**Week 6 : Practical: Artificial Intelligence (AI)**

In Data Science we process a lot data through AI. With the GDPR, it is becoming increasingly important to understand the ethics behind the data that is collected, stored, processed and evaluated.

Your task is to:

•Find out what Responsible AI is?

Responsible AI is a framework for bringing many of these critical. practices together. It focuses on ensuring the ethical, transparent and accountable use of AI technologies in a manner consistent with user expectations, organizational values and societal laws and norms.

(<https://www.accenture.com/_acnmedia/PDF-92/Accenture-AFS-Responsible-AI.pdf>)

•Find instances where AI has failed? Or been used maliciously or incorrectly.

# Footballer or Felon?

A leading facial-recognition system identified three-time Super Bowl champion Duron Harmon of the New England Patriots, Boston Bruins forward Brad Marchand, and 25 other New England professional athletes as criminals. Amazon’s Rekognition software incorrectly matched the athletes to a database of mugshots in a test organized by the [Massachusetts chapter of the American Civil Liberties Union](https://www.aclum.org/en/news/facial-recognition-technology-falsely-identifies-famous-athletes/#athletes) (ACLU). Nearly one-in-six athletes were falsely identified.The misclassifications were an embarrassment for Amazon, which has marketed Rekognition to police agencies for use in their investigations. “This technology is flawed,” Harmon said in an ACLU statement, and “should not be used by the government without protections.”

# Voice-Spoofing Software Cons CEO

In March the CEO of a UK-based energy firm got a phone call from his boss at the German parent company instructing him to transfer €220,000 ($243,000) to a Hungarian supplier. The ‘boss’ said the request was urgent and directed the UK CEO to transfer the money promptly.

It turns out the phone call was made by criminals who used AI-based software to mimic the boss’s voice, including the “slight German accent and the melody of his voice,” as reported in [The Wall Street Journal](https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402). Such AI-powered cyberattacks are a new challenge for companies, as traditional cybersecurity tools designed for keeping hackers off corporate networks can’t identify spoofed voices.

(<https://medium.com/syncedreview/2019-in-review-10-ai-failures-317b46155350>)

•Implications of when AI fails. There is a specific article in the GDPR Law that covers this, especially with automated decision making. (opt in and out options).

<https://gdpr-info.eu/art-22-gdpr/#:~:text=22%20GDPR%20Automated%20individual%20decision,significantly%20affects%20him%20or%20her>.

•What should organisations do to ensure that they are being responsible with AI and the wider use of data in general?

This is related back to responsible AI. There are outlines should be followed by the organisations to ensure they are responsibly to what data they have been collected. For example, Microsoft defined responsible AI with 6 basic principles

* Fairness – AI systems should treat all people fairly
* Inclusiveness – AI systems should empower everyone and engage people
* Reliability & Safety – AI systems should perform reliably and safely
* Transparency – AI system should be understandable
* Privacy & Security – AI systems should be secure and respect privacy
* Accountability – People should be accountable for AI systems

(<https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6>)

Other organisations also need to clearly define their principle when managing the data and follow the GDPR rules.