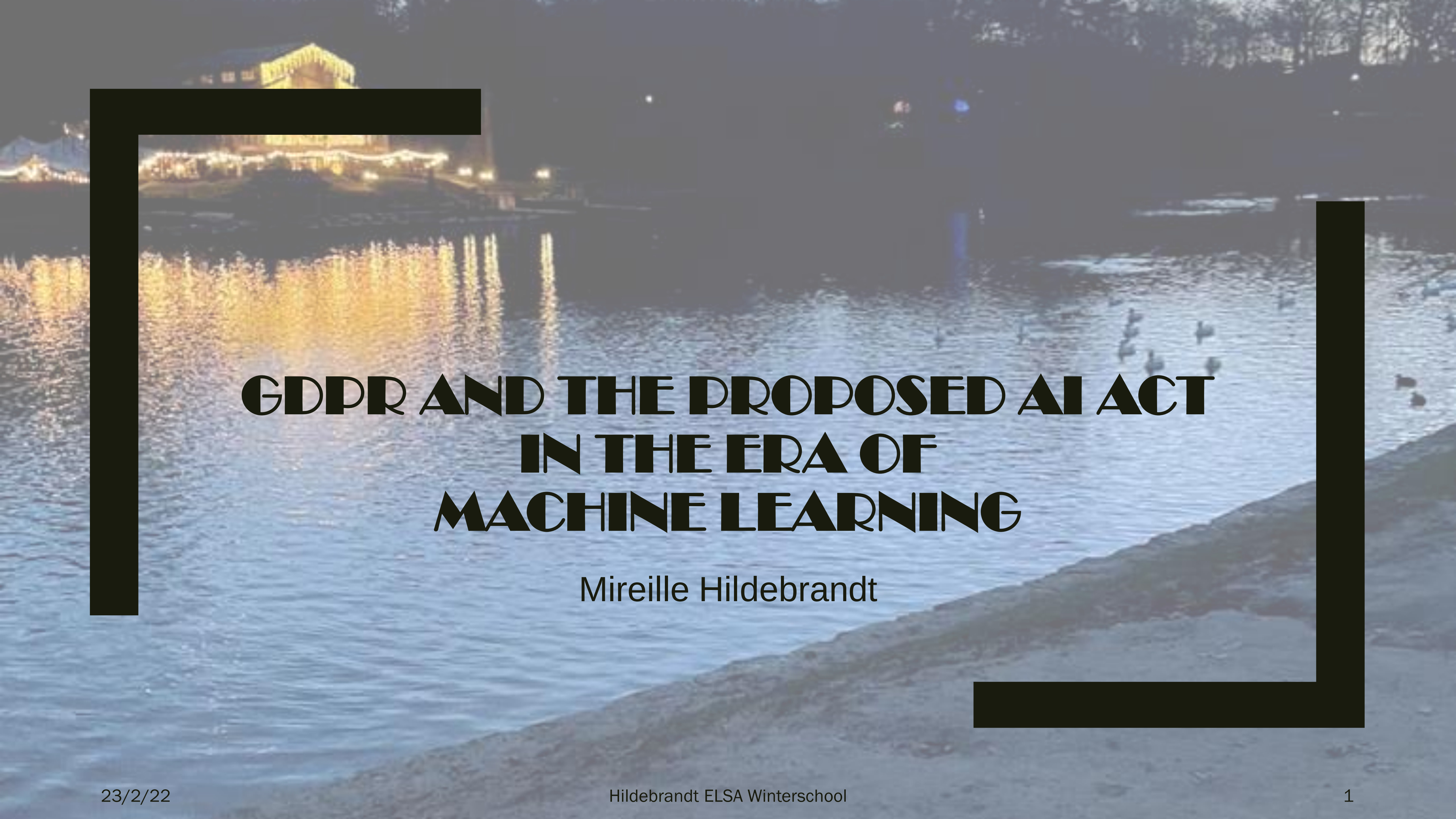


GDPR AND THE PROPOSED AI ACT IN THE ERA OF MACHINE LEARNING

Mireille Hildebrandt

Rule of law

Article 2 TEU

- The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.
- These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

