MATERNA
Information & Communications

INFORA

Gemeinsam gestalten!

25. März 2021

Künstliche Intelligenz als (datenschutz)rechtliche Herausforderung

Begrüßung und kurze technische Hinweise

Bernadette Seiler

Materna Information & Communications SE

Künstliche Intelligenz als (datenschutz)rechtliche Herausforderung

Andreas Werner

Infora GmbH

Merkmale von KI-Systemen und rechtliche Implikationen

KI Definition

- Verständnis von künstlicher Intelligenz (KI) und Machine Learning (ML) reicht von regelbasierten Entscheidungs-modellen auf Grundlage gut erforschter Regressionsanalysen bis zu subsym-bolischen Strukturen künstlicher neuronaler Netze (KNN).

KI Definition

Lernstil	Lernaufgabe	Lernverfahren	Modell
Überwacht	Regression	Lineare Regression	Regressionsgerade
		Klassifikations- und Regressionsbaum-verfahren (CART)	Regressionsbaum
	Klassifikation	Logistische Regression	Trennlinie
		Iterative Dichotomizer (ID3)	Entscheidungsbaum
		Stützvektormaschine (SVM)	Hyperebene
		Bayessche Inferenz	Bayessche Modelle
Unüberwacht	Clustering	K-Means	Clustermittelpunkte
	Dimensionsreduktion	Kernel Principal Component Analysis (PCA)	Zusammengesetzte Merkmale
Bestärkend	Sequentielles Entscheiden	Q-Lernen	Strategien
Verschiedene	Verschiedene	Rückwärtspropagierung	Künstliche Neuronale Netze

Aus Fraunhofer (Hrsg): Maschinelles Lernen, S. 10

KI Definition

Soweit im Folgenden von Künstlicher (KI) gesprochen wird, ist deren aktuell stärkste Ausprägung gemeint, nämlich KNN mit Deep Learning.

Deep-Learning-Systeme sind also nicht prüfbar, nicht evaluierbar, ändern Ihre Eigenschafen, liefern keinerlei Begründung, sind leicht zu manipulieren, willkürlich aufgebaut und immer ungenau.*

Die (datenschutz)rechtlichen Herausforderungen dabei sind sehr beachtlich.

* Günter Laßmann; Asimovs Robotergesetze – Was leisten sie wirklich?; E-Book; Heise Medien 2017, Pos 1299

KI und Recht

z. B.:

- Produkthaftung / Deliktische Haftung
- Vertragsrecht
- Urheberrecht
- Immaterialrechtlicher Schutz der KI
- Datenschutzrecht
- Verbraucherschutzrecht
- Arbeitsrecht
- Strafrecht

Hat KI eine eigene Rechtspersönlichkeit?

KI + Verwaltungshandeln

KI und Recht

Autonomieschutz → Einzelner darf nicht Objekt maschineller Entscheidung werden

Einzelfallorientierung → Untersuchungsgrundsatz muss erhalten bleiben

§ 24 (3) S. 3 VwVfG / § 31a S. 2 SGB X

Transparenz- / Begründungsgebote

Diskriminierungsverbote

Siehe dazu ausführlich: Wischmeyer: Regierungs- und Verwaltungshandeln durch KI in Ebers /Heinze / Krügel / Steinrötter: Künstliche Intelligenz und Robotik; 2020, § 20 R. 41 ff.

Automati-sierung vs. KI

§ 35a VwVfG / § 31a SGB X beschreiben zunächst Verwaltungsautomatisierung NICHT aber KI in Verwaltung.

