HÄRTING

RECHTLICHE ASPEKTE KÜNSTLICHER INTELLIGENZ

RA lic. iur. Nicole Beranek Zanon Exec. MBA HSG, CIPE/E

Berner Tagung ISSS – 23. November 2021

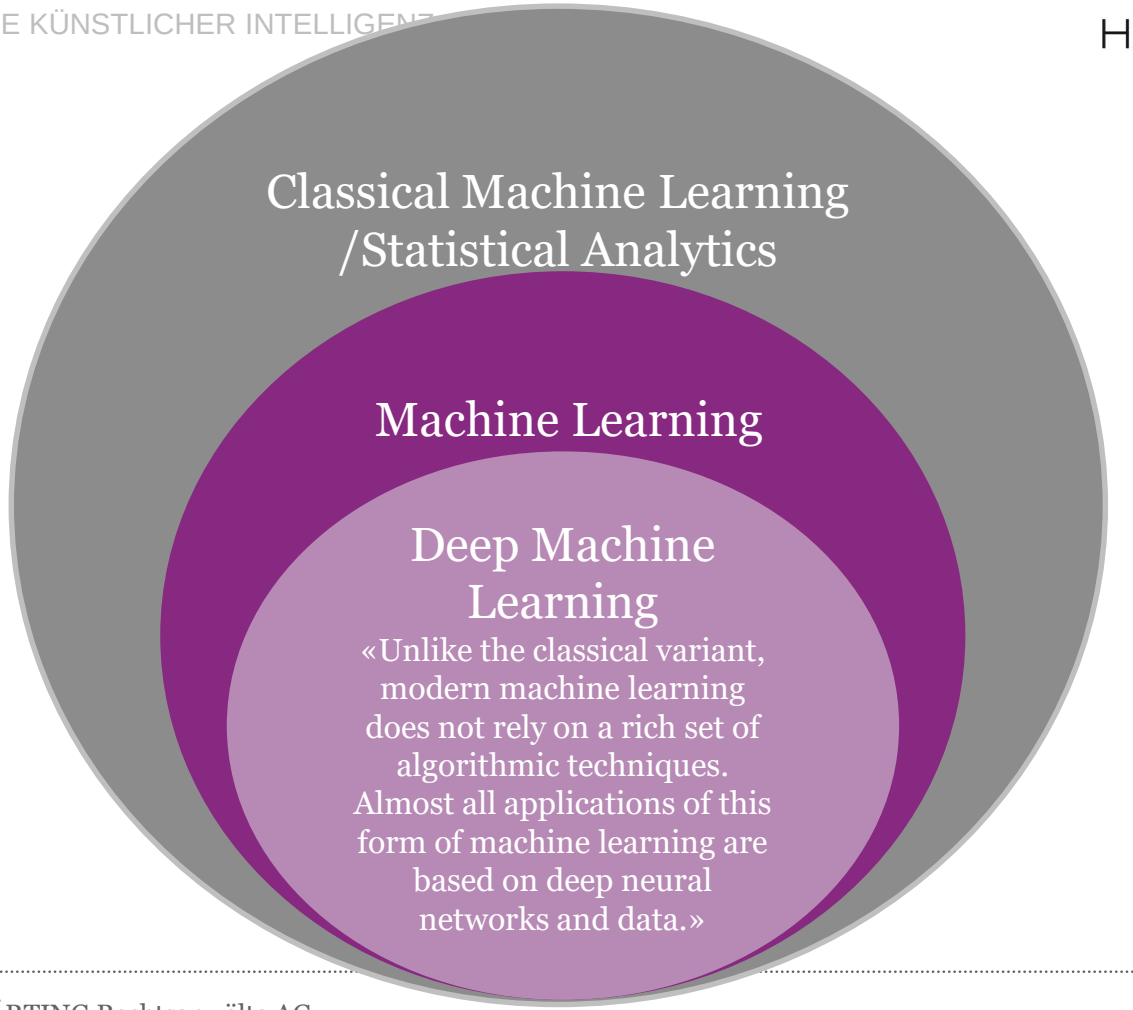
AGENDA

1. Begriffliches
2. Rechtliche Herausforderungen
3. Regulierungsbedarf für AI

1. Begriffliches

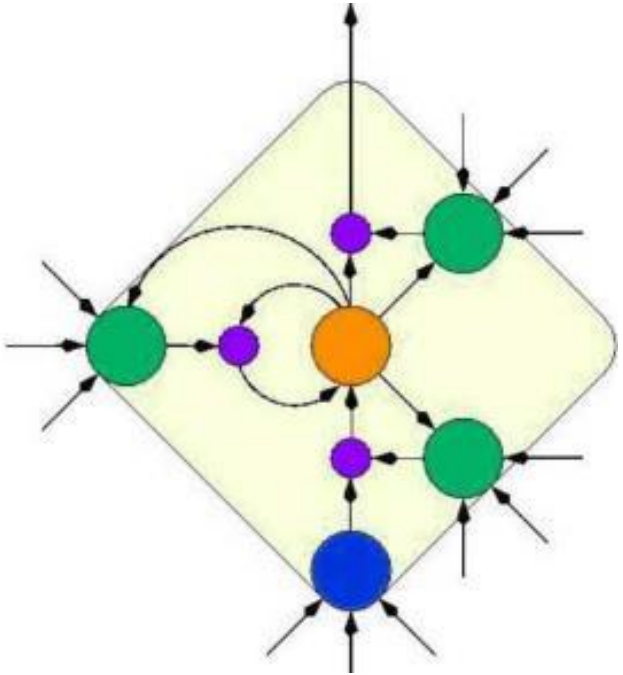
HÄRTING

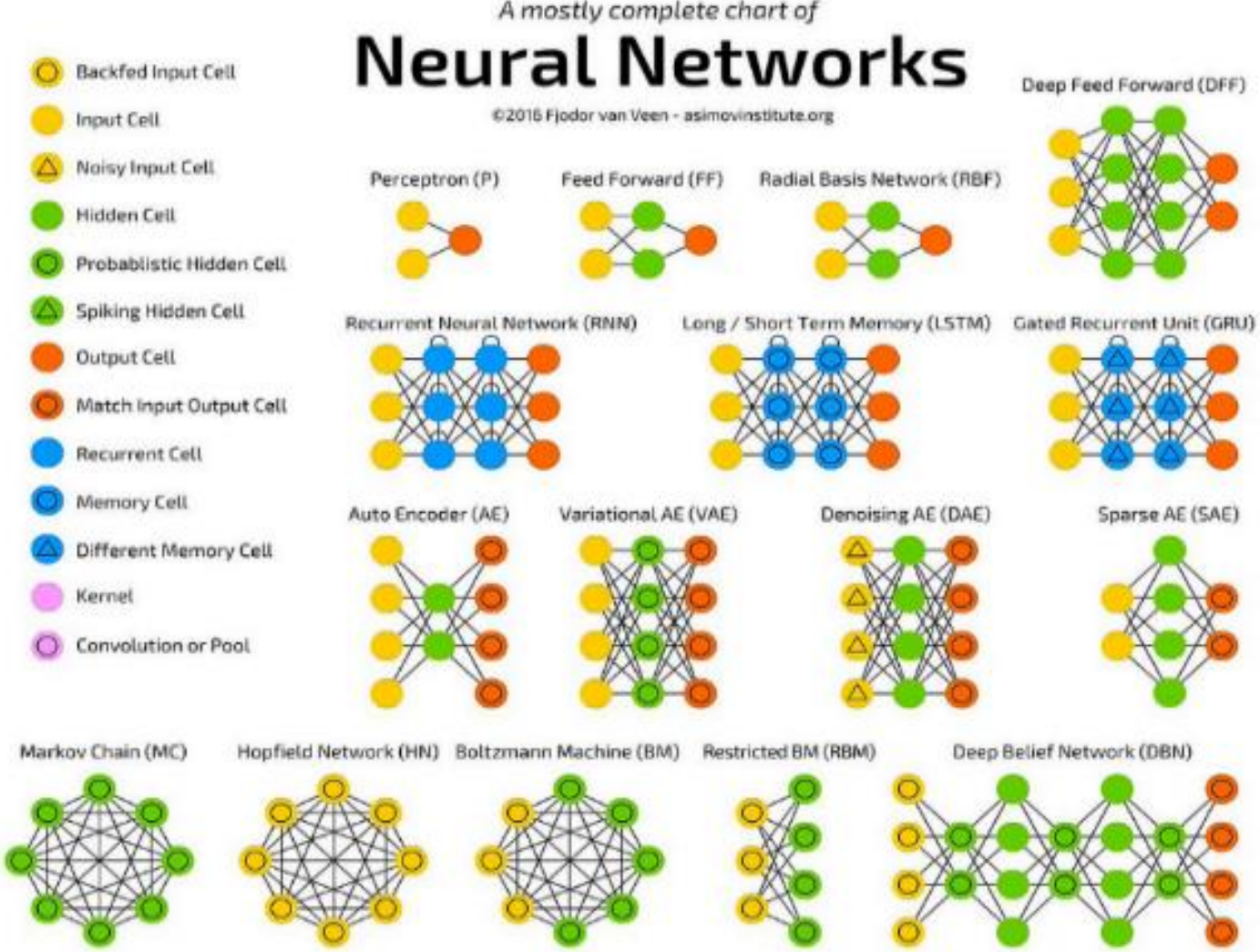
Definition



LSTM – LONG SHORT-TERM MEMORY – RECURRENT NEURAL NETWORKS

- Prof. Schmidhuber + Team
- Selbstlernende Software
- heute verwendet bei
  - *Spracherkennung z.B. von Siri, Alexa etc.*
  - *Bilderkennung*
  - *Gesichtserkennungssoftware*
- Was als nächstes?




A mostly complete chart of
Neural Networks
©2016 Fjodor van Veen - asimovinstitute.org
Backfed Input Cell
Input Cell
Noisy Input Cell
Hidden Cell
Probabilistic Hidden Cell
Spiking Hidden Cell
Output Cell
Match Input Output Cell
Recurrent Cell
Memory Cell
Different Memory Cell
Kernel
Convolution or Pool
Perceptron (P)
Feed Forward (FF)
Radial Basis Network (RBF)
Deep Feed Forward (DFF)
Recurrent Neural Network (RNN)
Long / Short Term Memory (LSTM)
Gated Recurrent Unit (GRU)
Auto Encoder (AE)
Variational AE (VAE)
Denoising AE (DAE)
Sparse AE (SAE)
Markov Chain (MC)
Hopfield Network (HN)
Boltzmann Machine (BM)
Restricted BM (RBM)
Deep Belief Network (DBN)

