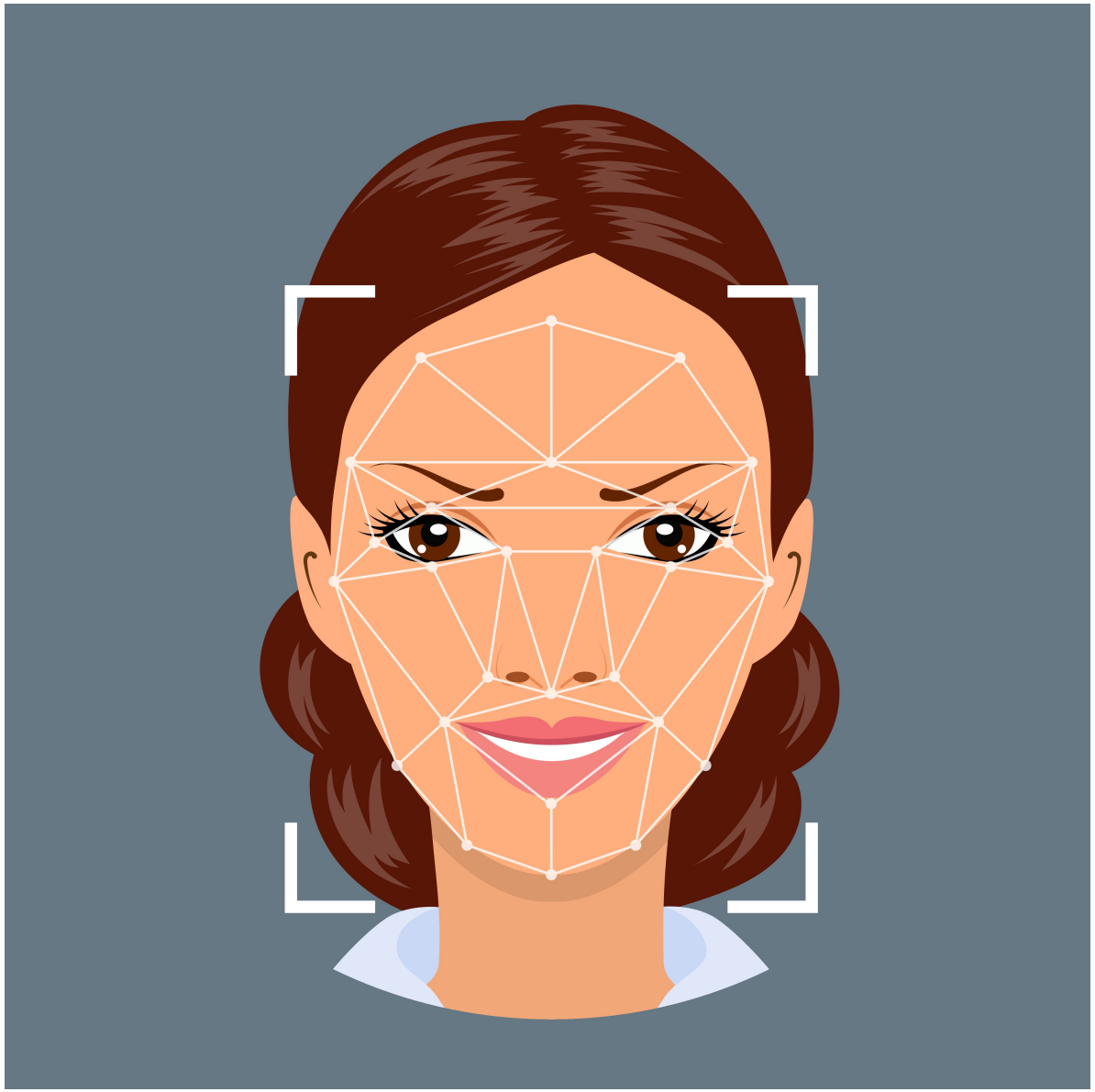


Bertelsmann Stiftung

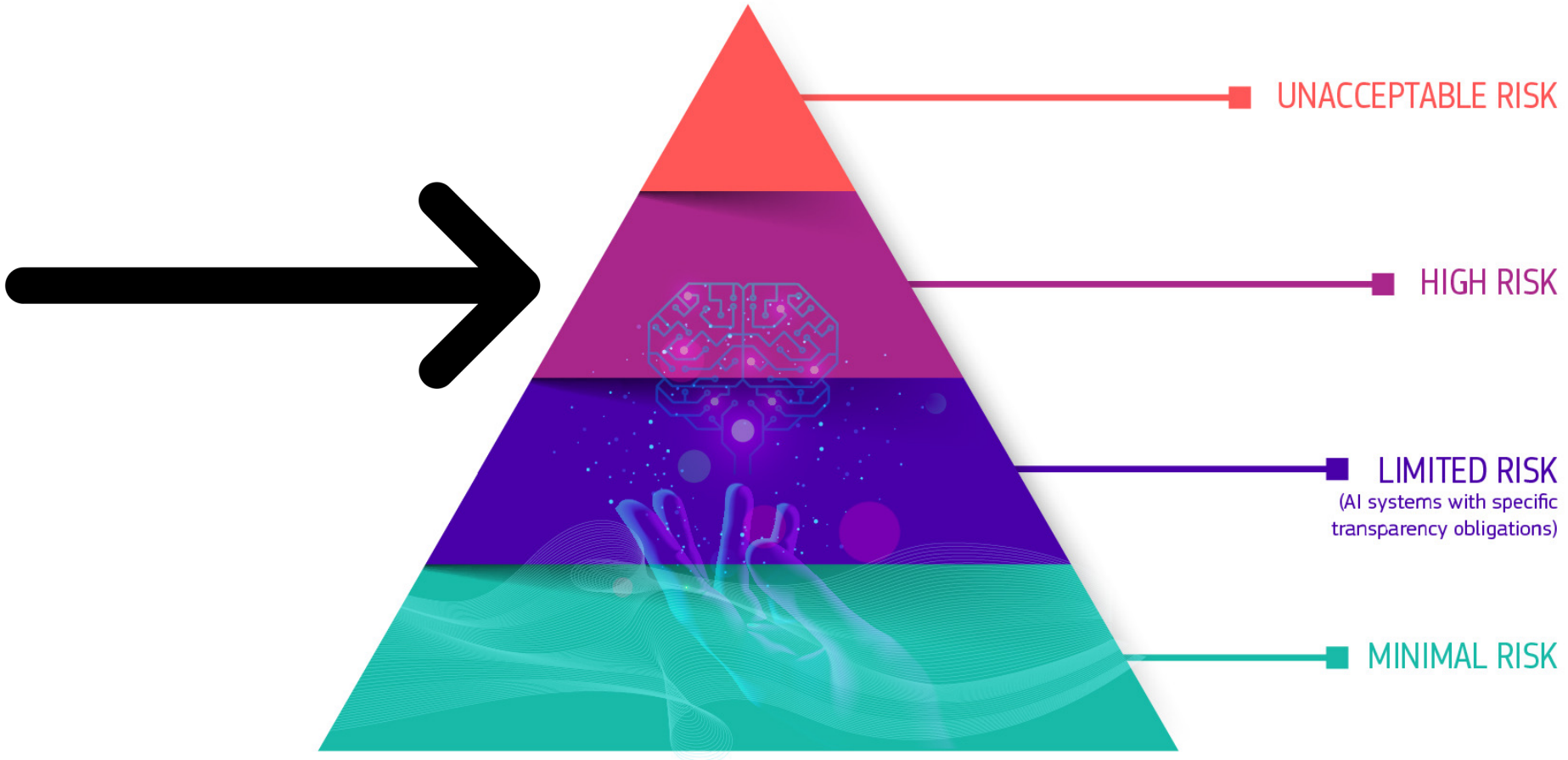
Forbud 4, med unntak

Biometrisk fjernidentifikation i sanntid

- på **offentlige** steder
- U: 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 retsforfølging av en **gjerningsperson**