Komplexe interpretatorische + Abwägungsfragen lassen KI-Einsatz problematisch erscheinen

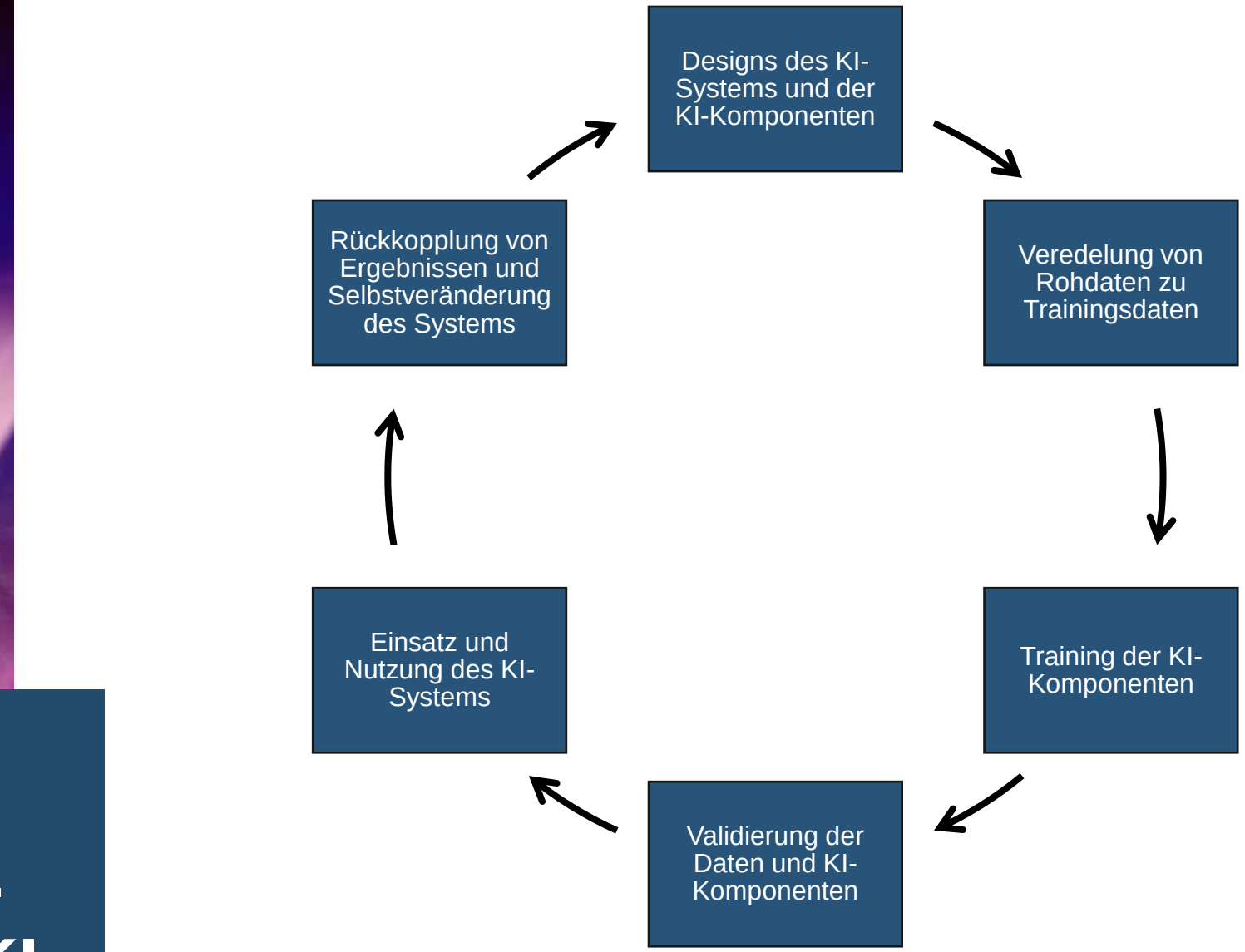
Beispiel AO

StModernG hat durch § 155 (4) AO mit Risikomanagementsystem § 88 (5) AO eine gesetzliche Grundlage geschaffen, Steuerfestsetzungen ausschließlich automationsgestützt vorzunehmen.*

Ausführlich dazu: Rüsken in Klein: Abgabenordnung, 15. Aufl., § 155 ab Rn. 50

Datenschutz und KI

Daten-schutz-Lebens-zyklus KI



gemäß DSK-Positionspapier KI-TOM

Pflichten Beteiligte und Verant-wortliche

Beteiligte

- Verantwortlichkeit ermitteln
- Verantwortlichkeit Kommunizieren
- Notwendigen Maßnahmen für
  - rechtmäßige Verarbeitung
  - Betroffenenrechte
  - Sicherheit der Verarbeitung
  - Beherrschbarkeit des KI-Systems

