Mathieu Serrurier

Applications of Deep Learning in Healthcare : Challenges and Limitations

ANITI
Université Fédérale Toulouse Midi-Pyrénées

Applications of AI to healthcare

Early application : Mycin

- Early 80's
- Expert system :
  - Based on logic
  - Automatic inference
  - Explainable model
- Limitation :
  - require to formalize manually expert knowledge
  - Logic

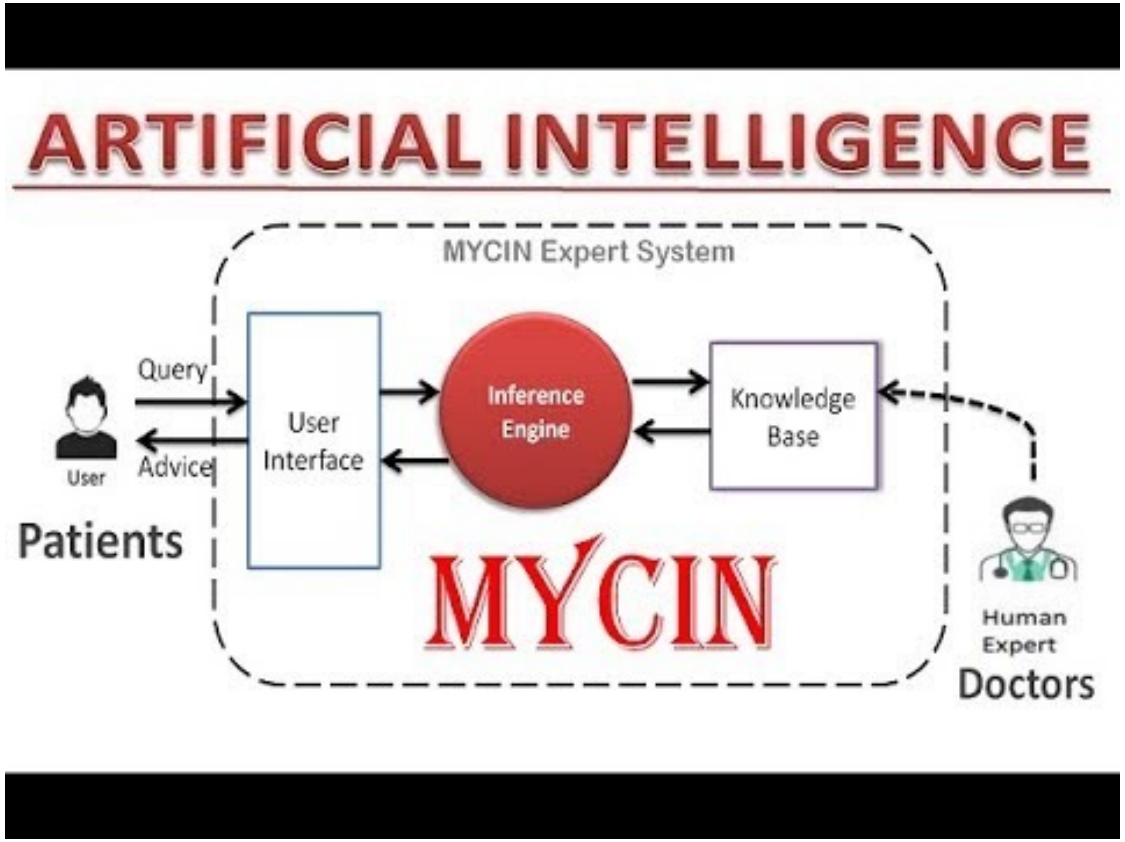
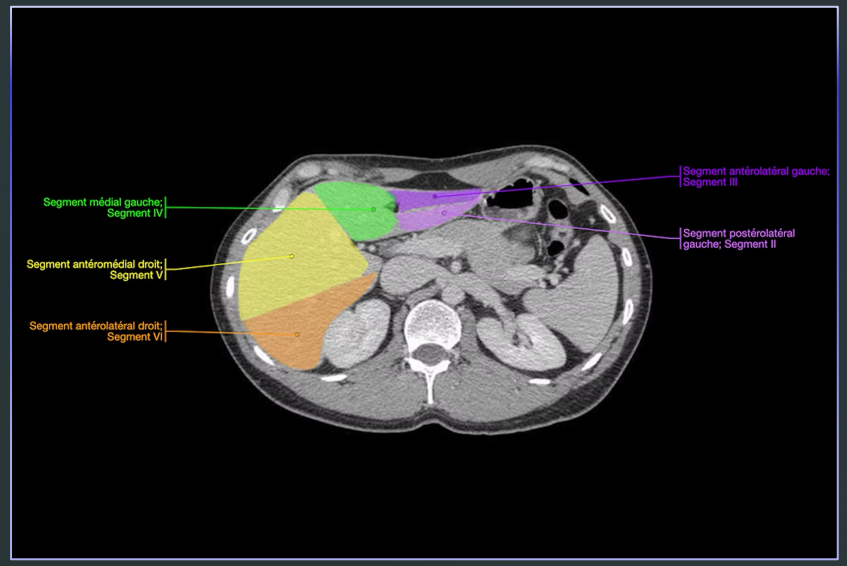
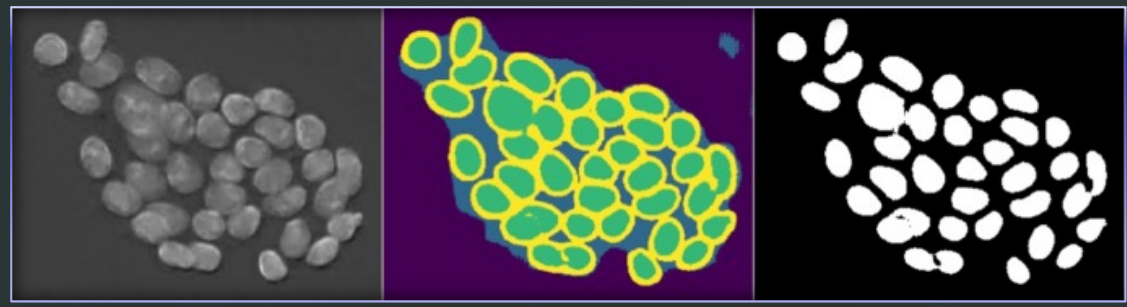


