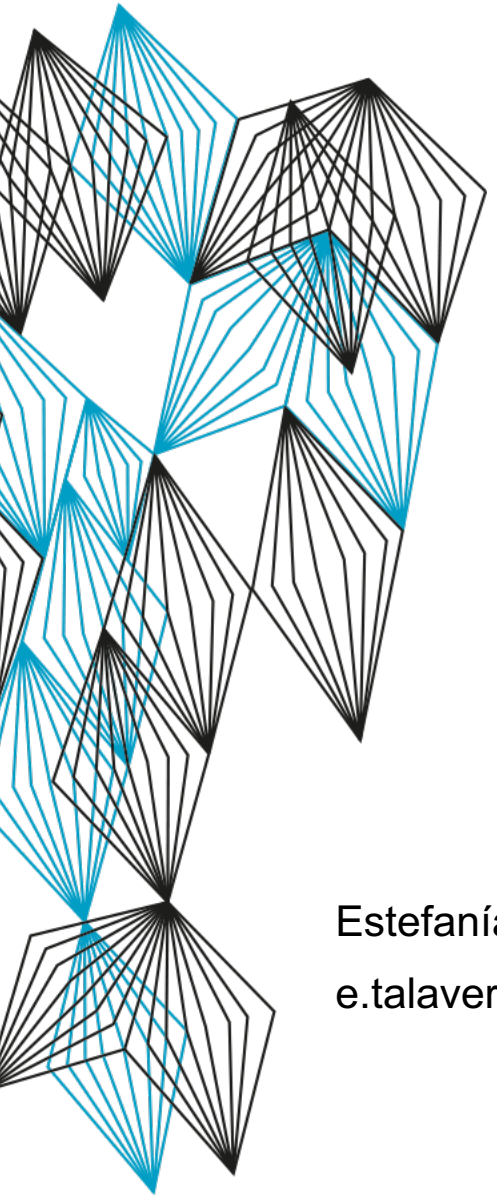


ARTIFICIAL INTELLIGENCE & CYBER SECURITY

NEURAL NETWORKS

Overview

Estefanía Talavera Martínez
e.talaveramartinez@utwente.nl

Types of machine learning problems

Unsupervised learning

input data, no labels

- Clustering: group similar data points.
- Density estimation
- Dimensionality reduction
- Outlier/novelty detection