Rule of law

Art. 322 TFEU

1. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, and after consulting the Court of Auditors, shall adopt by means of regulations:

   a) the financial rules which determine in particular the procedure to be adopted for establishing and implementing the budget and for presenting and auditing accounts;

Rule of law

Case C-156/21 (16 February 2022), ACTION for annulment of Regulation (EU, Euratom) 2020/2092 on a general regime of conditionality for the protection of the Union budget

Hungary, supported by the Republic of Poland, submits, (…)

- First, Article 322(1)(a) TFEU does not enable
  - *either the concept of 'the rule of law' or*
  - *that of 'breaches of the principles of the rule of law' to be defined.*
- Secondly, the relationship between
  - *breaches of the principles of the rule of law*
  - *and the Union budget is too broad*
  - *and would, if accepted, enable any area of EU law and significant aspects of the legal systems of the Member States to be linked to it.*

Rule of law

- Article 2(a) of the contested regulation states that the concept of ‘the rule of law’
  - *is to be understood, for the purposes of that regulation,*
    as the ‘Union value enshrined in Article 2 TEU’ and
  - *that that concept includes the principles of legality, legal certainty, prohibition of arbitrariness of the executive powers, effective judicial protection, separation of powers and non-discrimination and equality before the law.*

Rule of law

- That provision states, however, that the concept of ‘the rule of law’,
  - *as defined for the purposes of the application of the contested regulation,*
- ‘shall be understood having regard to the other Union values and principles enshrined in Article 2 TEU’.
- It follows that respect for those values and principles
  - *– in so far as they form part of the very definition of the value of ‘the rule of law’ contained in Article 2 TEU or, as is apparent from the second sentence of that article, are closely linked to a society that respects the rule of law –*
- may be required in the context of a horizontal conditionality mechanism such as that established by the contested regulation.

Rule of law

Article 2 TEU

- The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities.
- These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.

Rule of law

- Rule of law cannot be defined by way of a closed, logical definition
  - *It is about checks and balances and requires judgement rather than reckoning (Cantwell Smith)*
  - *This is not a bug but a feature*
- It is an essentially contested concept
  - *Formal, substantive and procedural conceptions*
  - *It cannot be 'fixated' completely in advance*
- As a foundational concept, if not vanishing point, 'the rule of law'
  - *Has open texture (Hart)*
  - *Requiring judgement and discretion*
  - *While such discretion cannot be arbitrary and assumes normative commitment (Dworkin)*

Rule of law

- Can we develop an algorithm for the rule of law?
- Does that imply that we cannot decide on violations?
- Should *lex certa* prevent us from giving legal effect to such violations?