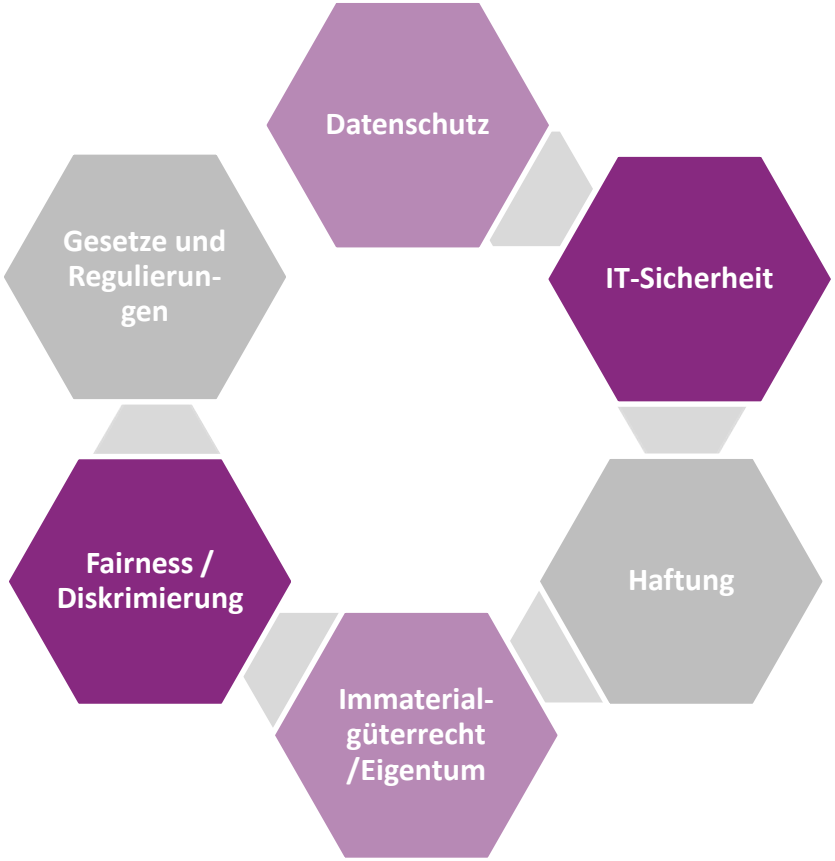
HÄRTING

ANWENDUNGSBEISPIELE

2. Rechtliche Herausforderungen

HÄRTING

RECHTLICHE THEMEN



DATENSCHUTZ - PERSONENBEZOGENE DATEN

- Personendaten vs. Sachdaten
- Alles was keinen Personenbezug hat und keine Identifizierung zulässt sind Sachdaten
- Personenbezug
- Identifizierung / Bestimmbarkeit
- Kontext
- Anonymisierung / Pseudonymisierung
- Betroffenenrechte

DATENSCHUTZ - DREI DATENSÄTZE GENÜGEN

The New York Times

Technology

A Face Is Exposed for AOL Searcher No. 4417749

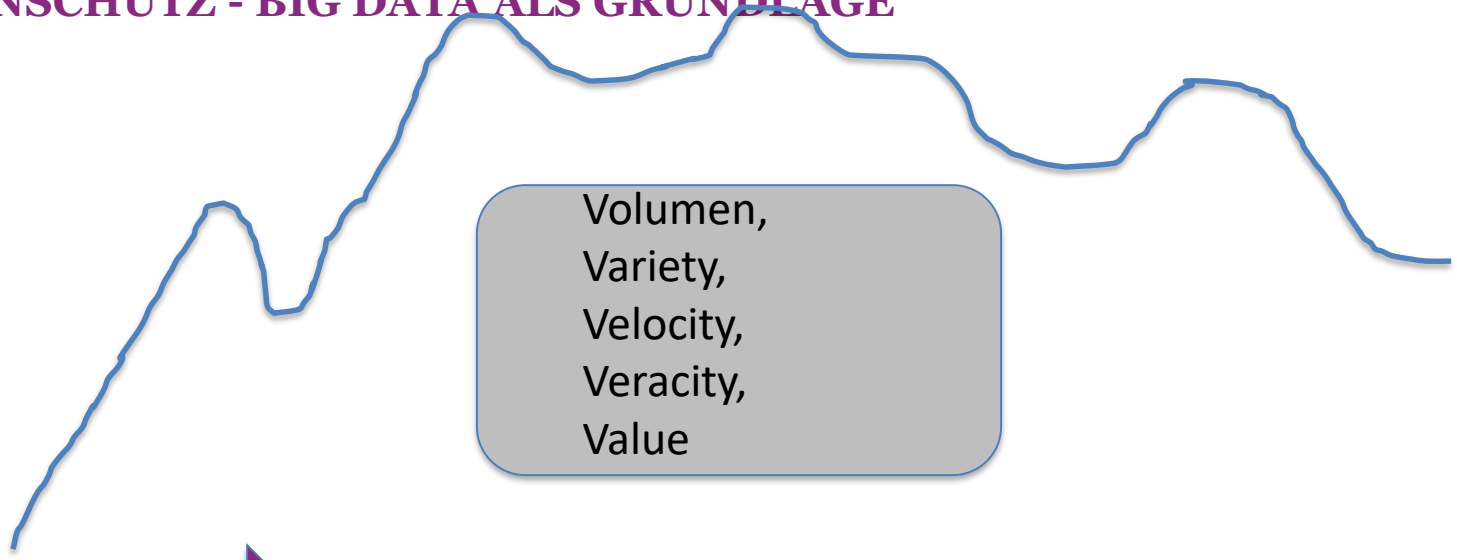
By MICHAEL BARBARO and TOM ZELLER Jr.
Published: August 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for "landscapers in Lilburn, Ga," several people with the last name Arnold and "homes sold in shadow lake subdivision gwinnett county georgia."