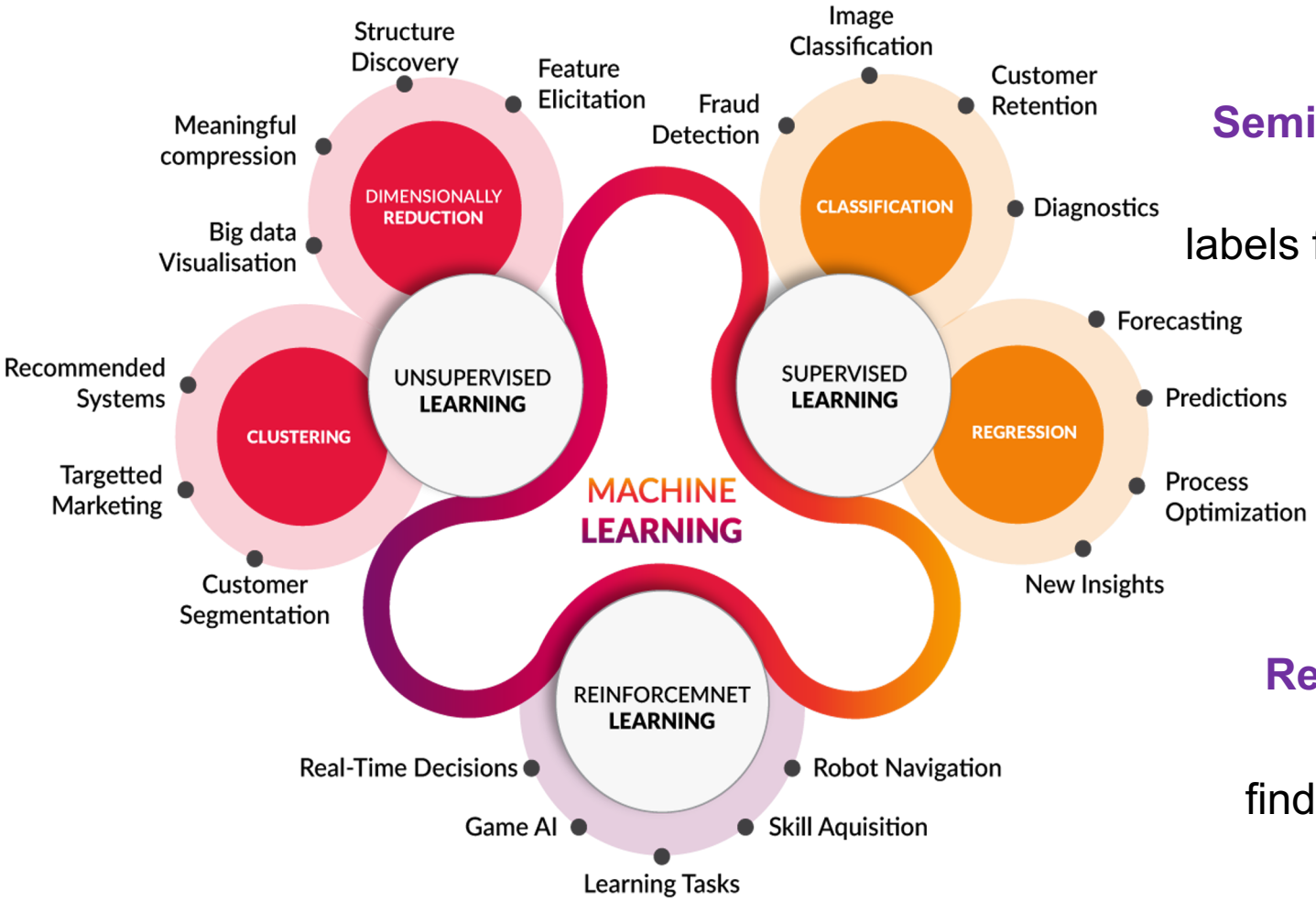


*Image from https://towardsdatascience.com/coding-deep-learning-for-beginners-types-of-machine-learning-b9e651e1ed9d

Supervised learning

labels are provided

- Classification
- Regression

Semi-Supervised learning

labels for just part of the data

Reinforcement learning

find a sequence of actions (policy) that reaches a target.