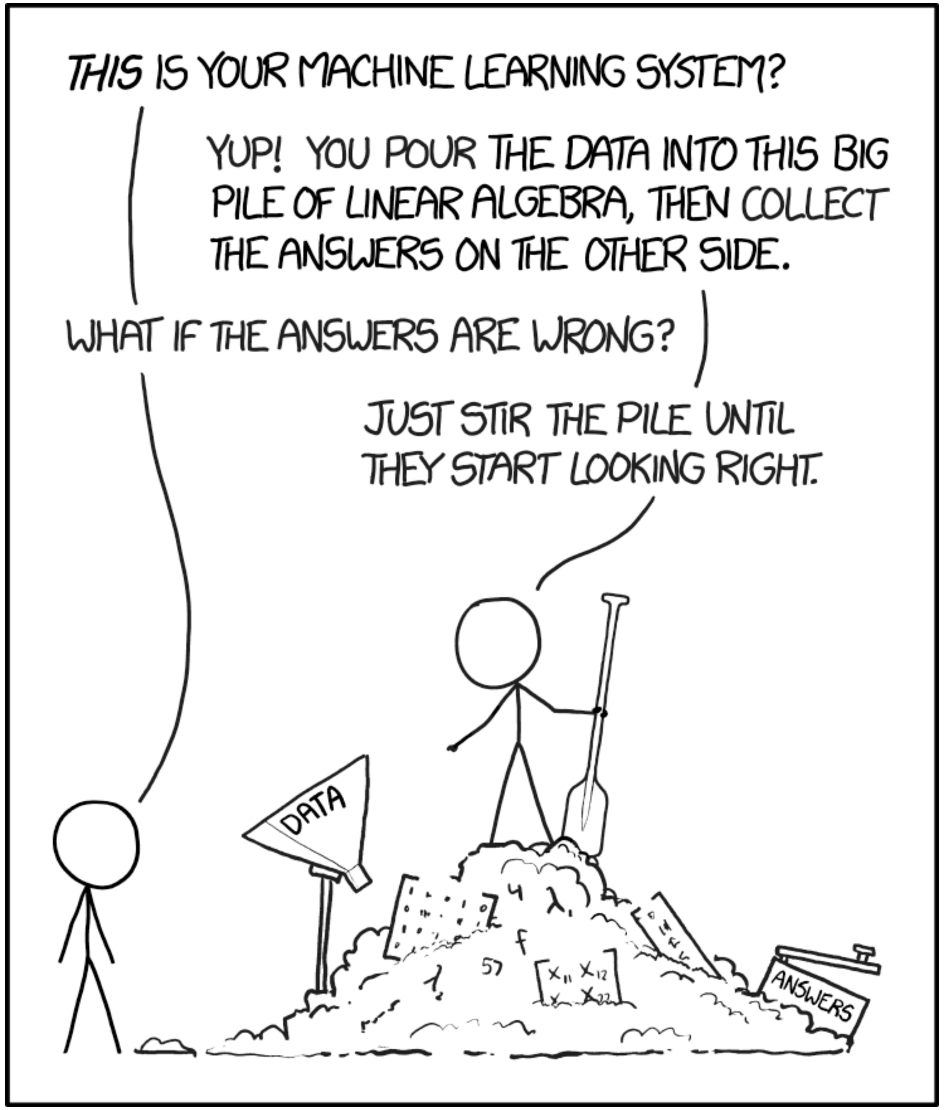
What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?


THIS IS YOUR MACHINE LEARNING SYSTEM?
YUP! YOU POUR THE DATA INTO THIS BIG PILE OF LINEAR ALGEBRA, THEN COLLECT THE ANSWERS ON THE OTHER SIDE.
WHAT IF THE ANSWERS ARE WRONG?
JUST STIR THE PILE UNTIL THEY START LOOKING RIGHT.
DATA
ANSWERS

Machine Learning

- You have a dataset
- You split it up 80/20 in a training set and validation set
- You deploy ‘an algorithm’ to detect patterns in the training data
- These patterns are mathematical functions (they are taken from your hypothesis space)
- The patterns depend on the distribution of the data
- To get things right you optimise the function as much as possible
- Once you find ’relevant’ patterns you test them against your validation set

Machine Learning

- You have a dataset, consisting of 1500 exam papers
- You (teacher) grade 50 papers
- You share the grade with the ‘learner algorithms’:
- This would be supervised learning: data is labelled (this data gets that grade)
- The learner figures out the statistical correlations between text and grades
- You and the system each grade another 50 papers
- You compare the grading and ‘correct’ the system (reinforcement learning)
- You repeat this until the system gets it right
- And hey, it works

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

Defining AI (CS Perspective)

- Code-driven systems (GOFAI)
  - *Rule-based, logic-based, knowledge-based, ITTT*
  - *ADM: tax or student-grant applications, social benefits, online insurance*

- Data-driven systems (AIMA)
  - *KDD, Machine learning, deep learning, natural language processing*
  - *Fraud detection (plagiarism), insurance, credit rating*

Defining AI (CS Perspective)

- AI: human intelligence as the benchmark for artificial intelligence
  - *Darmouth 1956 Workshop:*

‘The study is to proceed on the basis of the conjecture that

- every aspect of learning or any other feature of intelligence
- can in principle
- be so precisely described
- that a machine can be made to simulate it’