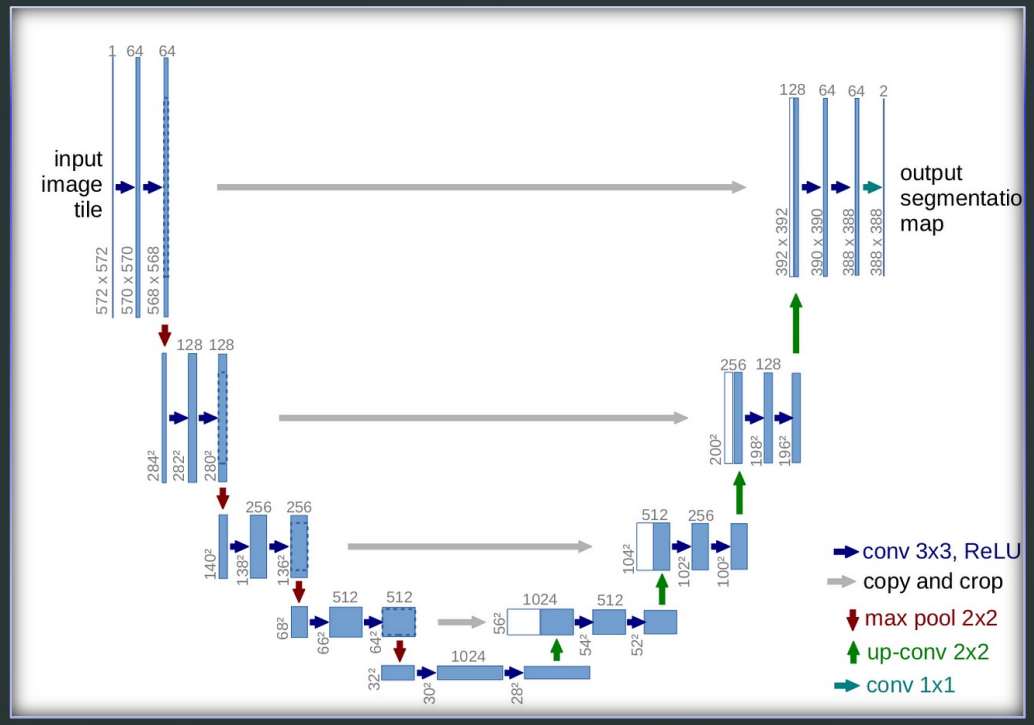
Image segmentation



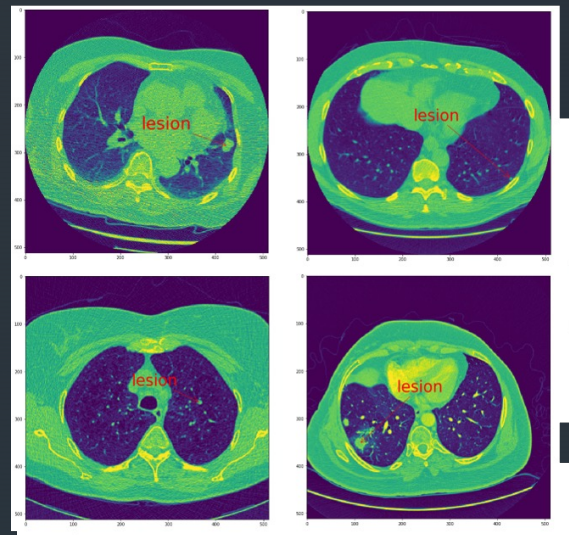


UNET

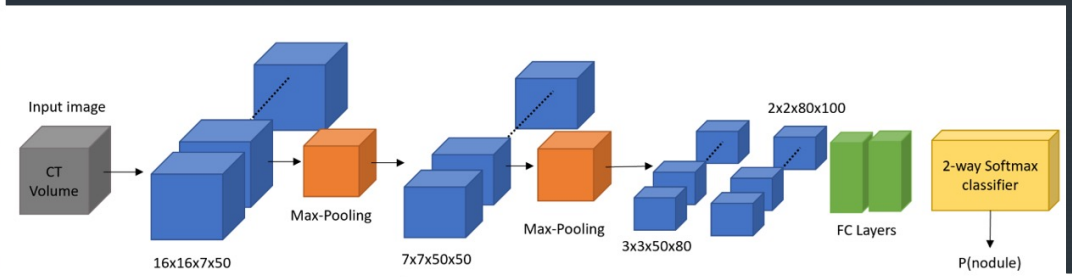
- Most used architecture for segmentation
  - Image to image network
  - Convolutional
  - Skip connection
  - Loss : IOU/dice