Types of machine learning problems

Supervised learning

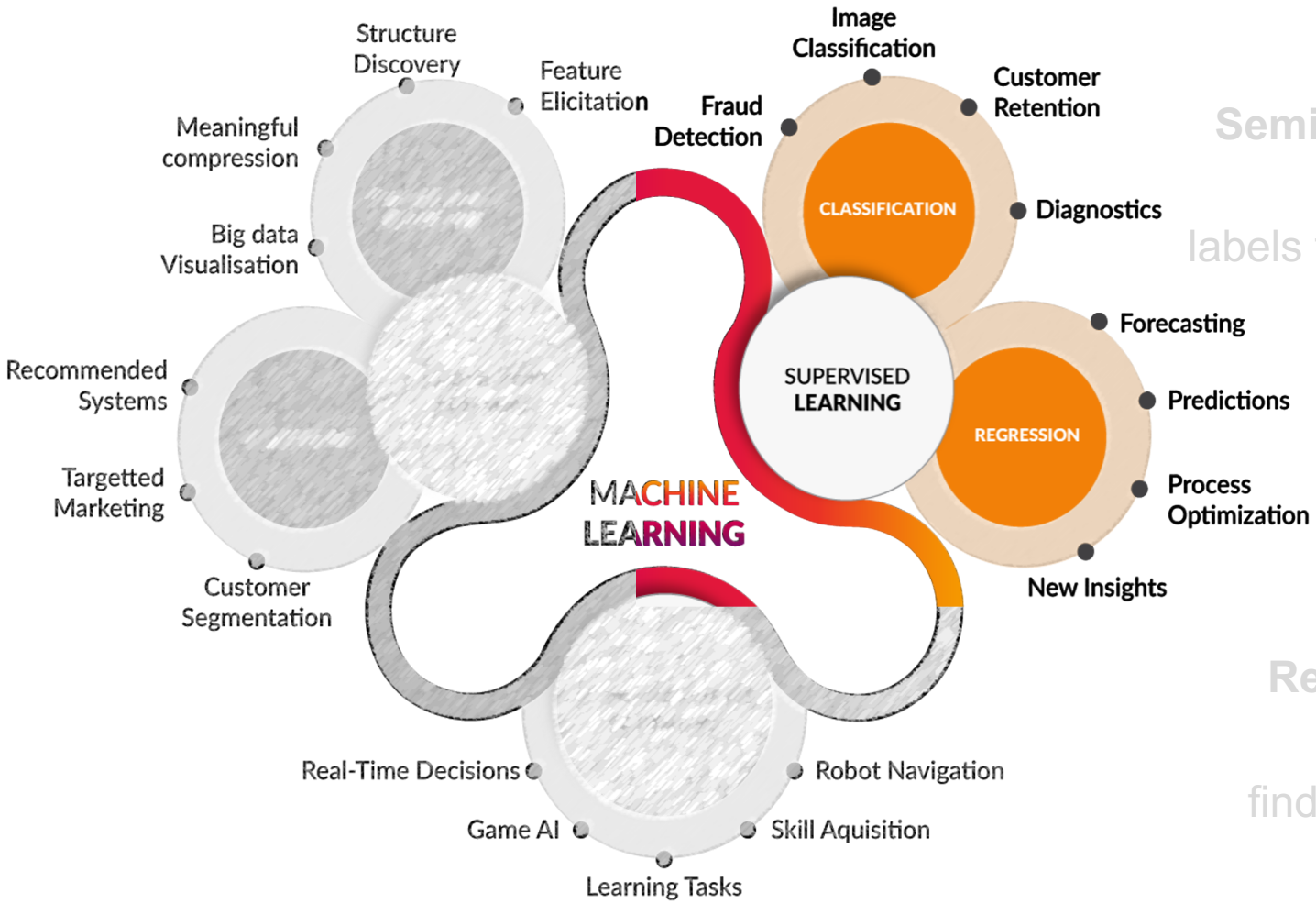
labels are provided

- Classification
- Regression

Unsupervised learning

input data, no labels

- Clustering: group similar data points.
- Density estimation
- Dimensionality reduction
- Outlier/novelty detection



