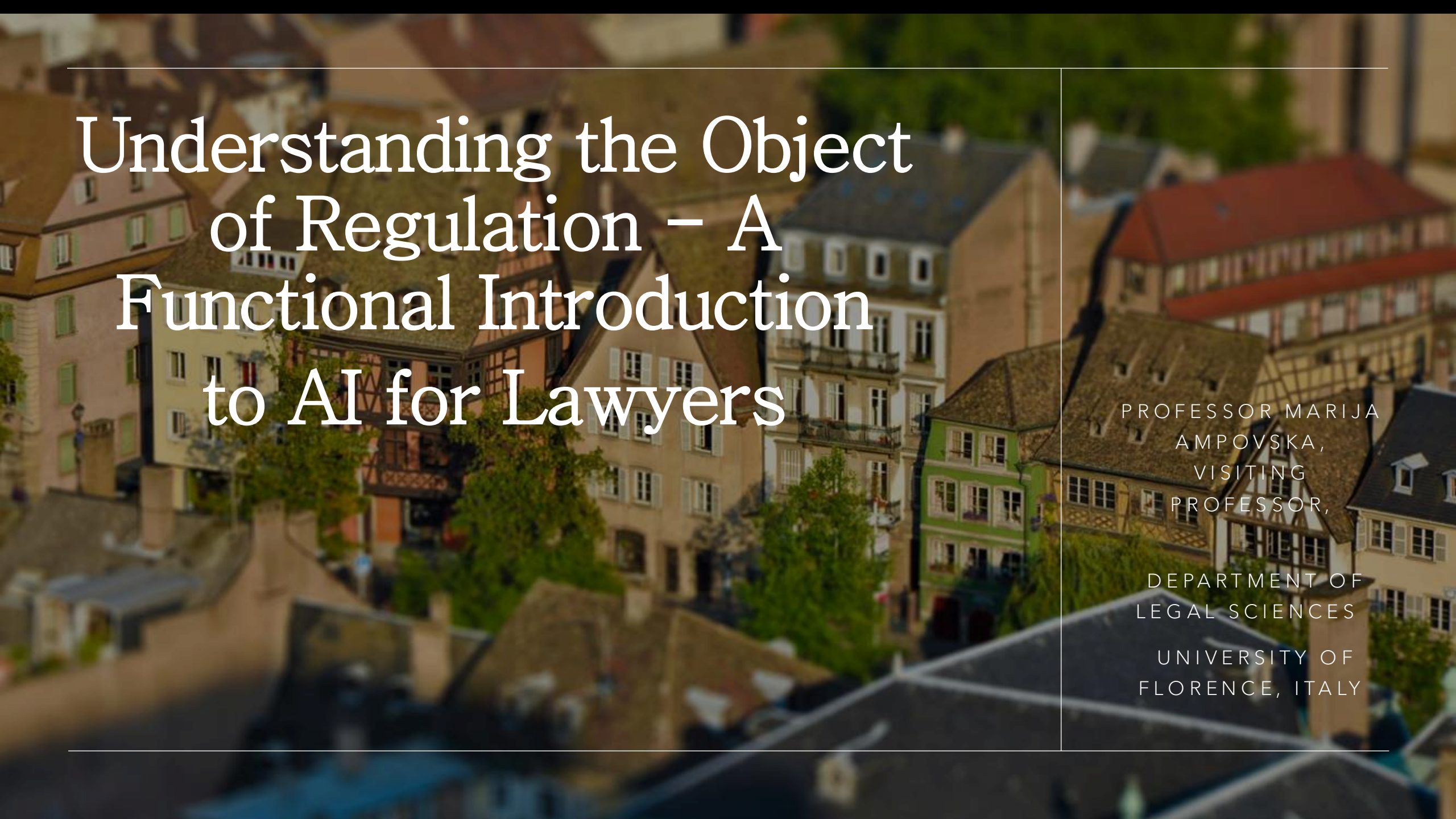


Understanding the Object of Regulation – A Functional Introduction to AI for Lawyers