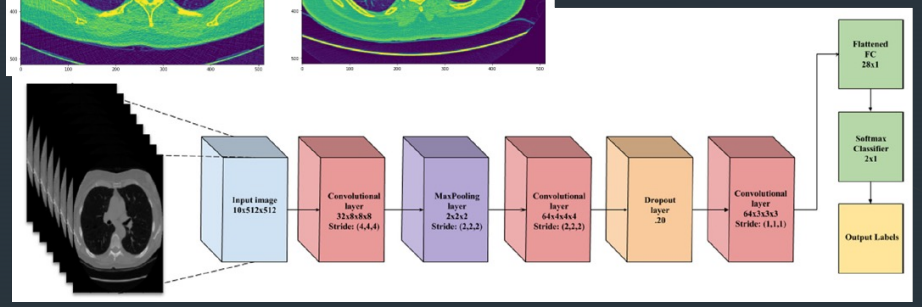


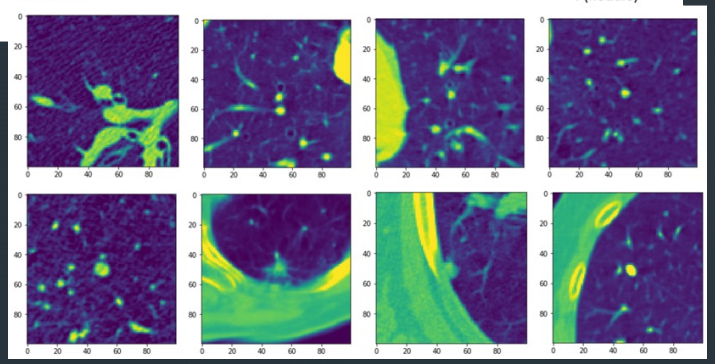
Lung Cancer detection



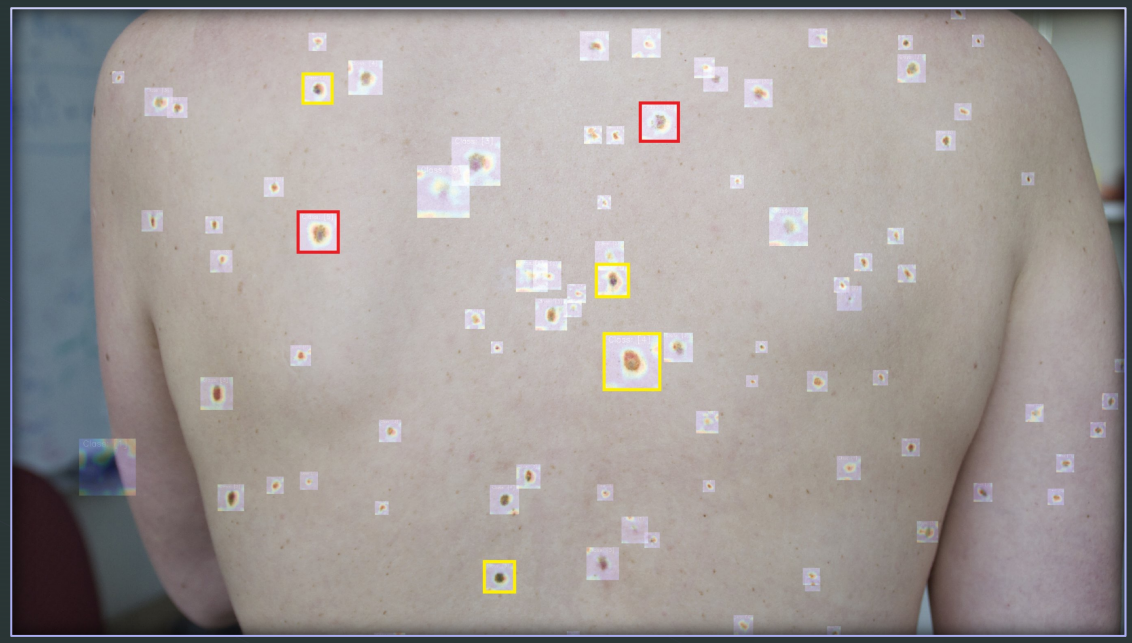
Deep Lung Cancer Detection





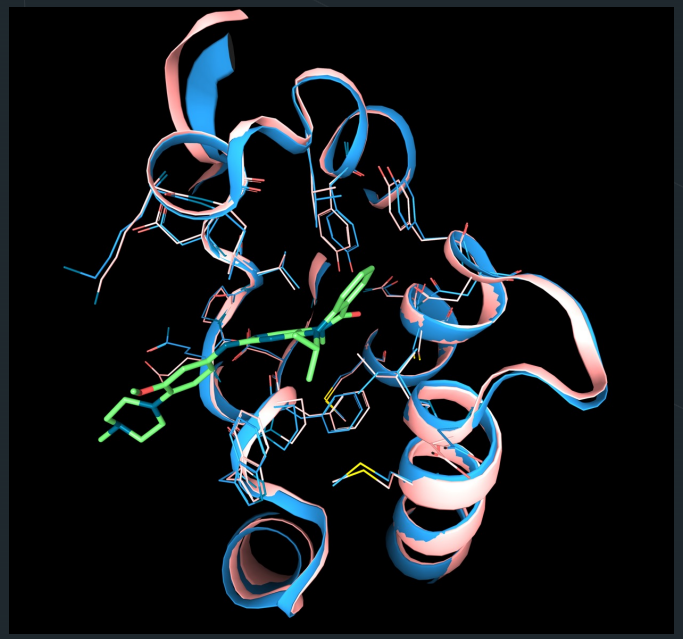


Skin cancer detection



Exploration

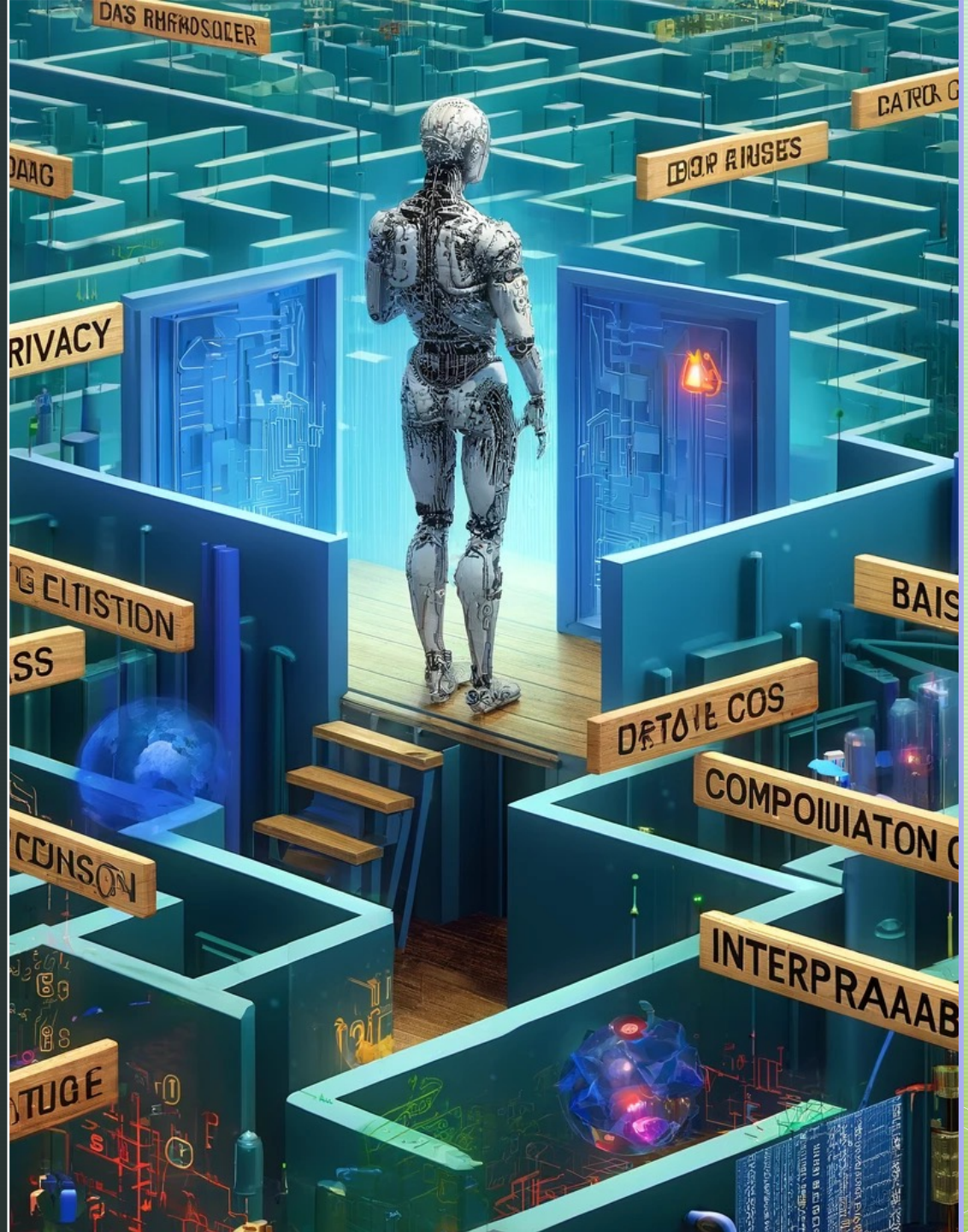
Alpha fold



Drugs discovery

What do we want for AI in heathcare

- Accuracy/precision
- Generalization
- Reproducibility
- Explainability
- Guarantees



Challenge 1

Data

Data issue in AI for healthcare

- Good models need :
  - A lot of data
  - Clean data
  - Annotations

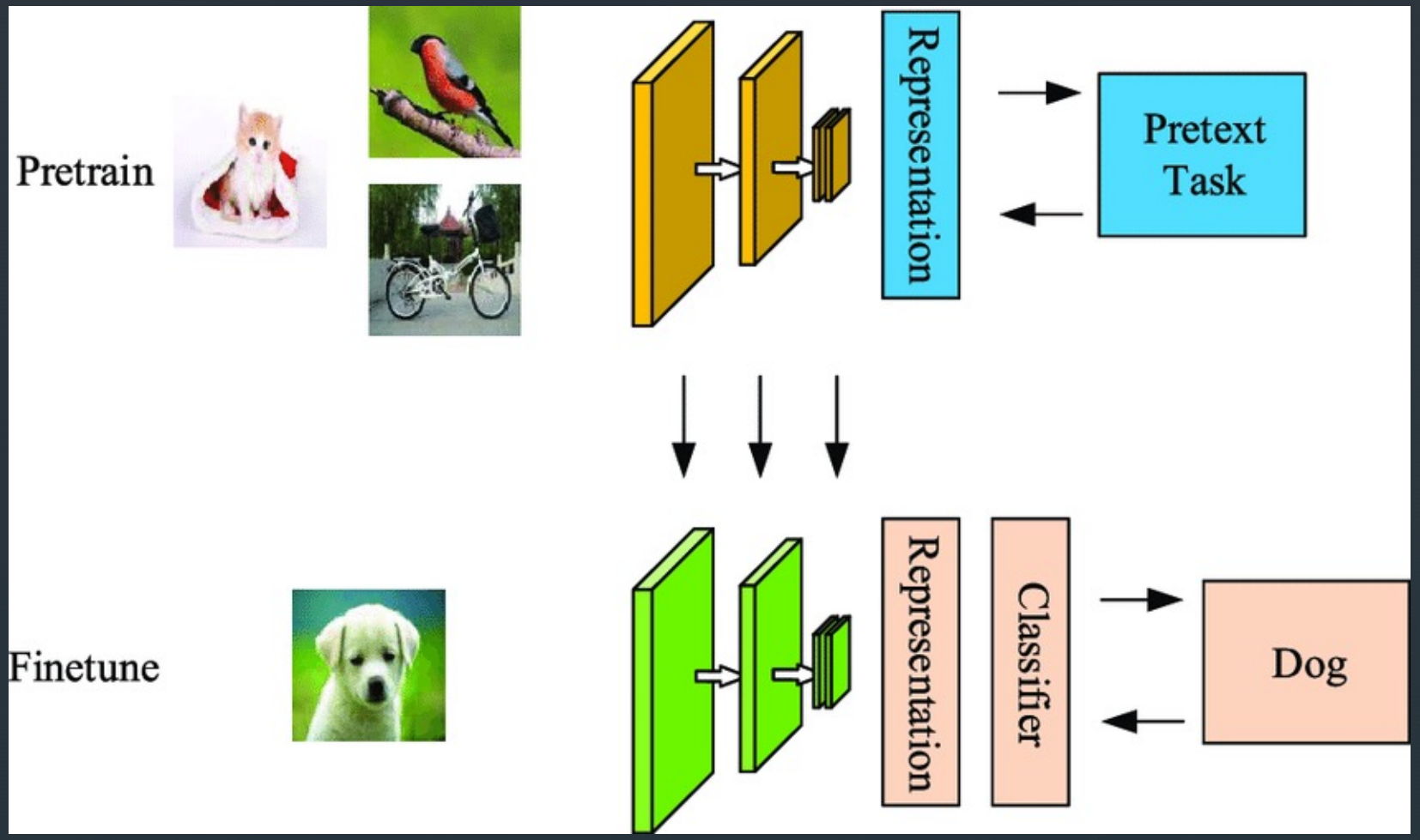
Ethics : annotation came from biological tissues