Source: Colourbox

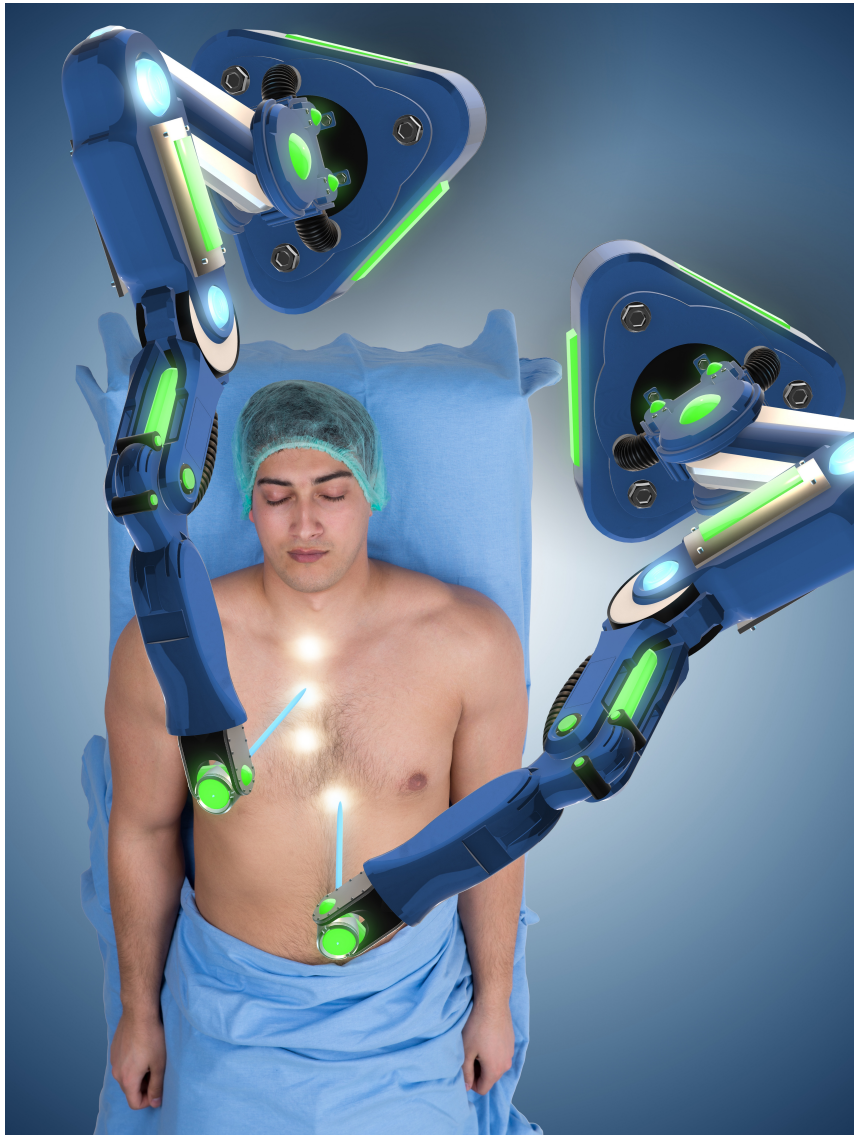

UNACCEPTABLE RISK
HIGH RISK
LIMITED RISK
(AI systems with specific transparency obligations)
MINIMAL RISK