Defining AI (CS Perspective)

- AI: human intelligence as the benchmark for artificial intelligence
  - *Newell and Simon 1976:*

'By 'general intelligent action' we wish to indicate

- the same scope of intelligence as we see in human action:
- that in any real situation
- behavior appropriate to the ends of the system and
- adaptive to the demands of the environment can occur,
- within some limits of speed and complexity '

Defining AI (CS Perspective)

- AI: as a research or developers’ activity concerning a quality
  - *Niels J. Nilsson 2010*

‘Artificial intelligence is that activity

- devoted to making machines intelligent, and
- intelligence is that quality that
- enables an entity to function appropriately and with foresight
- in its environment’

Defining AI (CS Perspective)

- AI: as a capacity
  - *Wang 2019*

‘Intelligence is

- the capacity of an information-processing system
- to adapt to its environment
- while operating with insufficient knowledge and resources’

Defining AI (CS Perspective)

- Note the paradox of autonomy:
  - *AI is defined in terms of independent adaptive behaviour in an environment*
  - *But it is made so and qualified as such by its developers*

- Current day AI is nothing like this, cf ‘autonomous’ cars levels 0-5:

  0. no sustained vehicle control [no automation]

  1. hands-on [driver assistance]

  2. hands-off [partial automation]

  3. eyes-off [conditional automation]

  4. mind off [high automation]

  5. steering wheel optional [full automation]

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

Defining AI (legal perspective)

OECD Recommendations 2019 (cp. FIPS 1980 and their impact)

- ‘An AI system is
  - *a machine-based system that can,*
  - *for a given set of human-defined objectives,*
  - *make predictions, recommendations, or decisions*
  - *influencing real or virtual environments.*
  - *AI systems are designed to operate with varying levels of autonomy.’*

Defining AI (legal perspective)

OECD Recommendations 2019 (cp. FIPS 1980 and their impact)

1. legislation should not target ‘AI’ in general, the research domain of AI, or inflated models of supposedly forthcoming systems, but identifiable real world systems,
2. it should only target systems that are machine-based,
3. AI systems should be understood in the context of their intended purpose as defined by their human creators,
4. they should be defined in terms of their output, notably predictions, recommendations or decisions, and
5. their impact on real or virtual environments, while
6. taking into account they can have very different levels of autonomy.

Defining AI (legal perspective)

Art. (3) of the US National AI Initiative Act of 2020

- The term "artificial intelligence" means
  - *a machine-based system that can,*
  - *for a given set of human-defined objectives,*
  - *make predictions, recommendations or decisions*
  - *influencing real or virtual environments.*

Artificial intelligence systems use machine and human-based inputs to

A. *perceive real and virtual environments;*
B. *abstract such perceptions into models through analysis in an automated manner; and*
C. *use model inference to formulate options for information or action.*

Defining AI (legal perspective)

Art. 3(1) of the proposed EU AI Act:

‘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;

Defining AI (legal perspective)

Art. 3(1) of the proposed EU AI Act (Council Amendment)

‘artificial intelligence system’ (AI system) means

- a system

i. that 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;

Defining AI (legal perspective)

Annex I of the proposed EU AI Act:

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.

Defining AI (legal perspective)

- **In terms of techniques and approaches (US, EU)**
  - ***Preventing both***
    - **Underinclusion: from software to system (future AI systems)**
    - **Overinclusion: adding ‘learning, reasoning and modelling’ (ADM?)**
- **In terms of impact (OECD, US, EU)**
  - ***Preventing both***
    - **Threats to safety, health and fundamental rights of natural persons**
    - **Unnecessary limitations on ‘innovation’**

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

Processing of personal data (legal basis, principles and transparency)

- Legal basis: Consent, contract, legal obligation, vital interests, task in the general interest or exercise of official authority, legitimate interest
- Principles:
  - *Lawfulness, fairness and transparency*
  - *Purpose limitation*
  - *Data minimisation*
  - *Accuracy*
  - *Storage limitation*
  - *Integrity and confidentiality*