- Lot of data = lot of biological tissues

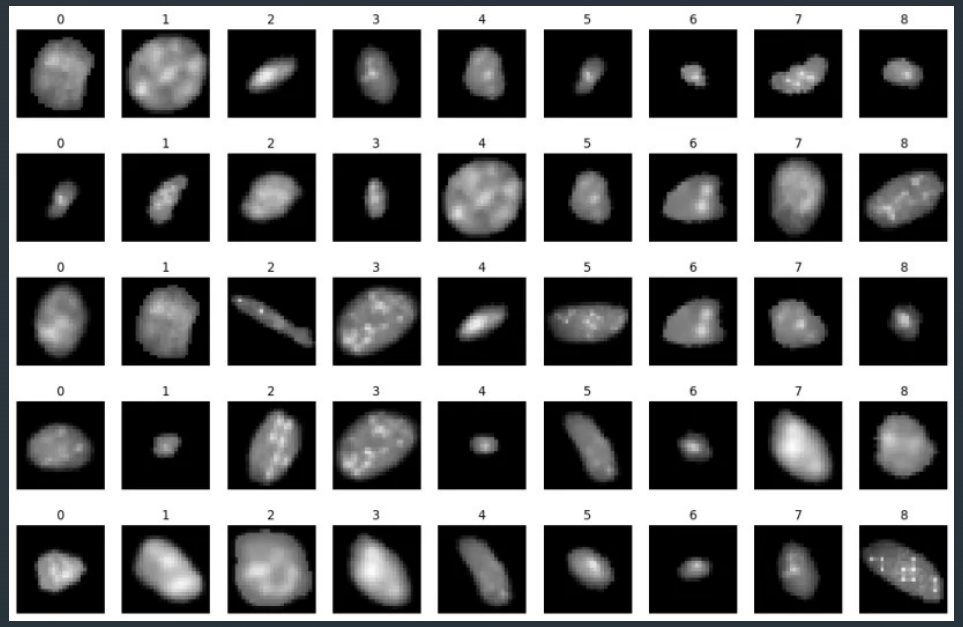
Cost of data

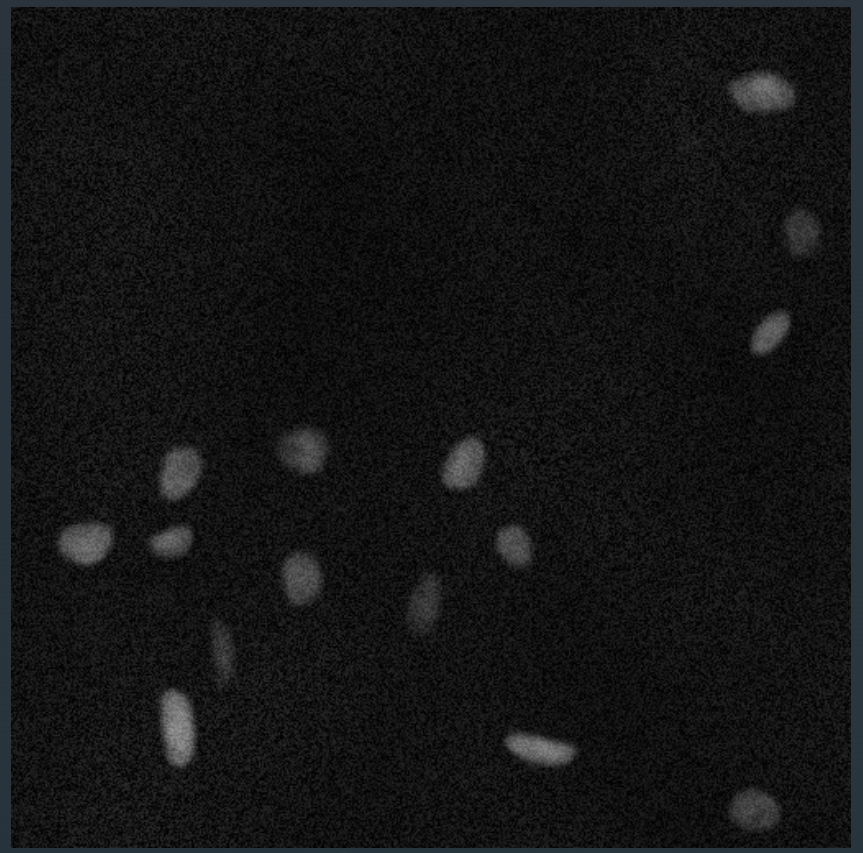
- Lot of data = lot of time and money :
  - Manual annotation takes time
  - It requires skills and experties
  - It requires expensive devices and material

