Künstliche Intelligenz und Persönlichkeitsschutz

am Beispiel Datenschutz

Mein Hintergrund zu diesem Thema:

- Informatiker
- Verwaltungsratsvorsitzender regiocom SE;
- Präs. Arbeitgeberdachverband Sachsen-Anhalt, BDI/BDA-Lv.
- Beiratsvorsitzender Deutsche Stiftung Datenschutz
- Mitglied im Nationalen Cybersicherheitsrat der Bundesregierung

snt regiocom

Gliederung (Versuch)

Künstliche Intelligenz	Datenschutz	Jeder von uns
▪ Was ist KI ▪ Beispiel: Autom. Übersetzen ▪ Werkzeuge der KI	▪ Was ist Datenschutz ▪ Was schützt er ▪ Was nicht	Im Zentrum steht … … eine Frage

Was ist Künstliche Intelligenz

Definitionen

- Es gibt keine allgemeingültige Definition
- Praktikabel: “Künstliche Intelligenz ist die Eigenschaft eines IT-Systems, der menschlichen Kognition ähnliche Fähigkeiten zu zeigen.“
- Schwache KI vs. starke KI
- KI ist nicht monolithisch (div. Modelle, Werkzeuge; “Methoden der KI”)

Historie

- Laplace’scher Dämon (1814)
- Mathematische Methoden (Euler 1750, Boole 1854, Frege 1879, Newell/Simon 1969)
- A. Turing (1950): “Computing Machinery and Intelligence”
- J. Weizenbaum ➔ ELIZA (1967)
- Technologietreiber (-Pull)
  - Sprachverarbeitung/Übersetzung (semantische Modelle)
  - Expertensysteme
  - Schachcomputer (Lösungsstrat.)
  - Roboter (Weltmodelle)

snt regiocom

Was ist Künstliche Intelligenz

Definitionen

- Es gibt keine allgemeingültige Defi
- Prak genz Syst Kogn zeig
- Schw
- KI is (div. Modelle, Werkzeuge; “Methoden der KI”)

Historie

- Laplace’scher Dämon (1814)

Alan Turing:

„Gib genau an, worin deiner Meinung nach ein Mensch einem Computer überlegen sein soll, und ich werde einen Computer bauen, der deinen Glauben widerlegt.“

(zitiert nach Karl Popper)

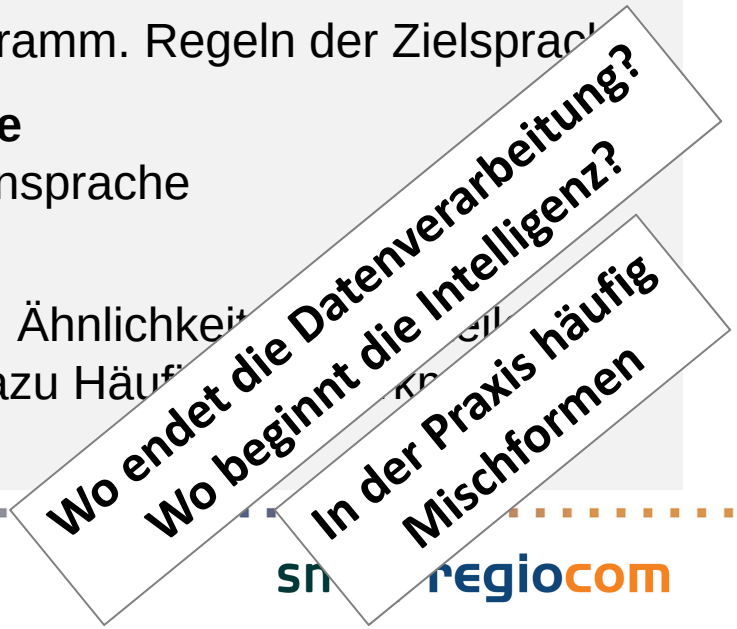
- Expertensysteme
- Schachcomputer (Lösungsstrat.)
- Roboter (Weltmodelle)