Goals and risk approach (DPbD and DPIA)

Art. 1 GDPR

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Goals and risk approach (DPbD and DPIA)

Art. 35 GDPR DPIA

1. Where a type of processing in particular using new technologies
   - *and taking into account the nature, scope, context and purposes of the processing,*
   - *is likely to result in a high risk to the rights and freedoms of natural persons,*
   - *the controller shall, prior to the processing,*
   - *carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

   (…)

Goals and risk approach (DPbD and DPIA)

Art. 35 GDPR DPIA

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

Goals and risk approach (DPbD and DPIA)

Art. 35 GDPR DPIA

7. The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Goals and risk approach (DPbD and DPIA)

Art. 25 GDPR DPbDD

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing
   - *as well as the risks of varying likelihood and severity for rights and freedoms of* **natural persons** *posed by the processing,*
   - *the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself,*
   - *implement appropriate technical and organisational measures,*
   - *such as pseudonymisation,*
   - *which are designed to implement data-protection principles, such as data minimisation,*
   - *in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

Goals and risk approach (DPbD and DPIA)

Art. 25 GDPR DPbDD

2. The controller shall implement
   - *appropriate technical and organisational measures for ensuring that, by default,*
   - *only personal data which are necessary for each specific purpose of the processing*
   - *are processed.*

   That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

   In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

Prohibition of ADM systems (conditions and exceptions)

Article 22 **Automated individual decision-making, including profiling**

1. The data subject shall have the right
   - *not to be subject to*
   - *a decision*
   - *based solely on automated processing, including profiling,*
   - *which produces legal effects concerning him or her or similarly significantly affects him or her.*

Prohibition of ADM systems (conditions and exceptions)

Article 22 **Automated individual decision-making, including profiling**

2. Paragraph 1 shall not apply if the decision:
   a) *is necessary for entering into, or performance of, a contract between the data subject and a data controller;*
   b) *is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or*
   c) *is based on the data subject's explicit consent.*

Prohibition of ADM systems (conditions and exceptions)

Article 22 **Automated individual decision-making, including profiling**

3. In the cases referred to in points (a) and (c) of paragraph 2,
   - *the data controller shall implement*
   - *suitable measures to safeguard the data subject's rights and freedoms and legitimate interests,*
   - *at least the right*
     - to obtain human intervention on the part of the controller,
     - to express his or her point of view and
     - to contest the decision.

Prohibition of ADM systems (conditions and exceptions)

Article 22 **Automated individual decision-making, including profiling**

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1),
   - *unless point (a) or (g) of Article 9(2) applies and*
   - *suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.*

Goals and Risks?

- Goal of the GDPR:
  - *Harmonisations of the protection of fundamental rights and freedoms*
  - *To take away obstructions for free movement of personal data*

- Risks to fundamental rights and freedoms in the GDPR:
  - *Risk of infringements or risk of violation?*
  - *DPIA and DPbDD is risk management or precaution?*
  - *Risk management is extra duty, does not rule out liability*

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

Goals and risk approach (safety, health, fundamental rights)

The Commission puts forward the proposed regulatory framework on Artificial Intelligence with the following **specific objectives**:

- *ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;*
- *ensure legal certainty to facilitate investment and innovation in AI;*
- *enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;*
- *facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.*

Goals and risk approach (safety, health, fundamental rights)

Roles:

- Most of the obligations are on the provider:
  - *Whoever first makes available on the market or puts into service an AI system under their own name or brand (in the course of a commercial activity)*
- Rather than on the user (deployer) of the system
  - *Using an AI system under their authority (deployment)*
  - *In the GDPR this 'user' would most often be the data controller*
- The AIA or AIR opts for upstream accountability, though it does not directly address developers, unless they are also the provider

Goals and risk approach
(safety, health, fundamental rights)

Horizontal EU legislation that takes a proportionate risk approach:

Art. 5: prohibited AI practices

- *Manipulation, exploitation, social scoring*
- *Use of real-time remote biometric ID systems by law enforcement*