Produktrelaterte høyrisiko AI systemer

AI som er produkt eller sikkerhetskomponent for produkt

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

CE



Source: Colourbox

Frittstående høyrisiko AI systemer med formål

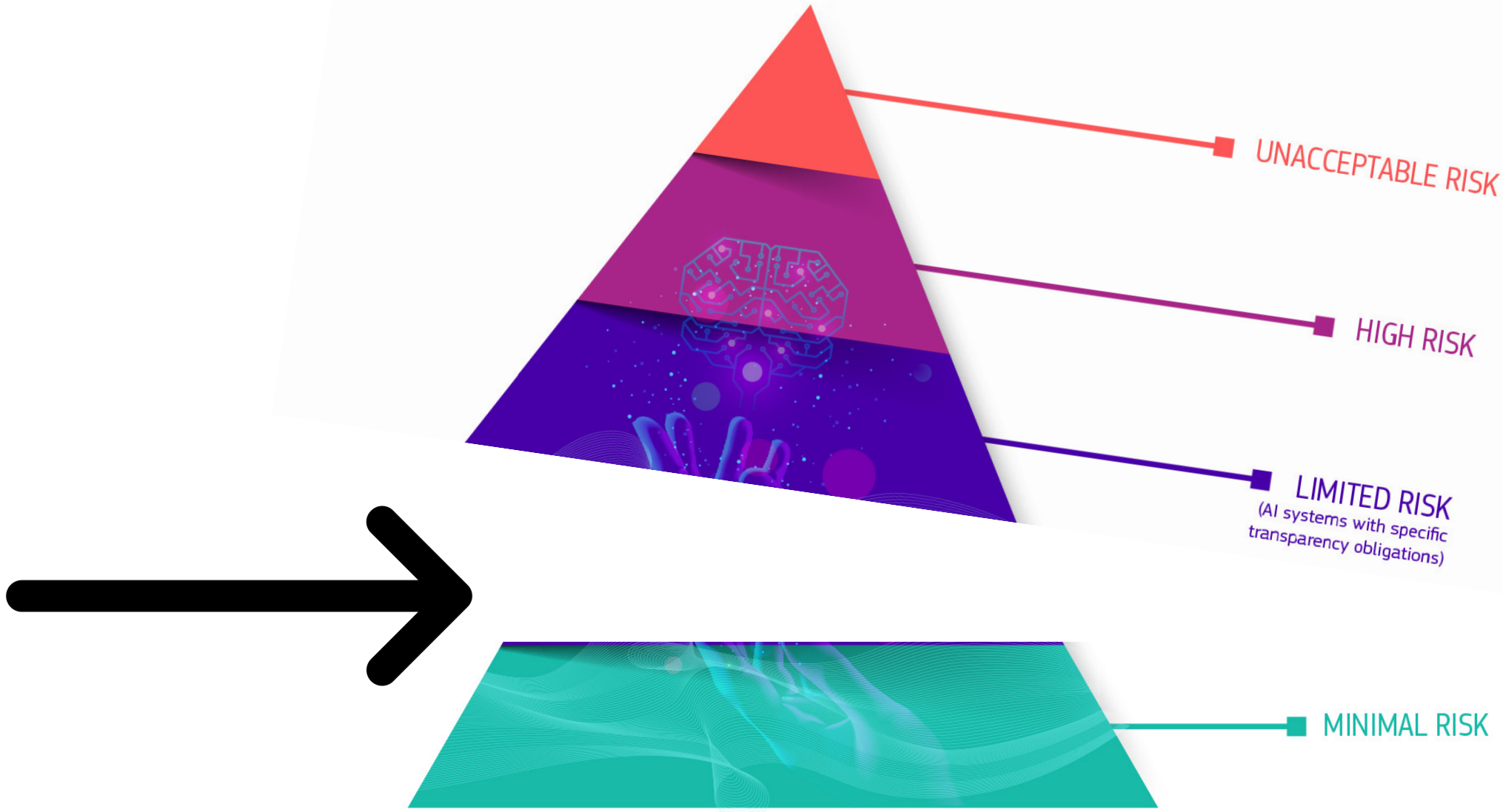
1. Biometrisk identifikasjon og kategorisering
2. Forvaltning og drift av kritisk infrastruktur/**miljø**
3. Utdanning og yrkesopplæring
4. Ansettelse, arbeidsledelse & tilgang til selvstendig arbeid
5. Tilgang til essensielle private og offentlige tjenester
6. Lovhåndhevelse
7. Migrasjon, asyl og grensekontroll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

Formål

‘intended purpose’

means the use for which an AI system **is intended by the provider**, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation**;**

general purpose AI systems shall not be considered as having an intended purpose within the meaning of this Regulation;