Semi-Supervised learning

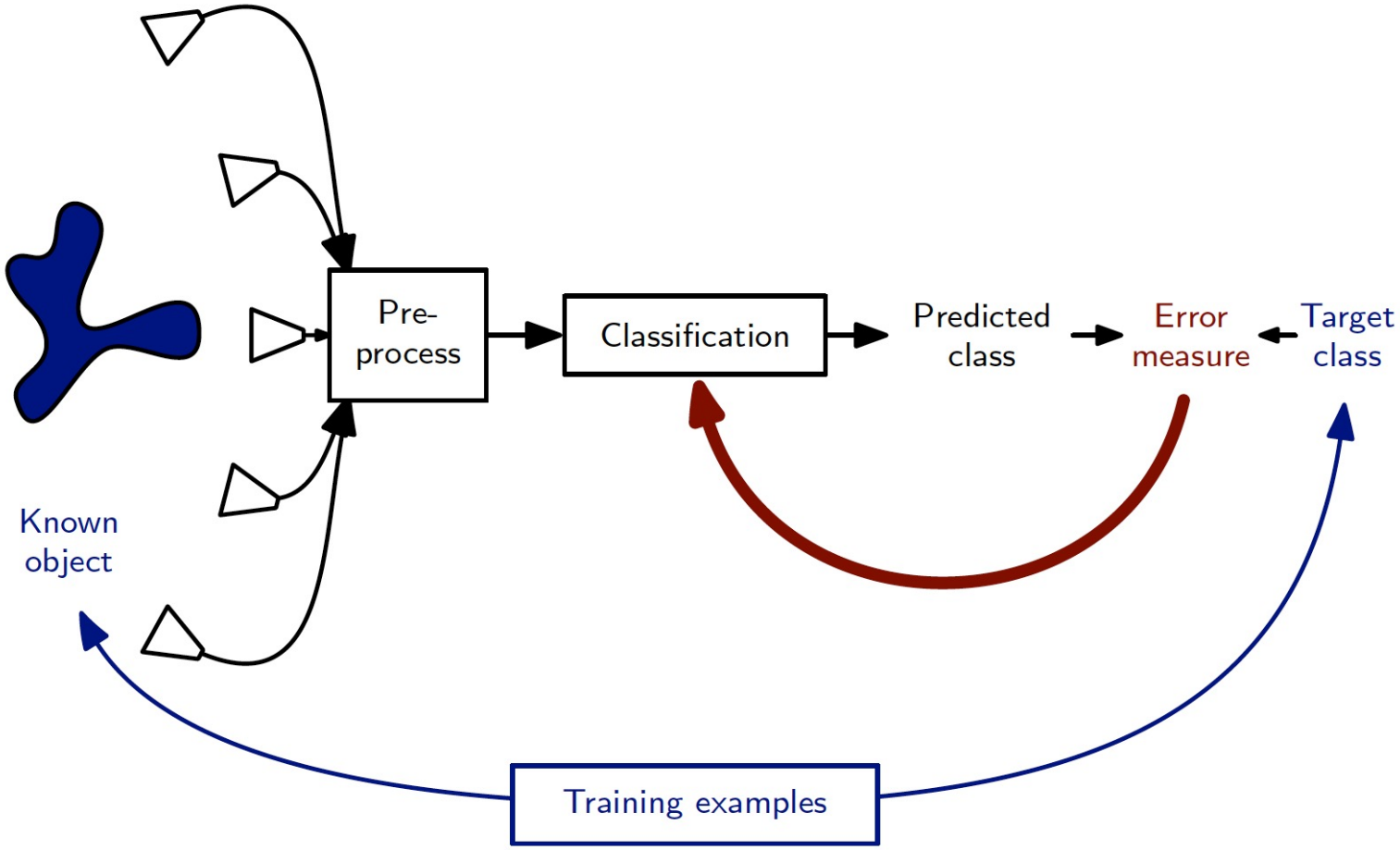
labels for just part of the data

Reinforcement learning

find a sequence of actions (policy) that reaches a target.

*Image from https://towardsdatascience.com/coding-deep-learning-for-beginners-types-of-machine-learning-b9e651e1ed9d

Supervised Training - Classification



Recap

Learning: obtain valid information about a problem from examples
Learning: obtain valid future information about a problem from past experience