snt regiocom

Werkzeuge/Methoden am Beispiel des automatisierten Übersetzens

Unterschiedliche methodische Ansätze

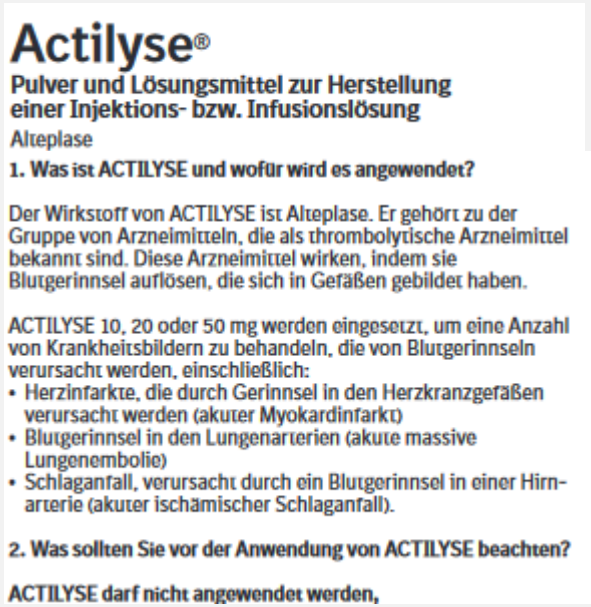
- **Direkte Übersetzung**
  Wort-für-Wort, Satzaufbau nach Strukturregeln (“S-P-O”), dazu Flexionsregeln
- **Transfer-Methode**
  Analyse der grammat. Struktur; Exzerpieren einer semantischen Struktur und Übertr. in die Zielsprache; Texterzeugung nach gramm. Regeln der Zielsprac
- **Interlingua-Methode/Metasprachliche Methode**
  Wie Transfer, aber mit einer “neutralen” Zwischensprache
- **Beispielbasierte Übersetzung**
  Großer Fundus korrekter Beispielübersetzungen, Ähnlichkeit
  Funduselementen mit statistischen Methoden; dazu Häuf
- **Übersetzung mit Hilfe neuronaler Netze**



Was kann KI: Beispiel Spracherkennung/Übersetzung

Problemlos?

Boehringer ist einer der frühen Anwender des autom. Übersetzens



Actilyse®

Pulver und Lösungsmittel zur Herstellung einer Injektions- bzw. Infusionslösung

Alteplase

1. Was ist ACTILYSE und wofür wird es angewendet?

Der Wirkstoff von ACTILYSE ist Alteplase. Er gehört zu der Gruppe von Arzneimitteln, die als thrombolytische Arzneimittel bekannt sind. Diese Arzneimittel wirken, indem sie Blutgerinnsel auflösen, die sich in Gefäßen gebildet haben.

ACTILYSE 10, 20 oder 50 mg werden eingesetzt, um eine Anzahl von Krankheitsbildern zu behandeln, die von Blutgerinnseln verursacht werden, einschließlich:

- Herzinfarkte, die durch Gerinnsel in den Herzkranzgefäßen verursacht werden (akuter Myokardinfarkt)
- Blutgerinnsel in den Lungenarterien (akute massive Lungenembolie)
- Schlaganfall, verursacht durch ein Blutgerinnsel in einer Hirnarterie (akuter ischämischer Schlaganfall).