Solution : self supervised training



Solution : data generation



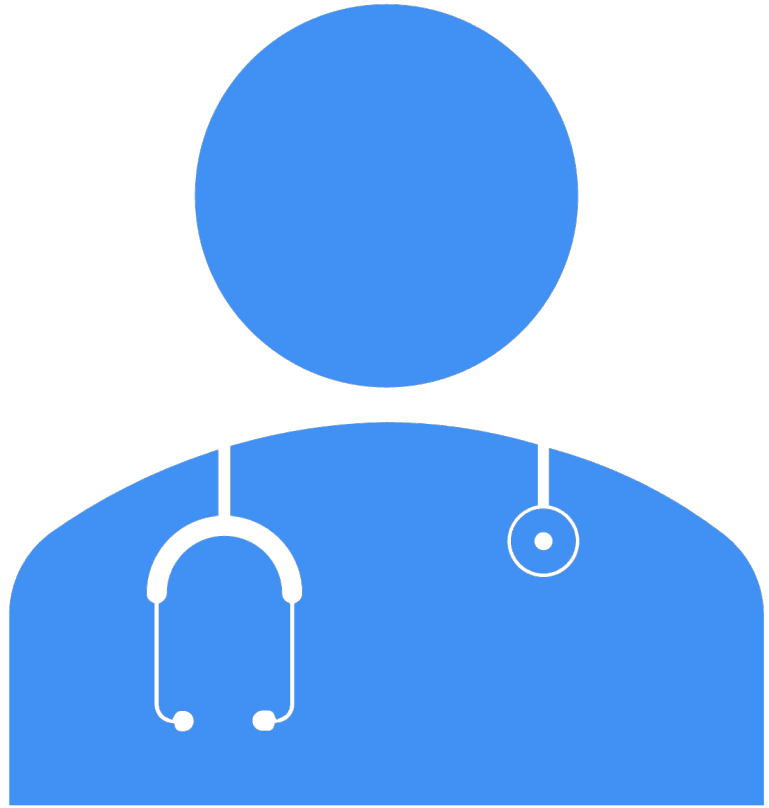


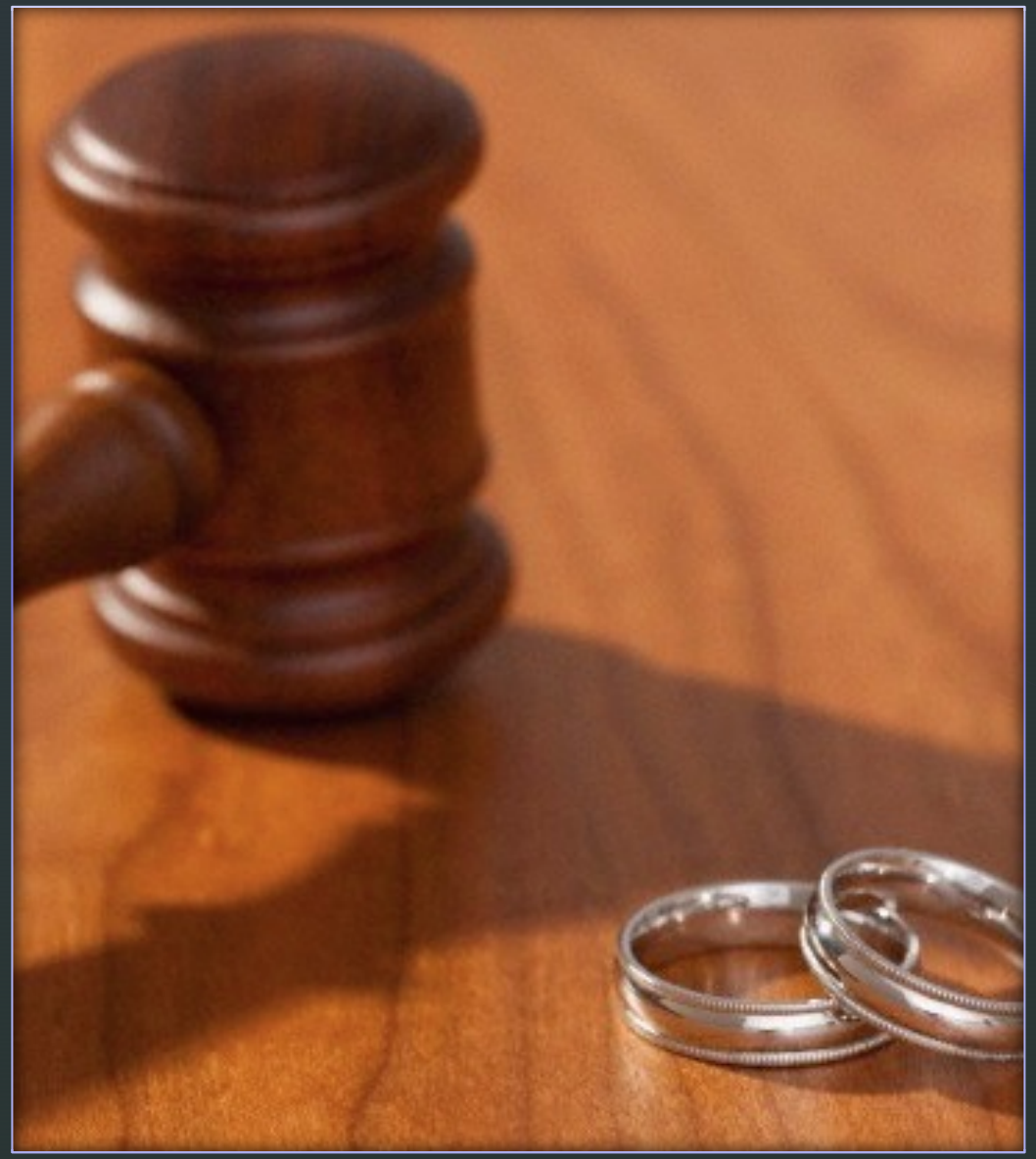
Challenge 2

Privacy

Privacy in healthcare data

- Healthcare data are protected by the law :
  - Require anonymisation
  - Require authorization for sharing





Differential privacy

- Question : What the model can deduce from me :
  - Facebook and the divorce
  - Stanford experiment 2017

And what about generative models

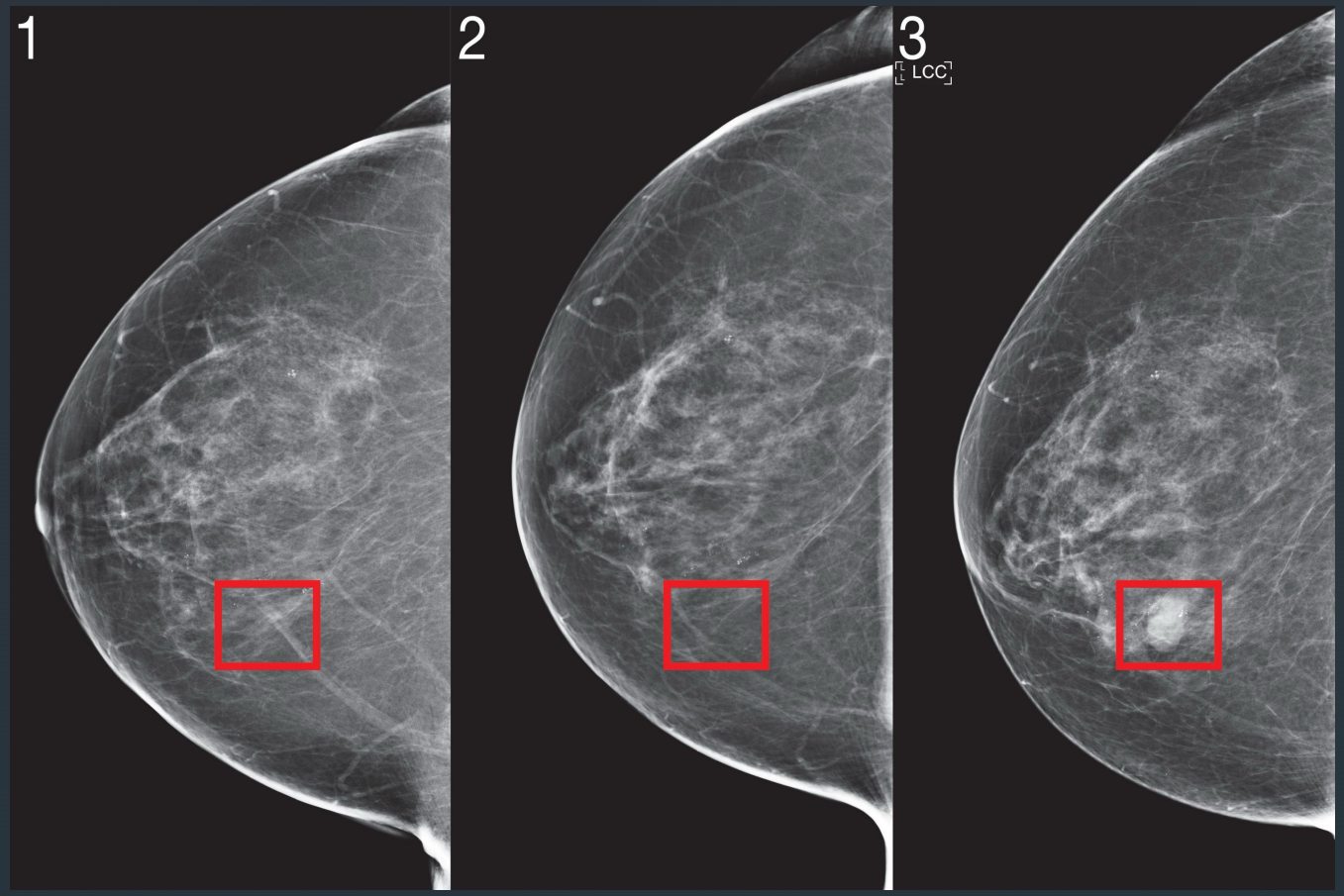
- LLM open questions:
  - Detect what is in the training
  - Data leakage