Art. 8-17: dedicated requirements for AI systems qualified as high risk (mostly providers):

- *Annex II: robotics, aircraft, medical devices (risk to safety and health)*
- *Annex III: biometric systems, specific contexts (risk to FRs)*

Art. 52: transparency requirements for certain AI systems:

- *AI systems that interact with natural persons (providers)*
- *Emotion recognition and biometric categorisation systems (users)*
- *Deep fake systems (users)*

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

Obligations in case of high risk systems

- Risk management system in place (iterant throughout life cycle):
  - *Identification and analysis of foreseeable risks of use for the intended purpose [and reasonably foreseeable misuse]*
  - *Taking into account information of postmarket monitoring*
  - *Taking a 'by design' approach insofar as possible*
  - *Implementation of mitigation and control measures*
  - *Testing of the effectiveness of risk mitigation mesures*

Obligations in case of high risk systems

- Data and data governance
  - *Training, validation and testing data*
  - *Keen attention to relevant design choices, completeness, being error free*
  - *Appropriate statistical properties*
  - *Bias monitoring (exception to prohibition of art. 9 GDPR)*

- Documentation and record keeping
- Information for those who deploy the system

Obligations in case of high risk systems

- Human oversight
  - *Designed and developed for effective human oversight*
  - *To prevent or minimise risks to health, safety or FRs*
  - *Oversight measures built-in by the provider or to be implemented by the user*
  - *Such that natural persons tasked with oversight:*
    - Understand the capacities and limitations of the system
    - Remain aware of automation bias
    - Correctly interpret the system’s output
    - Can disregard, override or reverse the output
    - Can stop the system if need be

Obligations in case of high risk systems

- Accuracy, robustness and cybersecurity
  - *Reliability, metrics, resilient against errors, robust (e.g. fallback plans)*
  - *Prevent feedback loops if systems continue to learn'*

- Quality management system
  - *Integrating the previous requirements*
  - *Examination, test and validation procedures*
  - *Postmarket monitoring system*
- Technical documentation, automated logging

What's next

- What is AI?
  - *Defining AI from a CS perspective (levels of autonomy)*
  - *Defining AI from a legal perspective (impact or methodology)*

- How does the GDPR apply to AI systems?
  - *Goals and risk approach (DPbD and DPIA)*
  - *Prohibition of ADM systems (conditions and exceptions)*

- How does the proposed AI Act apply to AI systems?
  - *Goals and risk approach (safety, health, fundamental rights)*
  - *Obligations in case of high risk systems*

- AI Systems under the rule of law?

AI systems under the rule of law?

- legality
  - *Public administration, police*
- legal certainty
  - *Corporations, natural persons, insurance, housing, credit rating, education*
- prohibition of arbitrariness of the executive powers
  - *Police, tax office, social benefits*
- effective judicial protection
  - *Facebook oversight board? Robocourts? Transparency, contestability?*
- separation of powers
  - *All using the same legal search engine?*
- non-discrimination and equality before the law
  - *Who can buy best legal technologies or resist ‘computer says no’ or obtain a credit?*

AI systems under the rule of law?

- Problems with legal protection in the GDPR and the AI Act:
  - *ADM has major impact, only partly within scope GDPR*
  - *ADM may fall outside scope of AIA, if not learning/reasoning/modelling*
  - *Council proposal to exclude general purpose AI systems from the scope*
  - *Pipeline issues:*
    - What counts as a decision in context art. 22 GDPR?
    - Who becomes accountable for bias in general purpose AI?
    - Distribution of responsibility between providers and deployers?

AI systems under the rule of law?

Hildebrandt proposes to add: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2662611_en

A. The right not to be subject to prohibited AI practices

B. The right to object to decisions made by high-risk AI systems

C. The right to file an injunction in a court of law, and to mandate that right to an NGO in case one is subjected to prohibited AI practices or to decisions made by high-risk AI systems

D. The right of dedicated NGOs to file an injunction in their own name with respect to the rights under A and B