2. Was sollten Sie vor der Anwendung von ACTILYSE beachten?

ACTILYSE darf nicht angewendet werden,

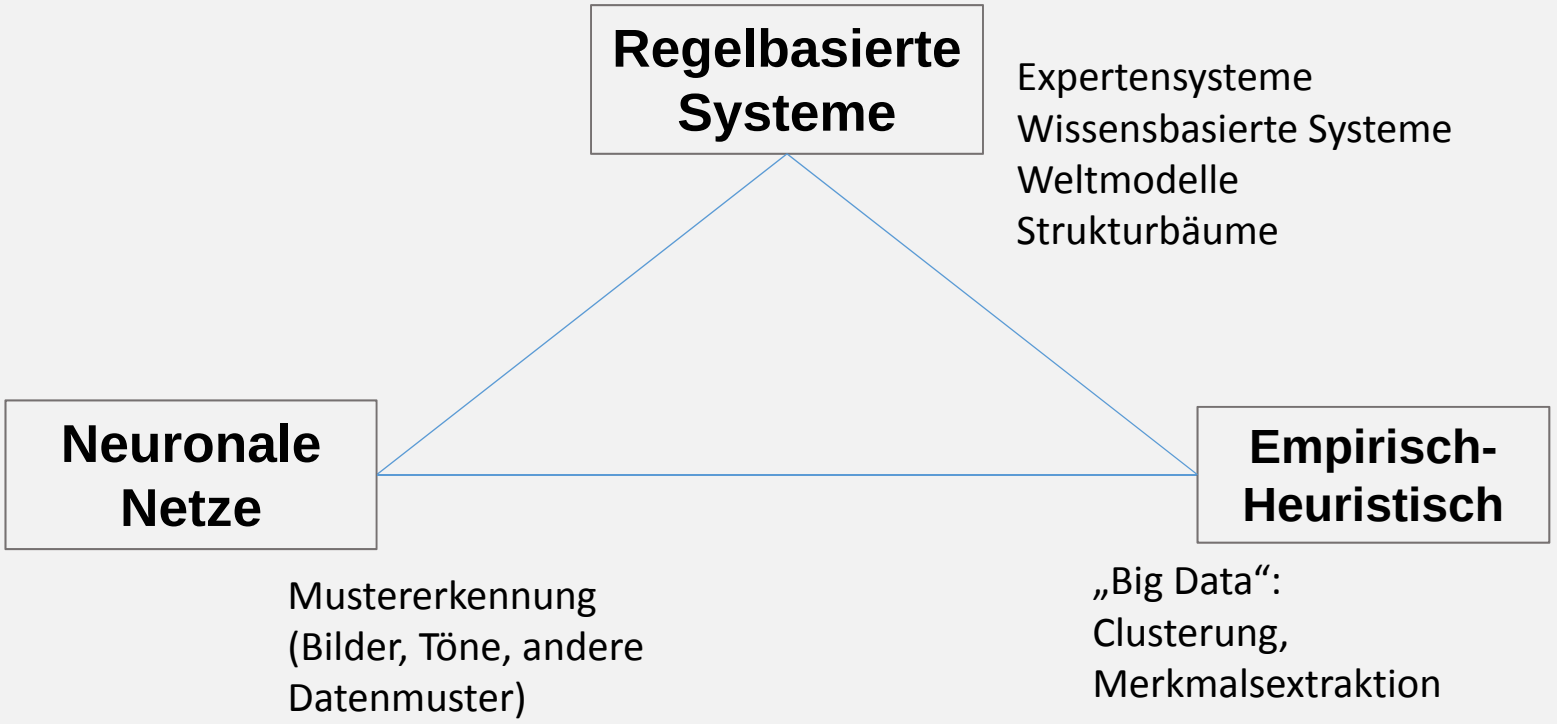
Problem?

“Do hot Nennberrch dene Lederhosn in de ledschdn Minuude den no reingsemmelt”