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

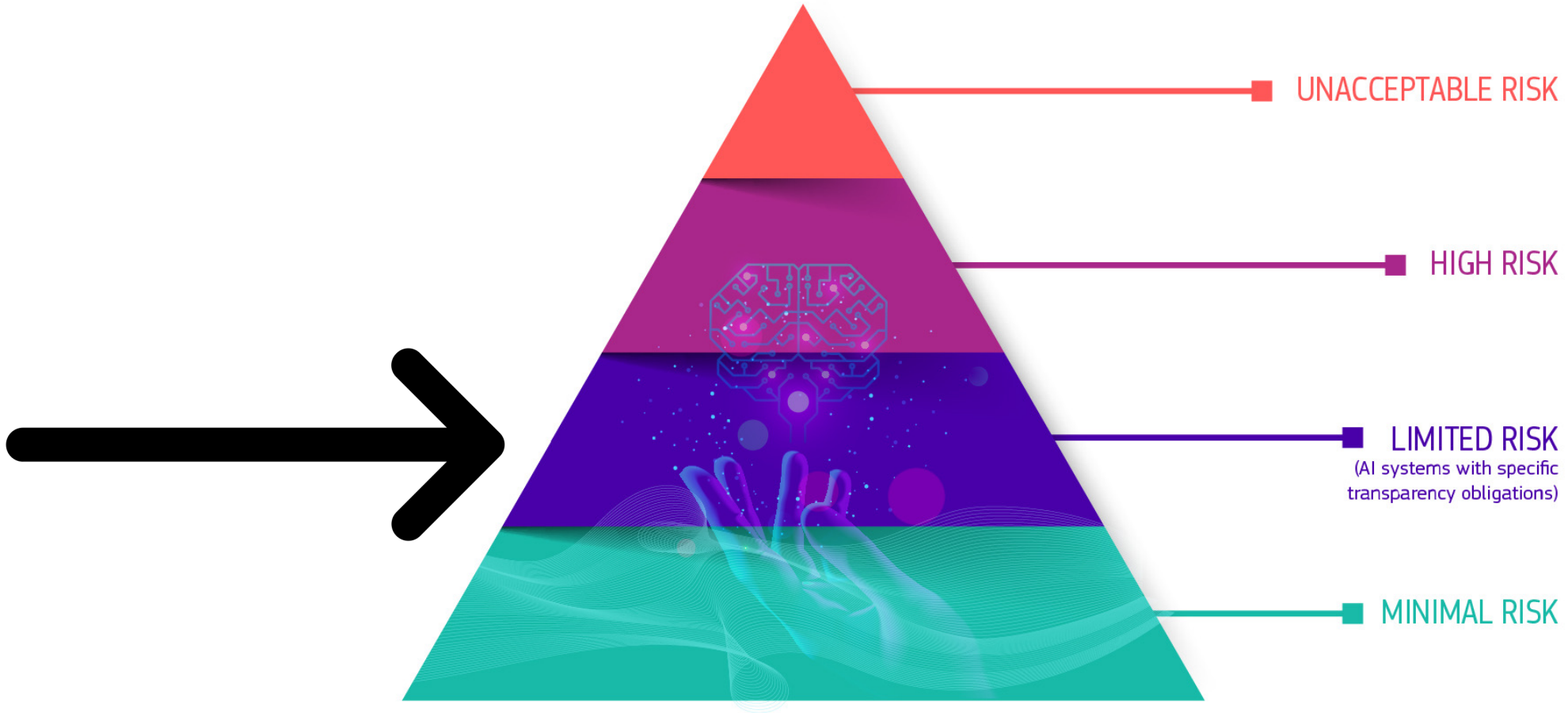
Krav til høyrisiko AI systemer

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

Forpliktelse for ulike aktører

Hvem er du?

- 'operator' [of AI system]
  - 'provider'
    - 'small-scale provider'
    - [any third party that substantially modifies AI System]
  - 'authorised representative'
  - 'importer'
  - 'distributor'
  - 'user'
- 'product manufacturer'
- various coformity assessment bodies & authorities, etc.