Verantwortliche

- Datenschutzrechtlichen Grundsätze (Art. 5 DSGVO) einhalten
- Sicherheit der Verarbeitung (Art. 32 DSGVO) gewährleisten
- Auch schwer erkennbare und vorhersehbare Risiken erkennen und Maßnahmen
  - definieren
  - implementieren
  - betreiben
- Dokumentation nachhalten

Span-nungs-verhältnis DSGVO und KI

Grundpflichten DSGVO	Realität KI
Zweckbindungsgrundsatz, d. h. Verarbeitung muss für festgelegte, eindeutige und legitime Zwecke erfolgen (Art. 5 Abs. 1 lit. b DSGVO)	Bei unüberwachten oder nicht-deterministischen Lernvorgängen können daran Zweifel aufkommen. Es gibt hier zwar für den Gesamtvorgang sehr wohl einen bestimmten Zweck, nur das konkrete Mittel muss mit Hilfe der KI erst noch gefunden werden.
Transparenz (Art. 5 Abs. 1 lit. a DSGVO)	Bei Deep Learning, aber auch bei IoT-vernetzten Prozessen oft problematisch.
Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)	z. T. Zielkonflikt, da die Entwicklung einer KI abhängig von der Menge und der Güte der Daten ist, die man ihr gibt.

Beispiel Trans-parenz

DSGVO	KI
Art. 5 Transparenz	
Art. 12 ff Entscheidungen auf Grundlage des Einsatzes von KI-Systemen müssen nachvollziehbar und erklärbar sein. Das betrifft nach Auffassung der Aufsichtsbehörden nicht nur die Erklärbarkeit des Ergebnisses, sondern auch die Nachvollziehbarkeit im Hinblick auf die Prozesse, die Logik und das Zustandekommen von Entscheidungen (DSK – Hambacher Erklärung, S. 3).	Bei den datenschutzrechtlichen Informationsrechten besteht der Grundsatz, dass die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums, nicht beeinträchtigt werden dürfen.

SCHUFA-Entscheidung

Als Faustformel wird man auch bei der Transparenz auf die Abwägung zurückkommen, die der BGH (BGH, Urt. v. 28.01.2014, VI ZR 156/13) auf Grundlage von § 34 BDSG alt angestellt hatte: Anzugeben sind die eingeflossenen Daten und eine grobe Erläuterung, was mit ihnen gemacht wird. Rechengrößen und deren Gewichtung sind dagegen in der Regel nicht zu erläutern.

TOM

TOM: Für den datenschutzkonformen Einsatz von KI-Systemen gab es bislang keine speziellen Standards oder detaillierte Anforderungen an die anzuwendenden technischen und organisatorischen Maßnahmen.

Positionspapier DSK KI: In der Anlage zum Positionspapier stellen die Aufsichtsbehörden eine tabellarische Übersicht über rund 70 technische und organisatorische Maßnahmen für KI-Komponenten und KI-Systeme vor und ordnen diese bestimmten Phasen im Lebenszyklus eines KI-Systems und den jeweiligen Gewährleistungszielen zu.

DSFA

Kriterien nach WP 248

1. Bewerten oder Einstufen
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche Daten oder höchstpersönliche Daten
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert

DSFA

KI einfaches maschinelles Lernen

1. Bewerten oder Einstufen
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche Daten oder höchstpersönliche Daten
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert

Handlungshilfen

Audit-empfeh-lung der AEPD

aepd agencia española protección datos

Audit Requirements for Personal Data Processing Activities involving AI

Positions-papier der DSK

Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 06.11.2019

Stand: 06.11.2019

Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen

Vielen Dank für Ihre Aufmerksamkeit

Unser nächster Webcast aus der Reihe IT Compliance:

Schwachstellenmanagement am 29.04.2021
Alle aktuellen Informationen:
https://www.infora.de/webcast-reihe/

Infora GmbH
Standort Berlin
Friedrichstraße 200
(Aufgang B, 6.OG)
10117 Berlin

Telefon: 030 893658-0
Internet:
http://www.infora.de
E-Mail: info@infora.de