snt regiocom

Werkzeuge der Künstlichen Intelligenz

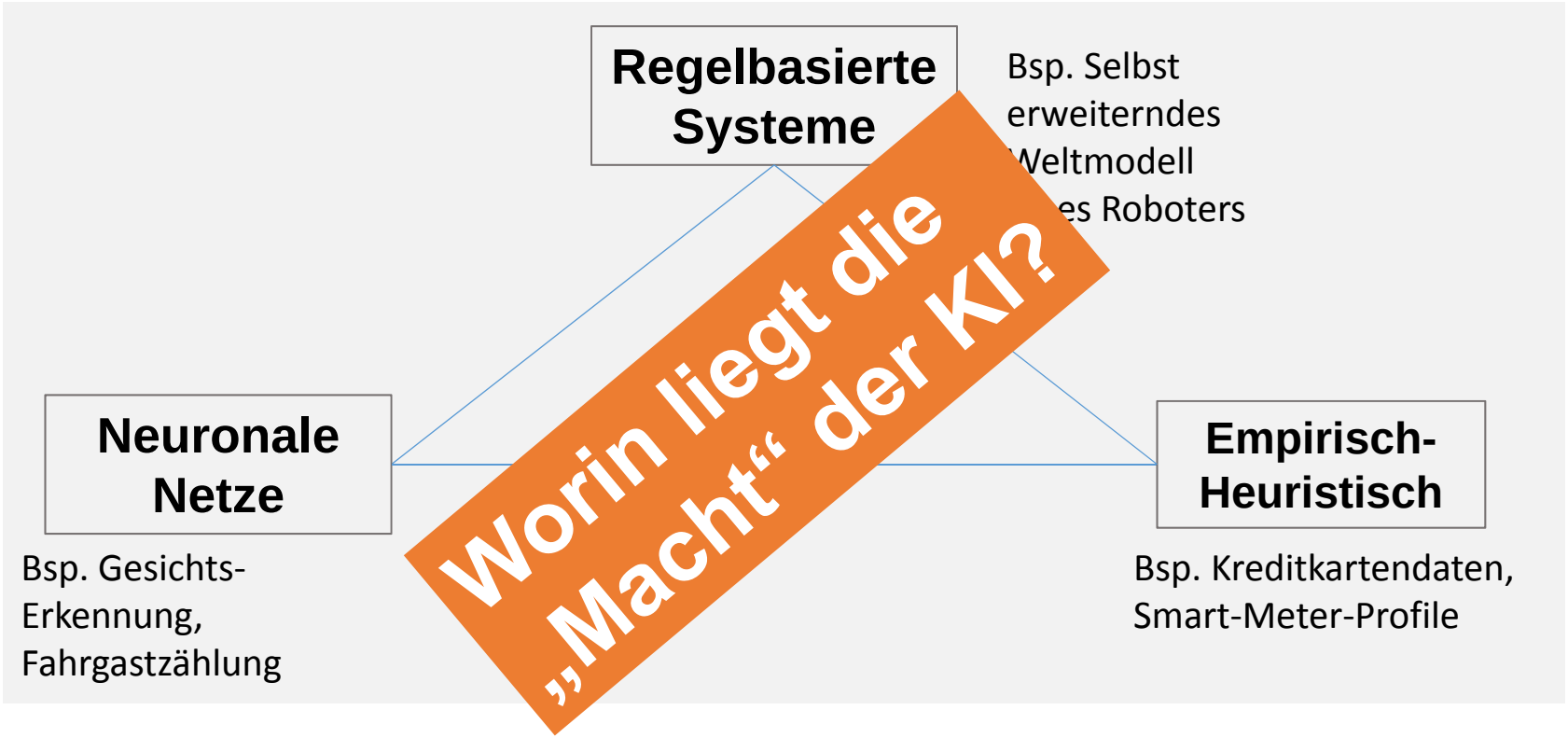
Drei Gruppen von Werkzeugen



snt regiocom

Werkzeuge der Künstlichen Intelligenz

Drei Gruppen von Werkzeugen / Illustrative Beispiele



snt regiocom

Werkzeuge der Künstlichen Intelligenz

Das “Potential” in den einzelnen Bereichen:

Regelbasierte Systeme

Beispiel: Ein selbst erweiterndes Weltmodell eines Roboters

Ausgangslage eines klassischen Weltmodells:

klassisches 3-D-Modell in einem Roboterkäfig

Positionierungsaufgaben bleiben innerhalb des Käfigs

Neu: Der Roboter lernt zum Beispiel

- Flächen (inkl. Käfigwand) können auch elastisch/nachgiebig sein
- der Manipulator kann diesen zusätzlichen Raum nutzen
- die Elastizität ist unterschiedlich stark
- das Drücken an der Wand beeinflusst die Positionierungsqualität

➔ **Vom starren Weltmodell zum selbstlernenden System**

Werkzeuge der Künstlichen Intelligenz

Das “Potential” in den einzelnen Bereichen:

Ein historisches Beispiel:

Ausgangslage: Ein weltweit führendes Kreditkarten-unternehmen will in den späten achtziger Jahren wissen, welcher Informationswert in seinen Daten steckt.

