LECTURE ONE – AI

LAW2291_2024

Contemporary Issues in Biolaw (24/25)

0.0

The lecturer

0.1 Overview

- Ongoing Legal Issues in Cybersecurity and Safety for AI in Healthcare
- LECTURE 1 – AI
- LECTURE 2 – SAFETY AND MEDICAL DEVICES (PART ONE)
- LECTURE 3 – MEDICAL DEVICES (PART TWO)
- LECTURE 4 - CYBERSECURITY

0.2

Perspective of the four lectures:

- **healthcare,**
- **the law,**
- **contemporary,**
- **cybersecurity,**
- **safety**

And other views/directions are not possible due to the time constraint

- Relevant law during lectures!
- Extent of understanding
- Usefulness
- Assessment versus potential

1.0 Introduction to AI

- Artificial Intelligence
- Intelligence?
- Artificial v natural
- History of AI (with AI winters in-between)

Formal reasoning and necessary math

Birth of CS

Expert decision-making systems

Machine-learning, neural networks

Large Language Models (<- you are here)

1.1

- Many categories
- Three used for this course:

Symbolic AI <-> ML AI <-> LLM AI

We could use AI Act distinctions literally, but this will not cover it widely, nor the technical concepts.

We instead do a bit of both.

1.2

- Symbolic AI
- Everything from extremely simple decision-making, in e.g., videogames, up to automated processing of legal applications and taxation
- Some CPS systems use this
- Healthcare?
- No ML elements, no learning, no generative elements
- Detailed but time-consuming to code
- Safer (more next lecture)

Fancy statistics

1.3

- ML AI
- Everything from simple slightly tweaked Symbolic AI to neural network based systems
- Works in everything from small robots, automated security detection systems (like antivirus or firewalls or terminal points elsewhere) to cars
- Can be very autonomous or almost fully supervised, real-time or not
- Can be unpredictable/variable
- Dataset based, learning based, choices, black/white boxes, transparency issues

1.4

- LLM AI
- Like ML AI, but at scale
- LLMs were originally made for languages – repurposed. Predicting the next steps, sentences/logic wise – and now for more.
- All types of datasets/basis for data (many different terms for the same thing, such as foundational models), extremely large
- AI as a service for everyone
- Demanding (power, computational, knowledge, etc.)
- Lack in adoption – maybe SLM (small language models) will be the solution?
- Unpredictable, more unsafe

  Relies on millions of man hours to fix (hiring people across the world)

law

2.0 The AI Act

- Background (https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence)
- GDPR
- Product Regulation

Always on the background of the usual suspects (https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en)

2.1 Structure

- Recitals!
- Initial aspects, definitions, prohibited practices, high-risk AI (wide, including obligations), transparency obligations, general-purpose AI (wide), innovation measures, governance (European Artificial Intelligence Board, national competent authorities and single points of contact), High-risk AI database, post-market monitoring/information sharing/market surveillance, codes of conduct and guidelines, delegation, penalties.

2.2 Purpose

- Art 1(1) and 1(2)

The purpose of this Regulation is to improve **the functioning of the internal market** and **promote the uptake of human-centric and trustworthy artificial intelligence (AI),** while **ensuring a high level of protection** of **health, safety, fundamental rights** enshrined in the Charter, including **democracy, the rule of law and environmental protection**, against the **harmful effects of AI systems in the Union** and **supporting innovation**

This Regulation lays down:

(a) harmonised rules for the **placing on the market**, the **putting into service**, and **the use** of AI systems in the Union;

(b) prohibitions of certain AI practices

(c) specific requirements for high-risk AI systems and **obligations** for operators of such systems;

(d) harmonised transparency rules for certain AI systems;

(e) harmonised rules for the **placing on the market of general-purpose AI models**

(f) rules on **market monitoring**, **market surveillance**, **governance** and **enforcement**

(g) measures to support innovation, with a particular focus on SMEs, including start-ups

2.3 AI Definition

- Art 3, (1)

‘AI system’ means a **machine-based** system that is designed to operate with **varying levels of autonomy** and that **may exhibit adaptiveness** after deployment, and that, for **explicit** or **implicit objectives, infers,** from the **input** it receives, how to **generate outputs** such as **predictions, content, recommendations, or decisions** that can **influence physical or virtual environments**;

… General-purpose AI and their models??

cumulative

2.4

- Machine based?
- Autonomy?
- Adaptiveness (note “may”)?
- Objectives?
- Inference?
- Generate?
- Output? (predictions, content, recommendations, or decisions)
- Influence physical or virtual environments?

2.5 Enforceability

- Usually, a combination of scope + special rules + powers of authorities
- **Entirety of Section 2 and 3 of Chapter VII**.
- National competent authorities, notified/notifying bodies and so on (also fundamental rights protecting ones). We will return to these in the next lectures in other legislation.
- Via post-market monitoring etc.

2.6 Liability

Without discussing the AI Liability Directive

- Obligations entail liability for providers, users, other types of third parties
- Violating obligations, standards, orders from authorities
- Proving it in court will follow the new Directive
- UK perspective = torts + specialised Product Liability Directive implementation (old one, not the newly introduced in the EU), but special rules may follow (??)

2.7 Obligations

- Minimum requirements (high-risk and otherwise)
- Legally positively defined
- At times, negatively
- Mirror other product legislation
- Written very widely
- Follows the requirements closely, Section 2 and 3 in Chapter III are generally great to read!

2.8 Prohibited Practices

- Art 5
- Manipulation, vulnerability abuse, social scoring etc., ”predicting crime”, untargeted facial scraping, emotion inference at work, real-time biometric identification (with exceptions and way too detailed for now)
- Future-proof?
- Circumventable?

2.9 High-risk

- For our purposes -> Art 6(1).

AI used in or as medical devices will always be considered high-risk.

Keep Art 15 in mind for later..

3.0 Legal Overlap

- AI Act and other legislation?
- Certification?
- Recital 46, 50
- Which is first – AI by itself, AI as part of a system, the whole system, specialised AI
- Annex I
- Open question – argument can be made in several directions

3.1 Legal Overlap

- AI in medical devices

Bridge to next lecture.

Questions (will not be recorded)