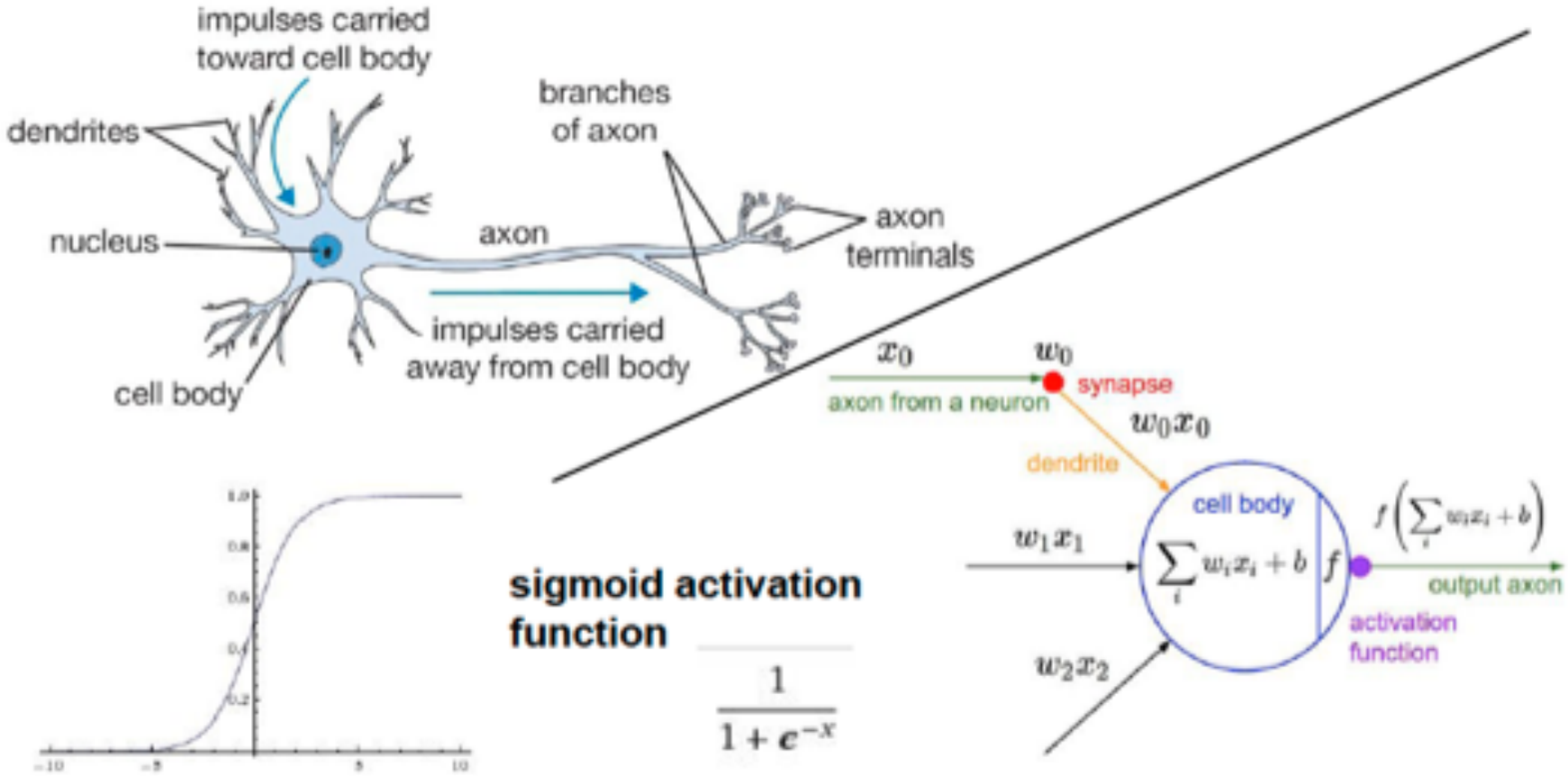
Probabilistic modelling
- Learn probability distributions over variables
- Independence assumptions: simplicity is key to future validity

Decision Trees
- Learn complex relationships between observed and latent variables
- Discriminant as a combination of piecewise linear, axis-aligned decisions

Neural Networks
- Create arbitrarily complex functions, with many interdependent parameters
- Network structure allows automated learning

Why are they called Neural Networks?

Artificial NNs ~ 100M neurons
Human NNs ~ 5B of neurons



Adapted from Fei-Fei Li & Andrej Karpathy & Justin Johnson

CONTENTS

- Perceptron learning algorithm
- Multi-layer perceptrons
- Regularization
- Error backpropagation

- Extra material: What comes next? A brief intro to DL & CV