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

Chatbots & deep fakes

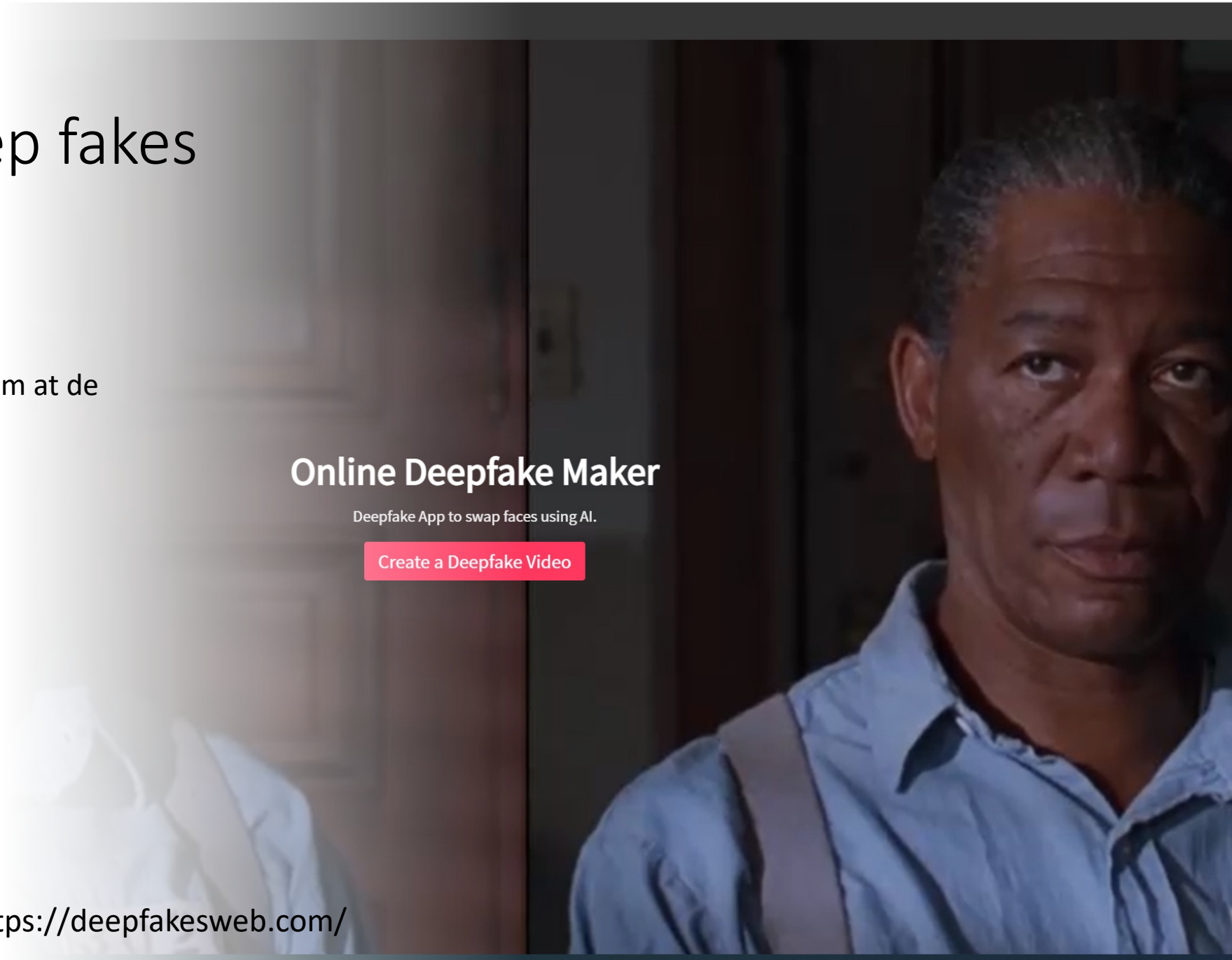
Article 52: Transparens

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?