PROFESSOR MARIJA AMPOVSKA, VISITING PROFESSOR,

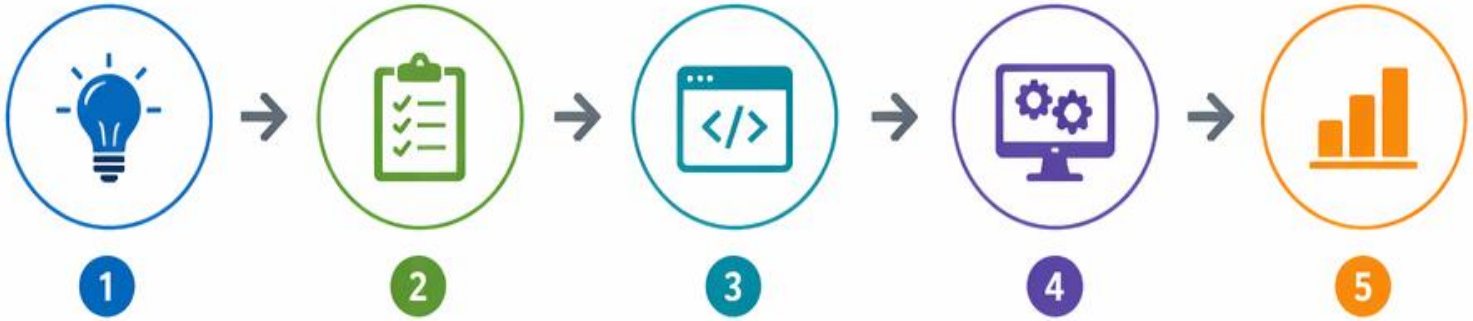
DEPARTMENT OF LEGAL SCIENCES

UNIVERSITY OF FLORENCE, ITALY

ALGORITHMS: THE FOUNDATION OF SOFTWARE

Algorithms are a set of **rules or instructions** that are followed when performing calculations, or more generally, a set of **problem-solving procedures** that when followed produce a certain **output**. They are now most familiar as instructions embodied within computer programs, such as those that make **AI** possible.

FROM PROBLEM TO OUTPUT



1. **PROBLEM** — A task or question that needs to be solved.
2. **ALGORITHM** — A step-by-step set of rules or instructions to solve the problem.
3. **CODE** — The algorithm is written in a programming language.
4. **SOFTWARE EXECUTION** — The computer follows the code and performs the instructions.
5. **OUTPUT** — The result or solution produced after execution.

ALGORITHM, CODE & SOFTWARE

Concept	Description	Example
ALGORITHM	Step-by-step problem-solving procedure or logic.	• Finding largest number • Sorting numbers • Calculating average
CODE	Implementation of algorithm in a specific programming language.	• Python code • Java code • C++ code
SOFTWARE	A complete program that uses algorithms to achieve goals.	• Mobile apps • Websites • AI systems

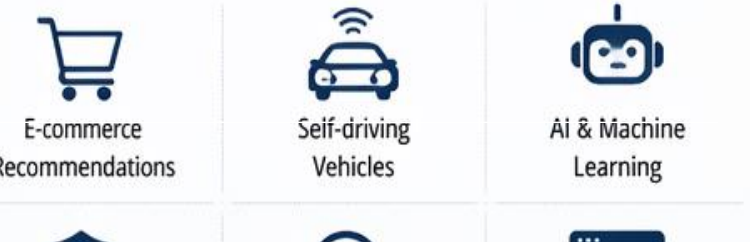
ROLE OF ALGORITHMS IN SOFTWARE

- Define the logic and flow of software
- Break complex problems into simple steps
- Improve efficiency and accuracy

FROM IDEA TO CODE

1. Algorithm
2. Programming
3. Executable Code

WHERE ALGORITHMS ARE USED



- E-commerce Recommendations
- Self-driving Vehicles
- AI & Machine Learning

AI SYSTEM: VISUAL OVERVIEW

1. PERCEIVE
Data Acquisition

Observe the environment through sensors or data sources.

2. INTERPRET
Data Processing

Clean, organize and understand the collected data.

3. REASON
Knowledge & Inference

Use AI models and knowledge to derive insights or predictions.

4. ACT
Decision & Action

Make decisions and take actions to achieve the goal.

GOAL
Achieve Objective

Achieve the desired outcome or solve the problem.

FEEDBACK LOOP

The system learns from results and improves over time.

EXAMPLES OF AI SYSTEMS IN REAL LIFE

RECOMMENDATION SYSTEMS
Suggest products, movies or content based on user preferences

VIRTUAL ASSISTANTS
Understand voice or text commands and provide information or help.

FACE RECOGNITION
Identify or verify individuals from images or videos.

INDUSTRIAL AUTOMATION
Use robots and AI to optimize production and reduce human effort

SELF-DRIVING CARS
Perceive surroundings, make decisions and drive autonomously

AI IN HEALTHCARE
Assist in diagnosis, predict outcomes and personalize treatment.

KEY AI TECHNIQUES & CAPABILITIES

MACHINE LEARNING
Enables systems to learn patterns from data.

NATURAL LANGUAGE PROCESSING
Enables systems to understand, interpret and generate human language.

COMPUTER VISION
Enables systems to interpret and understand visual information.

ROBOTICS
Enables physical actions in the real world through automation.

AUTONOMOUS SYSTEMS
Assisles systems to operate independently and make decisions in dynamic environments.