Challenge 3

Fairness and biases

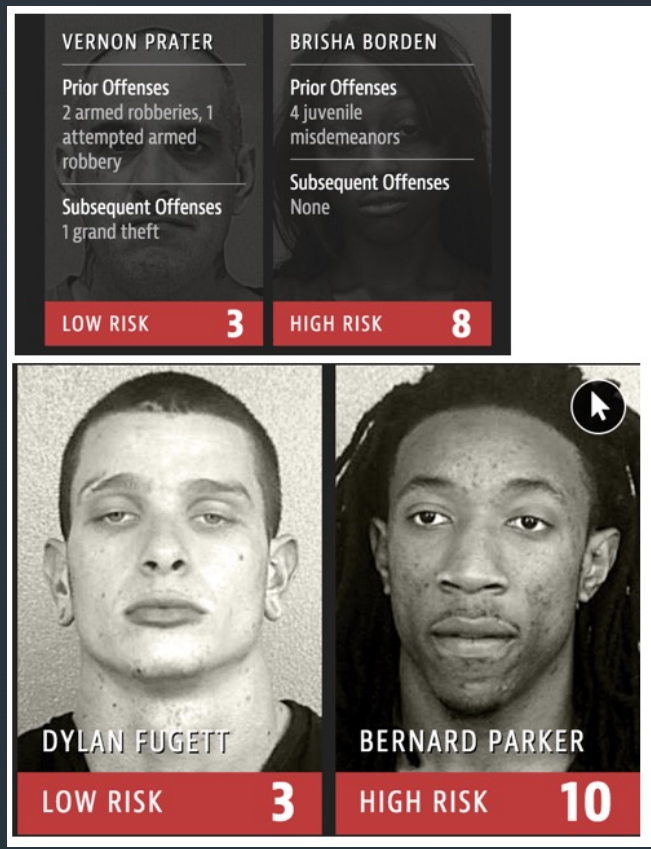
Dog vs wolfs

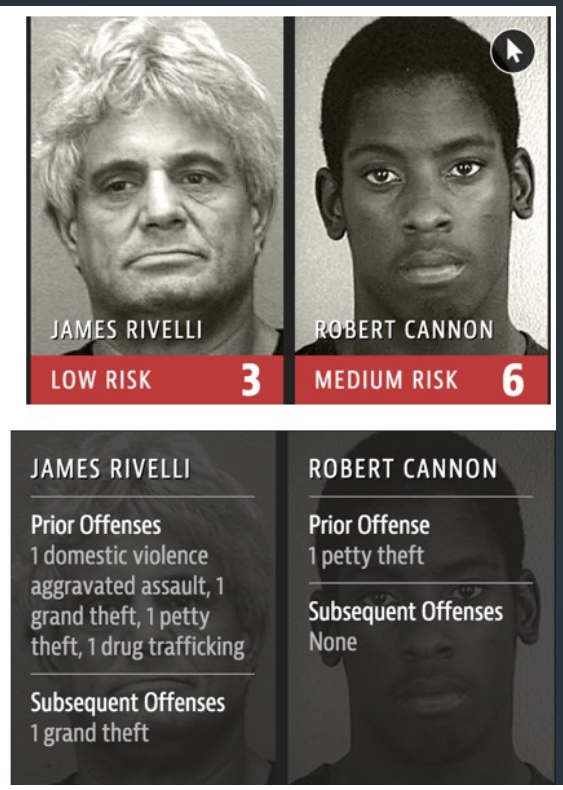
Generalization



Fairness

Fairness





	WHITE	AFRICAN AMERICAN
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

Are the performances the same for all skin colors ?

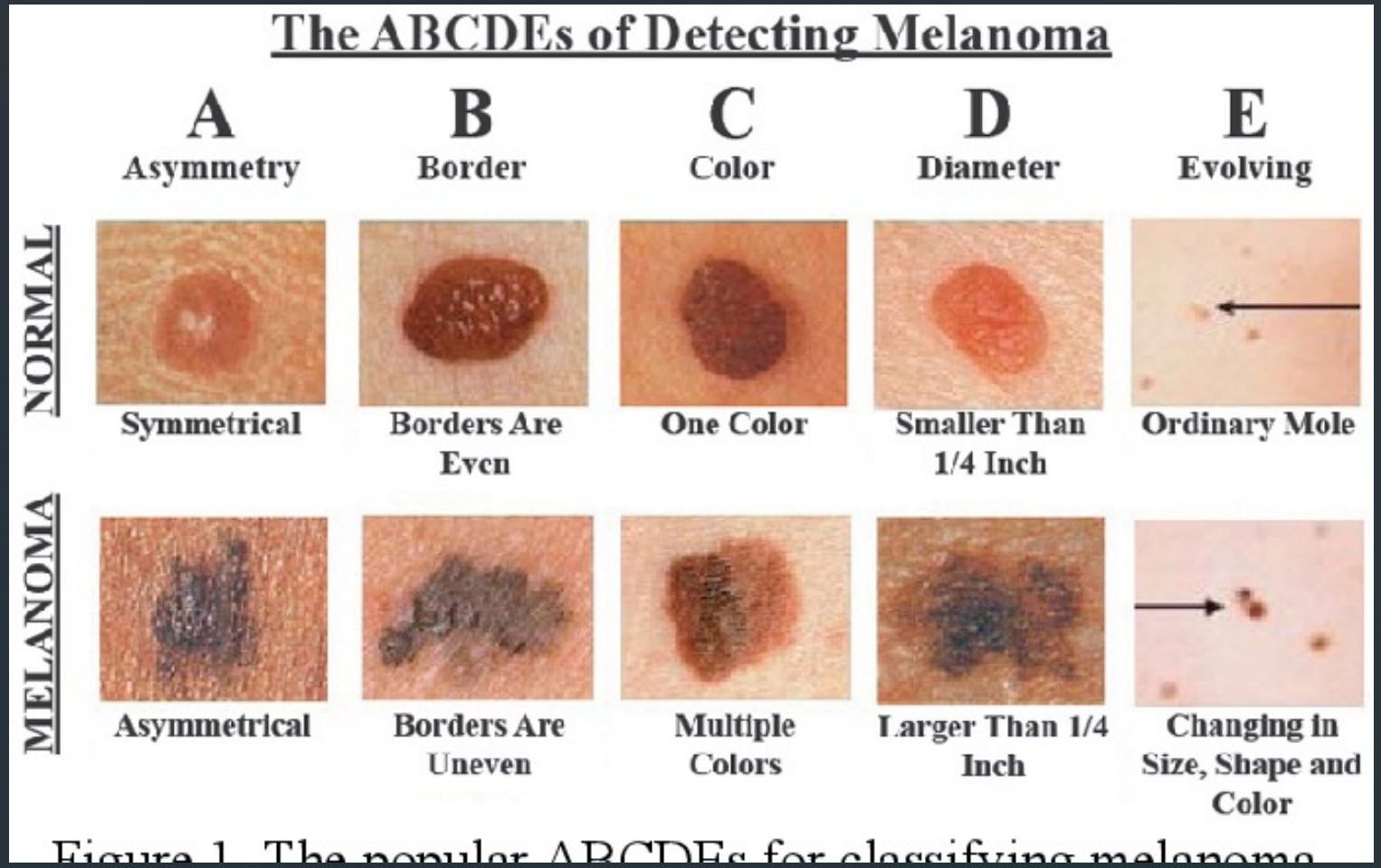


Figure 1. The popular ABCDEs for classifying melanoma

Solutions

- Resample the database in order to meet the condition of demographic parity.
- Force the learning algorithm to have predictions (or errors) independent of the protected variable.
- Change the prediction threshold in order to favor the protected variable.
- Constraint the model during the traning

And with generative AI ?