DATENSCHUTZ - BIG DATA ALS GRUNDLAGE



Prima vista diametral zum Datenschutz

HÄRTING

MLAAS - MACHINE LEARNING AS A SERVICE

- Als Dienst aus der Cloud
- Datenbearbeitung durch Dritte Art. 10a DSG
  - *Nur so, wie Auftraggeber*
  - *Keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet*
  - ***Einhaltung der Datensicherheit***
    - Datenschutzfolgenabschätzung (Risikoabwägung)
    - Transfer Impact Assesement
- Datentransfer ins Ausland Art. 6 DSG
  - *Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet*
  - *Angemessener Schutz Art. 6 Abs. 2 DSG*

DATENSCHUTZ – ANGEMESSENER SCHUTZ ART. 6 ABS. 2 DSG

- hinreichende Garantien, insbesondere durch Vertrag (SCC) + zusätzliche Massnahmen betr. Gewährleistung der Grundrechte (insbesondere Verfahrensrechte)
- Einwilligung
- In unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags
- Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
- Erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen;
- Öffentlich zugänglich ohne Verbot
- BCR

HÄRTING

DATENSCHUTZ – LÖSUNGSANSÄTZE

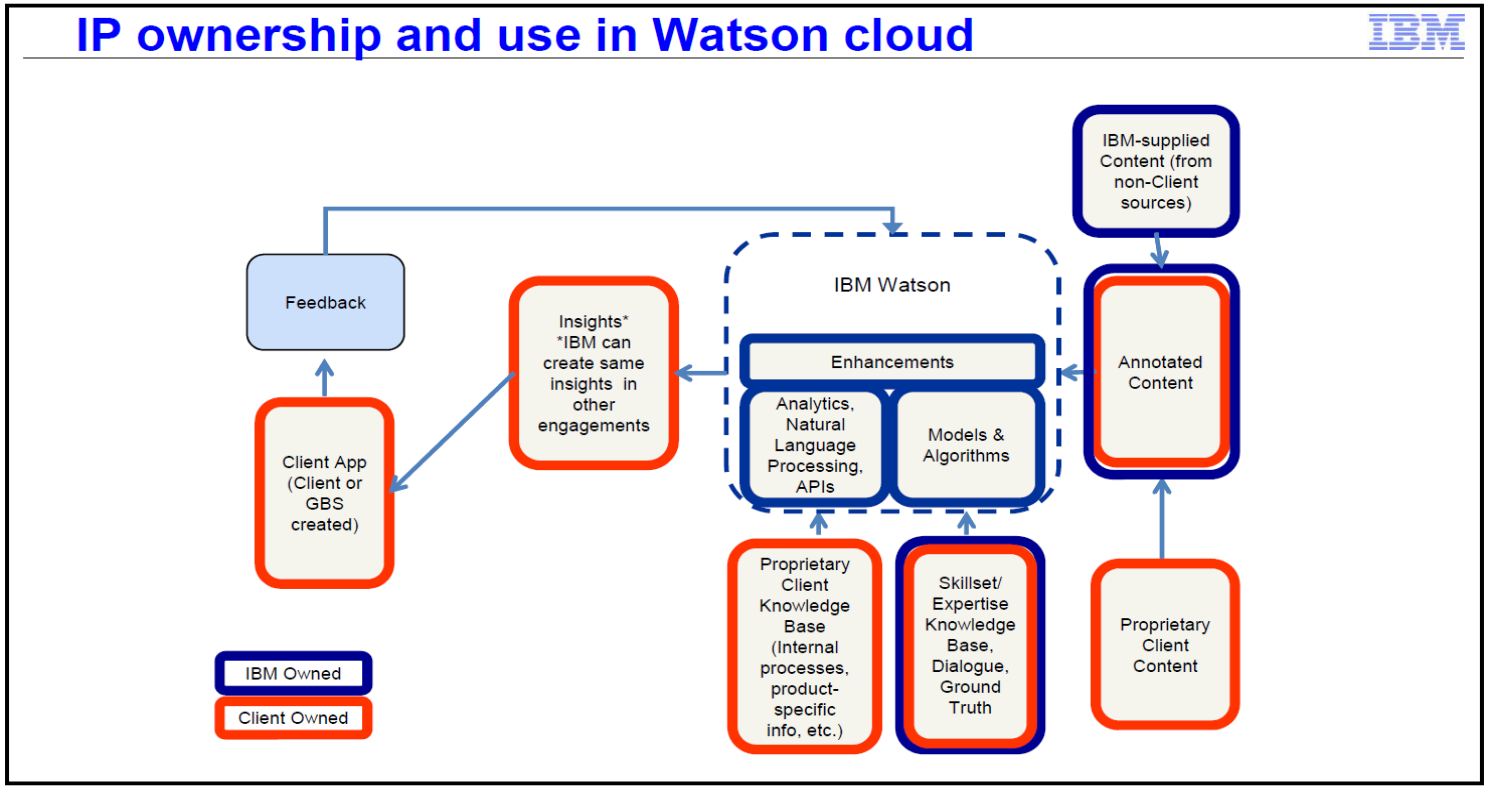
- «Select before you collect»
- Anonymisierte Daten
- Synthetische Daten
- dumb-in / clever-out
- 2-Phasen-Verarbeitung
- Getrennte Aufbewahrung der Schlüssel oder sofortige Zerstörung derselben
- Hashing/Re-Hashing
- Eliminierung von ausserordentlichen Werten
- Clustering
- Reduzierung des Datengehaltes (weniger Überschneidungen)