Nach intensiver wissenschaftlicher Analyse, damals ohne „Big Data“:
Auf Basis des Einkaufsverhaltens eines Ehepaares mit Partnerkarten konnte eine präzise Prognose der Scheidungswahrscheinlichkeit und des zu erwartenden Scheidungsjahres gegeben werden. (2-Jahres-Vorausschau mit >80% Sicherheit)

Empirisch-Heuristisch

Bsp. Kreditkartendaten

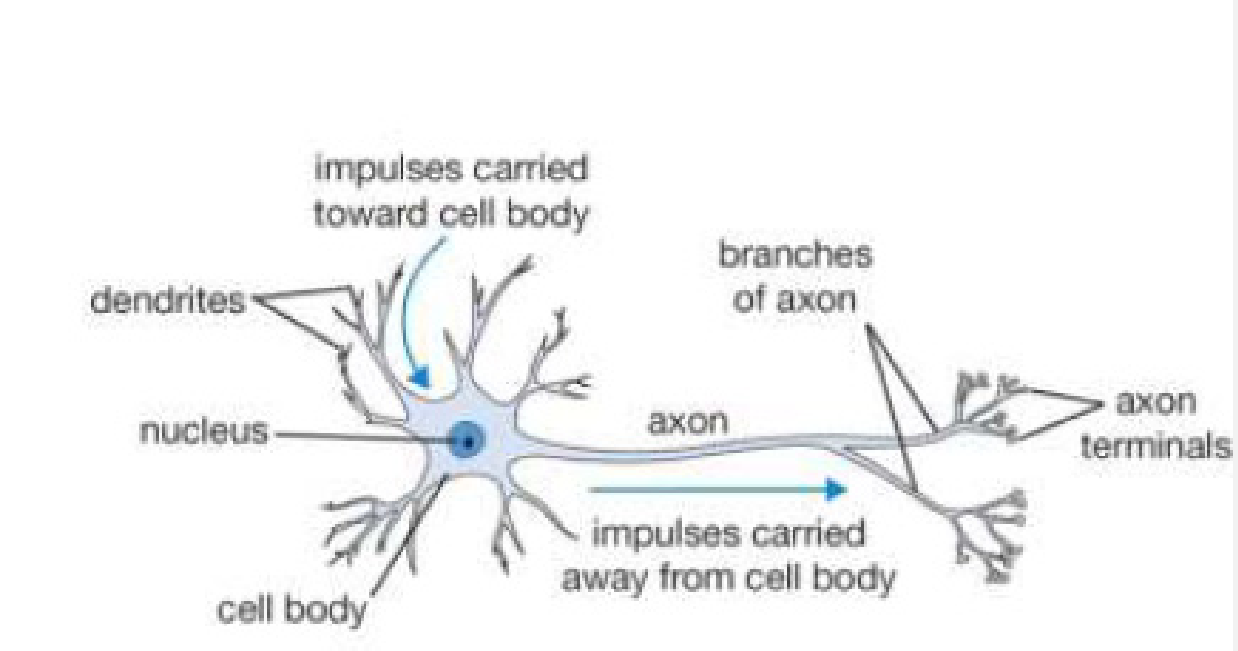
snt regiocom

Werkzeuge der Künstlichen Intelligenz

Das “Potential” in den einzelnen Bereichen:

Neuronale Netze

Bsp. Gesichts-erkennung



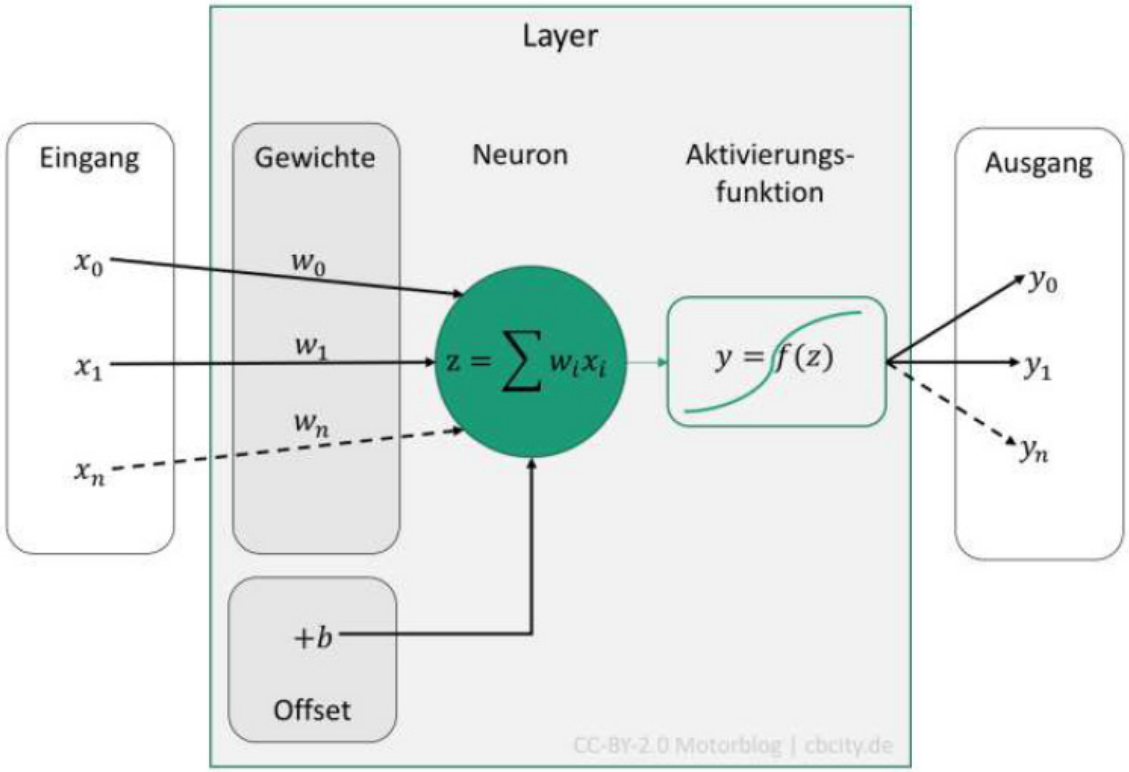
snt regiocom

Werkzeuge der Künstlichen Intelligenz

Die Stärken der einzelnen Bereiche:

Neuronale Netze

Bsp. Gesichts-erkennung



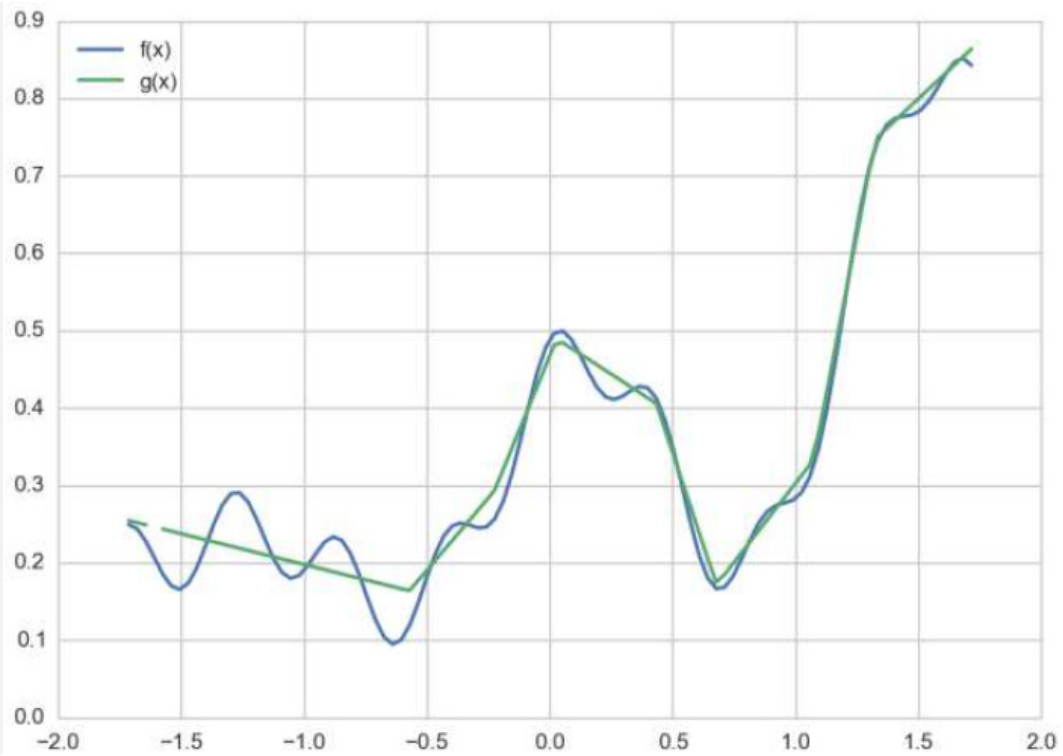
snt regiocom

Werkzeuge der Künstlichen Intelligenz

Die Stärken der einzelnen Bereiche:

Neuronale Netze

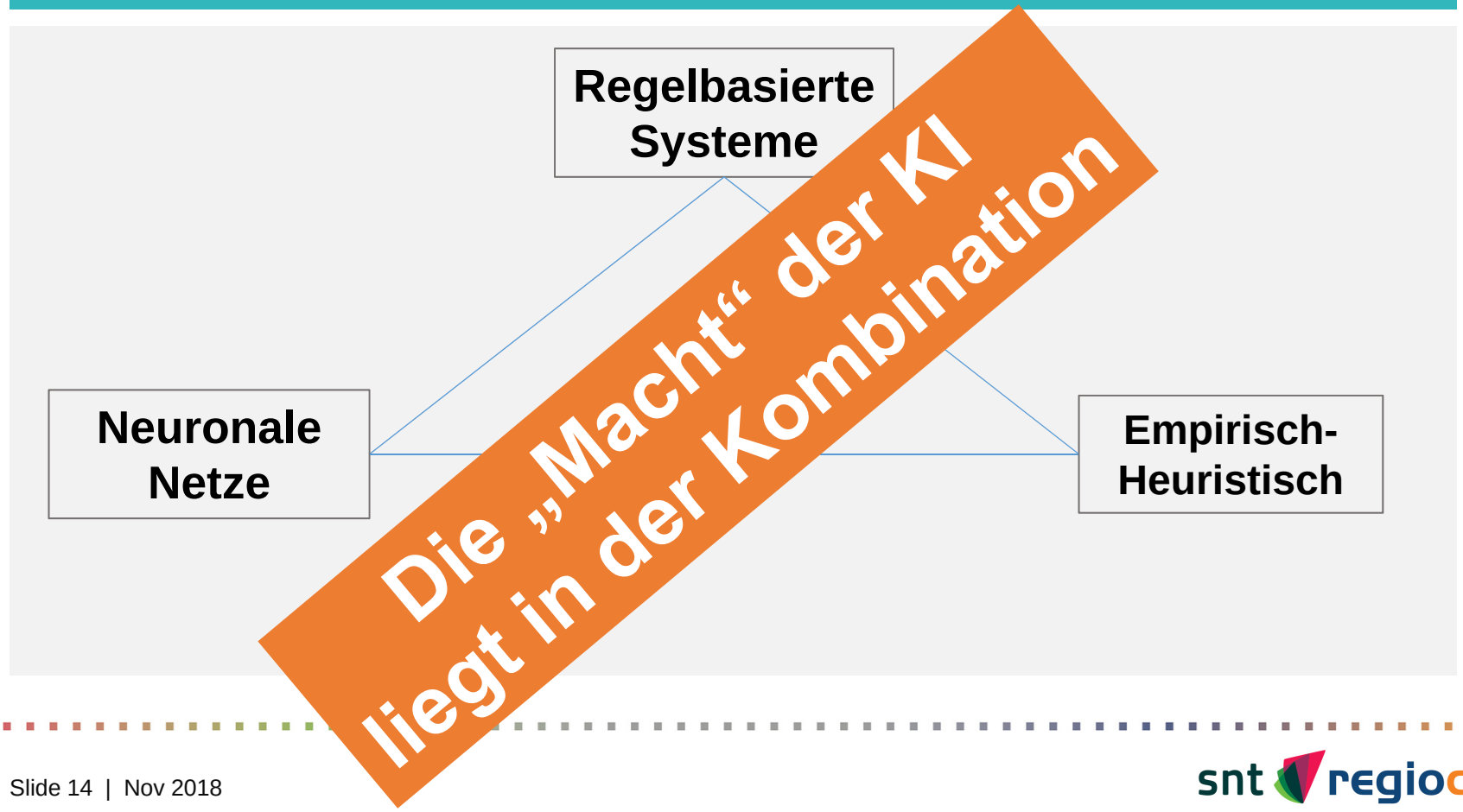
Bsp. Gesichts-erkennung



snt regiocom

Werkzeuge der Künstlichen Intelligenz

Die Stärken der einzelnen Bereiche:



snt regiocom

Was ist Datenschutz?

Verständnis(se) von Datenschutz

Unterschiedliche Schwerpunkte in unterschiedlichen Kulturkreisen,
z.B.

- Schutz vor mißbräuchlicher DV
- Informationelle Selbstbestimmung, Erlaubnisvorbehalt, Datensparsamkeit
- Schutz der Privatsphäre
- Machtungleichgewicht zwischen Einzelpersonen und Organisationen
- “Right to be alone”

Elemente des Datenschutzes

- Weltweit erstes Datenschutzgesetz in Hessen, 1971 (Bürger-Verwaltung)
- BDSG 1977, div. Novellen
  u.a. Adresshandel, Markt- und Meinungsforschung, Opt-in, Kopplungsverbot, Beschäftigten-DS, Auftragsdatenverarbeitung;
- EU-DSGVO mit hehren Zielen:
  - EU-einheitliche Regulierung
  - „Konsens der Kulturen“
  - Privacy by Design / by Default
  - Pol. Zielrichtung: US-Datenkonzerne

Was ist Datenschutz?

regiocom

Was schützt er

- Persönliche Daten
- Recht auf Anonymität bei der Nutzung einer öffentlichen Leistung
- Schützt den Bürger vor dem Staat (unberechtigte Erhebung von Daten, Verstoß gegen Datensparsamkeit, u.a.)

Was schützt er nicht

- Schützt nicht vor nicht erreichbaren Organisationen
- Schützt nur wenig im entgrenzten Datenverkehr
- Schützt nur wenig bei der KI-basierten „Sachbearbeitung“ (Tinder-Beispiel)
- **Schützt nicht vor den Folgen der massendaten-basierten Profilbildung**

snt regiocom

Machtfrage B-to-B

- Wer Massendaten hat muß nicht mehr de-anonymisieren
- Wer Massendaten hat ist in der Individualisierung von Dienstleistungen immer im Vorteil
- Es stellt sich die Machtfrage,
  - ➔ zwischen kleinen und großen Unternehmen;
  - ➔ zwischen Plattformen und Nicht-Plattformen

Machtfrage B-to-C

- KI ist ein zentraler Bestandteil sämtlicher plattformbasierter Dienste
- In einigen (auch wichtigen) Bereichen ist die Ergebnisbildung nicht mehr nachvollziehbar und deterministisch
- Privatpersonen können einer KI-Entscheidung “ausgeliefert” sein
- Die Forderung “KI-Entscheidungspfade offenlegen” steht im Raum

Auf dem Weg zu einer Antwort

- Welche KI-basierten Entscheidungen sind vital, welche nebensächlich?
- Wer auswählen kann, ist nicht ausgeliefert?
  (z.B. Baugenehmigung / Kreditzusage / TINDER)
- Gibt es Anwendungsbereiche, in denen KI mehr nutzt als schadet?
  (Radiographie / Geothermie / Strombelieferung / Versicherung)
- Wann stellt die KI ein Geschäftsgeheimnis/Technologie dar?
- Wie wäre die Offenlegung von KI machbar?
- Löst eine Regulierung die „Machtfrage“