Challenge 4

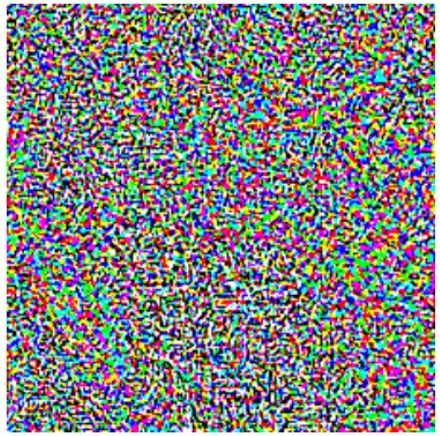
Robustness

Adversarial attacks

$\boldsymbol{x}$

"panda"
57.7% confidence

$+ .007 \times$



$\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$

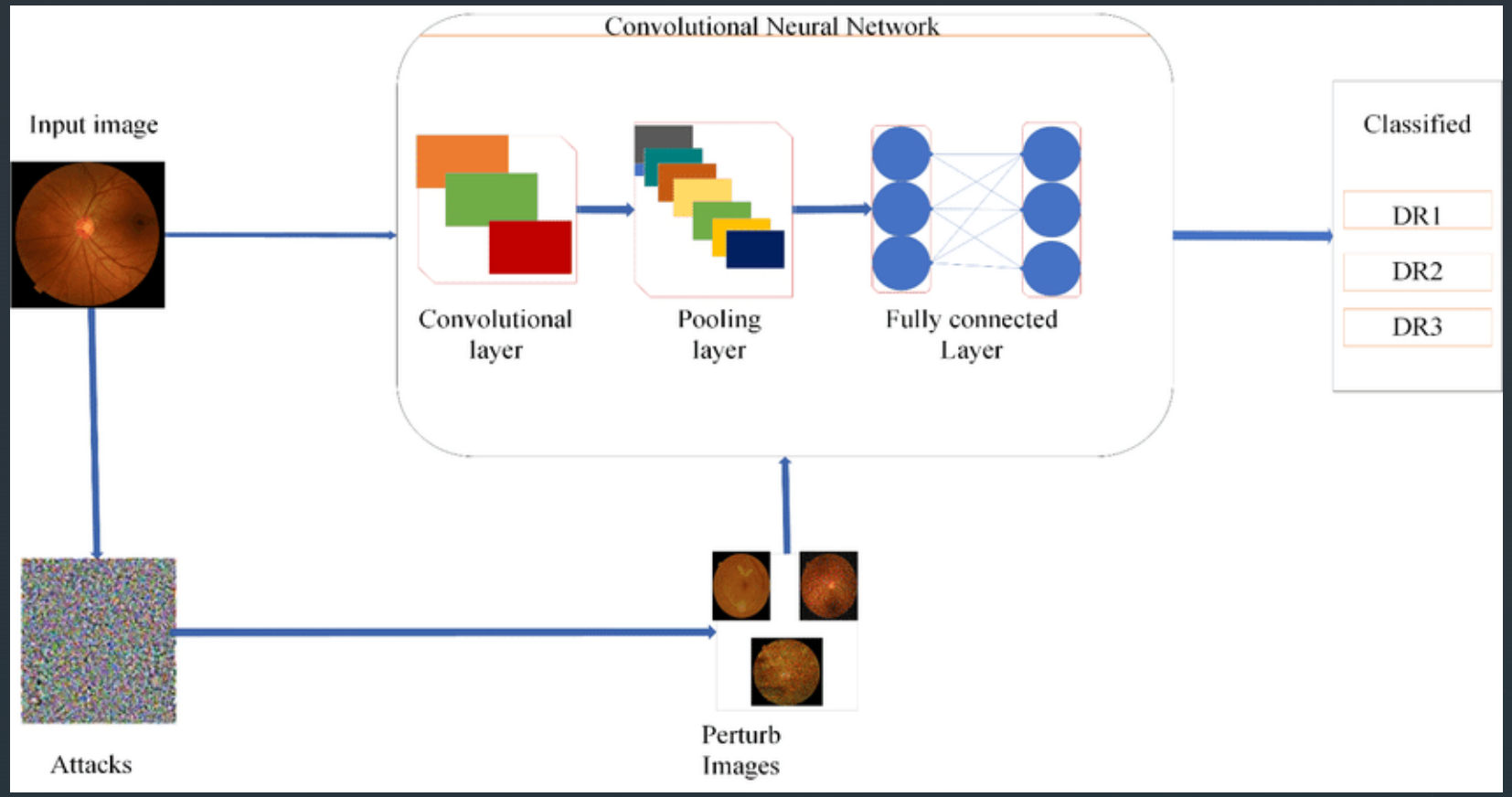
"nematode"
8.2% confidence

$=$

$\boldsymbol{x} + \epsilon\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$