HÄRTING

Geistiges Eigentum

- Wem gehört die KI?
- Code / Algorithmus ist keine Sache
- Urheberrecht (URG)
  - «Als Werke gelten auch Computerprogramme.» Art. 2 Abs. 3 URG
  - «geistige Schöpfung mit individuellem Charakter» Art. 2 Abs. 1 URG
  - «Urheber oder Urheberin ist die natürliche Person, die das Werk geschaffen hat.» Art. 6 URG

IMMATERIALGÜTERRECHTE



Quelle: Präsentation Dr. Alesch Staehelin, Lead Counsel Research Europe, IBM, Zurich, Europainstitut an der Universität Zürich / ICT – Recht und Praxis, 26. September 2017

HÄRTING

HAFTUNG

- Zivilrechtliche Haftung (OR 41, OR 97, SVG 58, PrHG 1)
- Verschuldenshaftung / Kausalhaftung
- Haftung des Herstellers oder des Betreibers/Halters?
- KI, die erst beim Kunden entwickelt wird

HÄRTING

Etische Überlegugnen – Meinungsfreiheit und Diskriminierung

- Manipulation hat demokratische Auswirkung
- Beispiele:
  - *Cambridge Analytica*
  - *Target Marketing*
  - *Social-Media Bots*
  - *Beeinflussung von Wahlen*
  - *Bias*
  - *Wer soll leben (autonomes Fahren)? «ein autonomes Auto sollte bei einem Unfall im Zweifel immer die Insassen schützen» (Christoph Hugo, Daimler*
- Massnahmen:
  - *Beschränkungen*
  - *Transparenz*

3. Regulierungsbedarf für AI?

EU Kommission - AI Ethics Guidelins 2020

- European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG) hat am im 2019 **AI Ethics Guidelines** vorgestellt:
  - Human agency and oversight
  - Robustness and safety
  - Privacy and data governance
  - Transparency
  - Diversity, non-discrimination, and fairness
  - Societal and environmental well-being
  - Accountability

HÄRTING

EU Vorschlag für eine VERORNDUNG zur KI

- Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION COM/2021/206 final
- EU als proaktive Akteurin in digitalpolitischen Themen
- Druck auf andere Staaten KI-Systeme zu regulieren

AI GESETZESFAMILIE

- DSGVO – Erw. 71, 75 & 85:

  Persönliche Daten sollen so verarbeitet werden, dass keine diskriminierenden Effekte entstehen so z.B. bei automatisierten Einzelfallentscheiden, welche die Rechtsposition von betroffenen Personen beeinflussen.

- AI Act – Erw. 17, 28, 33, 35-39:

  Weil bestimmte KI-Systeme diskriminierende Effekte haben können, sind sie verboten oder sollen nur unter Auflagen betrieben werden.