Categories of AI Systems under the AI Act

Risk Level	Category	Regulatory Outcome
Unacceptable Risk	Prohibited AI Practices (Article 5)	**Banned** – cannot be placed on the market, put into service, or used
High Risk	High-risk AI systems (Article 6 + Annex III)	**Strict obligations** – conformity assessment, risk management, transparency, human oversight
Limited Risk	AI systems with transparency obligations (Article 50)	**Transparency duties** – inform users that they interact with AI / content is AI-generated
Minimal or No Risk	All other AI systems	**No additional obligations** – voluntary codes of conduct (Article 95)

AI Act, Article 3(63) Definition for GPAI

- *"'General-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."*
- GPAI is a special category under the AI Act, regulated separately from high-risk or prohibited AI.

Two-tier system:

Standard GPAI – basic obligations (documentation, copyright, training data summary)

GPAI with systemic risk – enhanced obligations (evaluation, risk assessment, incident reporting)

Examples of GPAI Models

Model	Type	Why it is GPAI
ChatGPT (GPT-4, GPT-4o)	Large language model	Can write, summarize, translate, code, reason – performs many tasks
DALL·E 3	Text-to-image model	Generates images, edits images, can be adapted for video or design tasks
Stable Diffusion	Text-to-image (open source)	Same as above – general-purpose generation
Llama (Meta)	Large language model	Read, write, code, reason – can be fine-tuned for specific uses
Gemini (Google)	Multimodal model	Text, image, audio, video – wide range of tasks
Claude (Anthropic)	Large language model	General conversation, analysis, coding, reasoning

Where ChatGPT Can Be High-Risk

High-Risk Area (Annex III)	Application of ChatGPT
Employment (& Art. 26)	Screening CVs, analyzing job applications, or evaluating candidates for recruitment/performance triggers high-risk obligations for the employer .
Education	Automated grading of exam answers, evaluating student essays, or determining admission to academic programs .
Access to Essential Services	Assisting in credit scoring decisions, analyzing loan applications, or evaluating insurance risk assessment for life/health policies .
Law Enforcement	Profiling individuals, assessing risk of re-offending, or evaluating the reliability of evidence (subject to legal professional constraints)

Where ChatGPT Cannot Be High-Risk

High-Risk Area (Annex III)	Why ChatGPT Fails Here
Biometrics	**Limitation:** Pure text interface. ChatGPT lacks vision capabilities to process biometric data (fingerprints, iris scans, facial structure) or operate "real-time" identification systems.
Critical Infrastructure	**Safety Risk:** LLMs "hallucinate." You cannot use a probabilistic text generator as a safety component for traffic management (e.g., controlling railway switches) or water/gas supply due to lack of deterministic reliability.
Migration/Asylum	**Legal & Verification Limits:** While text analysis is possible, critical tasks like verifying the authenticity of travel documents or performing polygraph-like assessments require physical inspection or specialized hardware/physical sensors.

Unacceptable risk

- Social scoring for public and private purposes;
- Exploitation of vulnerabilities of persons, use of subliminal techniques;
- Real-time remote biometric identification in publicly accessible spaces by law enforcement, subject to narrow exceptions;
- Biometric categorisation of natural persons based on biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation.
- Filtering of datasets based on biometric data in the area of law enforcement will still be possible;
- Individual predictive policing;
- Emotion recognition in the workplace and education institutions, unless for medical or safety reasons (i.e. monitoring the tiredness levels of a pilot);
- Untargeted scraping of the internet or CCTV (closed-circuit television is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes) for facial images to build-up or expand databases.

Criteria for high-risk AI

High-risk AI systems under the AI Act are not defined by the technology itself, but by the purpose for which they are used and the potential harm they can cause to health, safety, or fundamental rights.

Example

- Medical devices (including AI in robot-assisted surgery) are covered by **Annex I** (Regulation (EU) 2017/745 on medical devices). Under **Article 6(1) of AI Act**, such AI systems are **automatically high-risk** if the product requires third-party conformity assessment.

Limited risk

The AI Act does not provide a standalone, abstract definition of "limited risk." Instead, the Act defines this category by its **regulatory outcome** and the **specific systems it covers**

LEGAL DEFINITION (BY OUTCOME)	MATERIAL DEFINITION (BY CHARACTERISTICS)
• Limited risk AI systems are those that trigger only **transparency obligations** under **Article 50** of the AI Act. Unlike high-risk systems, they are not subject to extensive conformity assessments, risk management systems, or post-market monitoring	• These systems primarily pose risks of **impersonation, deception, or lack of awareness** for users, rather than direct threats to health, safety, or fundamental rights. The obligations are designed to ensure that humans interacting with AI are properly informed