"gibbon"
99.3 % confidence

Adversarial training



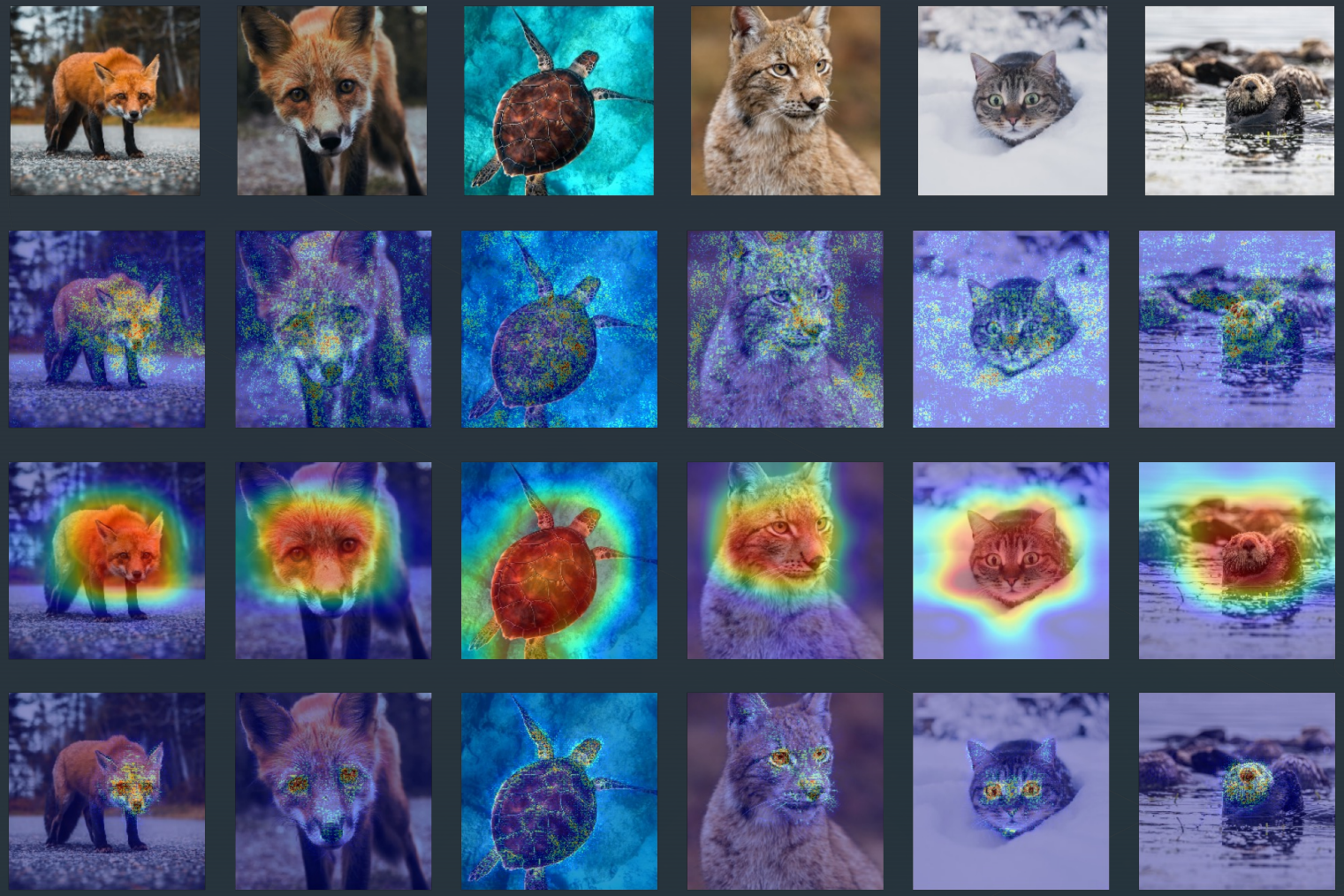
Challenge 5

Explainability

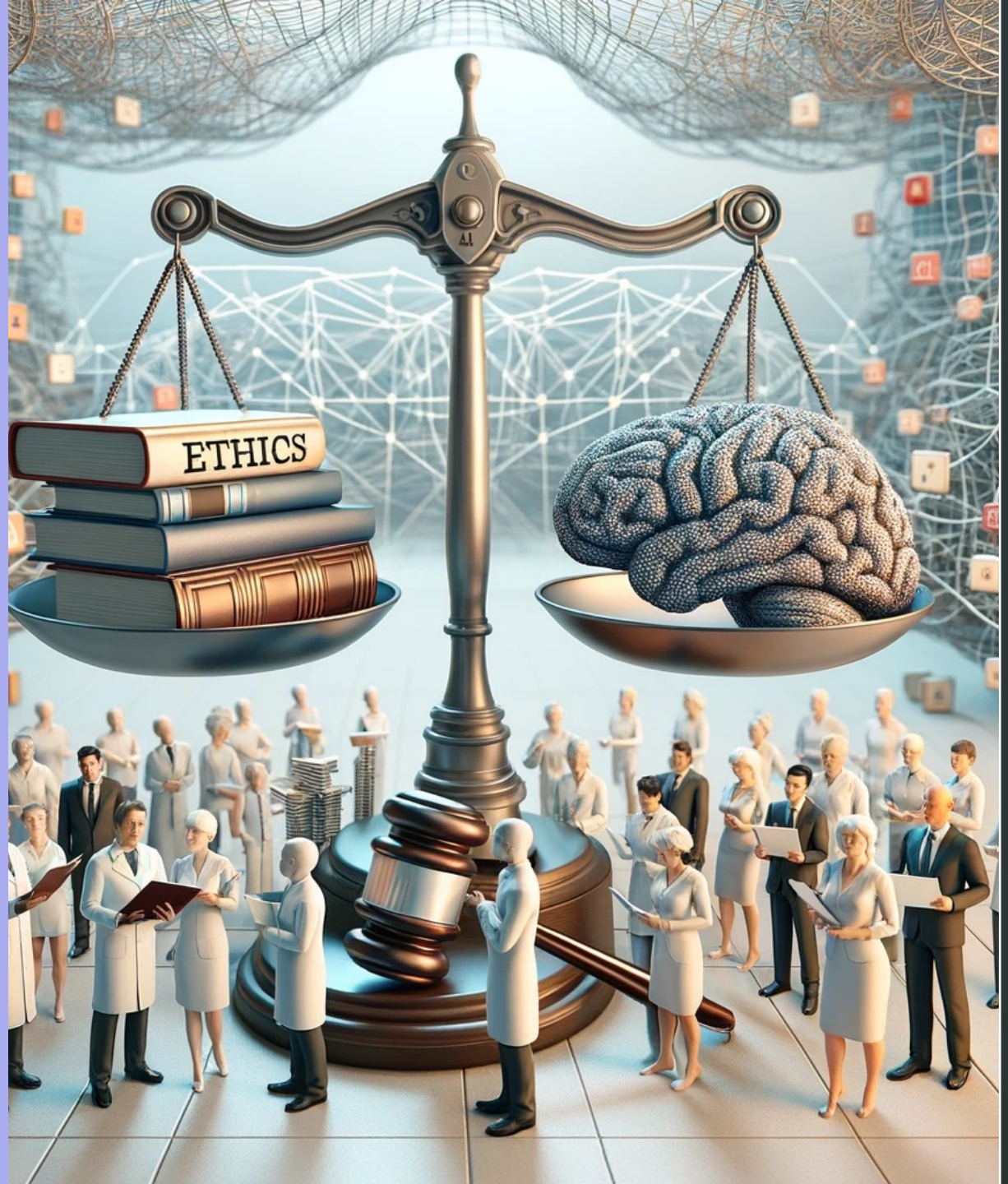
Deep learning models are black boxes

What model sees

Attribution functions



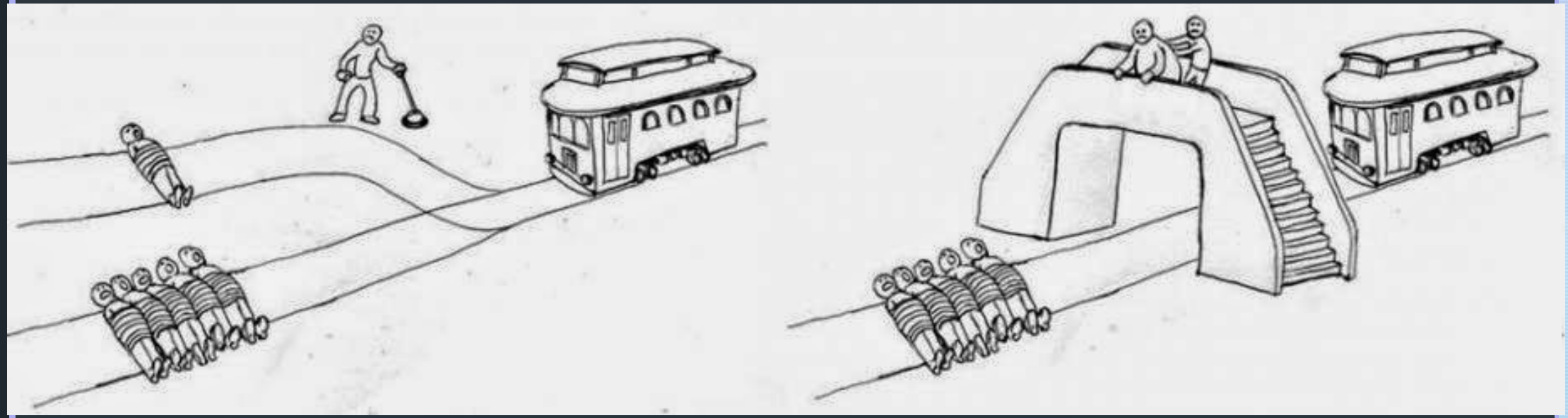
Concept associations



Challenge 6

Ethics and law

Acceptability

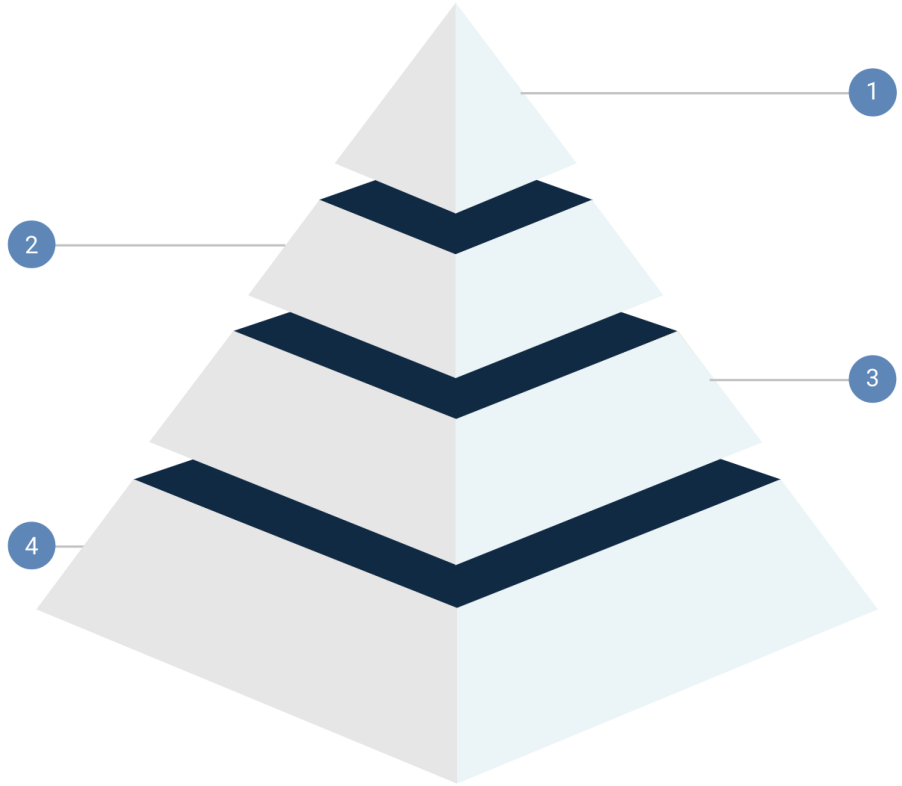


Unacceptable Risk

Highest level of risk prohibited in the EU. Includes AI systems using e.g. subliminal manipulation or general social scoring.

High Risk

Most regulated AI systems, as these have the potential to cause significant harm if they fail or are misused, e.g. if used in law enforcement or recruiting.



Limited Risk

Includes AI systems with a risk of manipulation or deceit, e.g. chatbots or emotion recognition systems. Humans must be informed about their interaction with the AI.

Minimal Risk

All other AI systems, e.g. a spam filter, which can be deployed without additional restrictions.

AI act

Conclusions