Vorschlag AI-Verordnung

- **Titel I:** (Extraterritorialer) Anwendungsbereich + Definitionen
- ANHANG I TECHNIKEN UND KONZEPTE DER KÜNSTLICHEN INTELLIZENZ gemäß Artikel 3 Absatz 1

  a) *Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (**Deep Learning**);*

  b) *Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme; **(=ML?)***

  c) *Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden. **(=klassische KI?)***
- **Titel II:** Liste von verbotenen Praktiken, gemäss risikobasiertem Ansatz
- **Titel III:** Regelung von Hochrisiko KI-Systeme
  - Hohes Risiko für Sicherheit, Gesundheit und Grundrechte
  - Vorgängige Komformitätsbewertung

HÄRTING

Vorschlag AI-Verordnung

- **Titel IV:** Regelung spezifischer Manipulationsrisiken
  - *Transparenzpflichten bei KI-Systeme die:*
    - mit Menschen interagieren
    - Emotionen erkennen
    - zur Assoziierung (gesellschaftlicher) Kategorien anhand biometrischer Daten eingesetzt werden
    - **Inhalte erzeugen bzw. manipulieren («Deep fake»)**
- **Titel V:** Massnahmen zur Innovationsförderung
- **Titel VI-VIII:** Leitung und Durchführung
- **Titel IX:** Verhaltenskodizes
- **Titel X-XII**: Schlussbestimmungen

ZULÄSSIGKEIT DER KI NACH RISIKO

HÄRTING

Internationaler Ansatz

- Neues Regelungswerk für KI
- Grundprinzipien mit Umgang von KI
- Risikobasierter Ansatz
- Horizontale Regeln
- Staat und Private unterstehen gleichen Regelungen

Schweizer Ansatz

- Bestehendes Recht neu interpretieren, evt. weitere Ansätze
- Technologieneutral
- Sektorenspezifische Regeln
- Unterscheidung zwischen Staat und Privaten

ÜBER AMNESTY

SCHWEIZ

GRUNDRECHTE SCHÜTZEN – GESICHTSERKENNUNG STOPPEN!

Medienmitteilung 18. November 2021, London/Bern – Medienkontakt

Der Einsatz von Gesichtserkennungssystemen breitet sich in Europa rasant aus. Gesetzliche Schranken gegen die Überwachung mittels Gesichtserkennung fehlen. Ein Bündnis aus Amnesty International, AlgorithmWatch CH und der Digitalen Gesellschaft fordert ein Verbot von automatischer Gesichtserkennung und biometrischer Massenüberwachung in der Schweiz. Gemeinsam lancieren die Organisationen eine Petition für ein solches Verbot.

NEWS

Petition von Amnesty International

Darum wollen Datenschützer die Gesichtserkennung im öffentlichen Raum stoppen

Mo 22.11.2021 - 11:45 Uhr
von Oliver Wietlisbach / Watson.ch, san

Der Einsatz von Gesichtserkennungssoftware im öffentlichen Raum ist weltweit auf dem Vormarsch. Datenschützer und Datenschützerinnen sowie Politiker und Politikerinnen wollen nun die biometrische Überwachung in der Schweiz verbieten.

HÄRTING

Ausblick Schweiz

- Schweiz hat sich bislang weitgehend passiv verhalten, aber immerhin:
  - Bericht im Dezember 2019 der interdepartementalen Arbeitsgruppe des Bundes
  - Leitlinien für den Umgang mit KI in der Bundesverwaltung im November 2020 des Bundesrat
  - Einzelne Kantone haben sich bereits mit dem Einsatz von KI in der Verwaltung befasst (z.B. ZH)
  - Schweiz an einer Arbeitsgruppe des Europarates, dem «Ad hoc Committee on Artificial Intelligence (CAHAI)», beteiligt

HÄRTING

Ausblick Schweiz

- Grössere Unternehmen werden aus Einfachheit und Effizient auch für die Schweiz das EU-Recht anwenden
- EU-Recht kann nicht einfach vorbehaltlos übernommen werden, da dieses auf anderen Werten basiert
- Grundsätzlicher Regulierungsbedarf in der Schweiz auch vorhanden

HÄRTING

TEAM

Nicole Beranek Zanon

Partnerin | Notarin | Exec. MBA HSG

Olivia Boccali

Juristin

Alessio Frongillo

Jurist

Roman Rey

Rechtsanwalt | Musiker

HÄRTING Rechtsanwälte AG

Landis + Gyr-Strasse 1
6300 Zug
Switzerland
Tel. +41 41 710 28 50
www. haerting.ch
beranek@haerting.ch