

Strategien und Techniken zur Regulierung Künstlicher Intelligenz

Impulsreferat im Rahmen des Deutschen EDV-Gerichtstags am 15. Dezember 2023

Professor Dr. Rolf Schwartzmann

Prof. Dr. Rolf Schwartmann



- Leiter Kölner Forschungsstelle Medienrecht, Technische Hochschule Köln
- Vorsitzender der GDD e.V., Bonn
- Mitglied der Plattform 5 des Digitalgipfels der Bundesregierung
- Mitglied der Datenethikkommission der Bundesregierung
- Sachverständiger des Deutschen Hochschulverbandes für IT- und Datenrecht

Kölner Forschungsstelle
für Medienrecht

Technology
Arts Sciences
TH Köln

Funktionsweise von Foundation Models (GPAI)

Früher: "Diskriminative" Modelle

Heute: "Generative" Modelle

kontextbezogenes Lernen der Wahrscheinlichkeit von Wortfolgen

Wenn

Textbaustein A



Dann

Textbaustein B

Bremse

80 %

Fahrzeugteil

20 %

Insekt

Bremse

(im Kontext Kfz)

99 %

Fahrzeugteil

1 %

Insekt

„Generierung“ neuer Datensätze

Er war in einen Unfall verwickelt. Grund war die defekte Bremse.

99,99 %

Er konnte das Auto nicht stoppen.

0,01 %

Sie ist ihm ins Gesicht geflogen.

Risiken des Einsatzes von Foundation Models

- **Unsinnige Ergebnisse**
Generierung von Datensätzen, die keinen Sinn ergeben
- **Halluzinationen**
Generierung von Datensätzen, die faktisch falsche Informationen enthalten
- **Rechtswidrige Ergebnisse**
Generierung von Datensätzen, die im Einzelfall die Rechte Dritter verletzen können
- **Reproduktion häufig geäußerter Meinungen**
Generierung von diskriminierenden Datensätzen

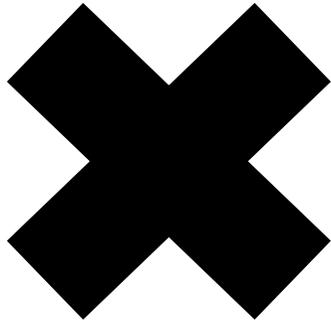


kognitive Verzerrungen, z.B.

- Automatisierungsbias
- Ankereffekt
- Default-Effekt

unreflektierte Übernahme der Ergebnisse

Keine Regulierung



**keine Regulierung des
Basismodells**

Der Hersteller eines Hammers ist nicht verantwortlich, wenn der Hammer als Mordwaffe eingesetzt wird.

Eine Regulierung von Basismodellen passt nicht zur anwendungsbezogenen Regulierung der KI-Verordnung.

Es ist unmöglich, Foundation Models so zu trainieren, dass Rechtsverletzungen ausgeschlossen sind.



**Verantwortung
beim Nutzer**

Verpflichtende Selbstregulierung



Gesetzliche Regulierung



gesetzliche Mindestanforderungen,
die Anbieter von Foundation Models
erfüllen müssen

Nur durch eine sachgerechte Zuweisung
von Verantwortlichkeiten entlang der
gesamten KI-Wertschöpfungskette
können die Grundrechte der
Betroffenen geschützt werden.

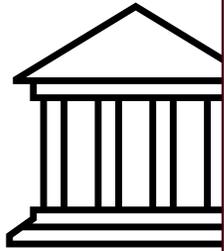


Nur durch eine ausformulierte
Regulierung kann Rechtsunsicherheit
vermieden werden.



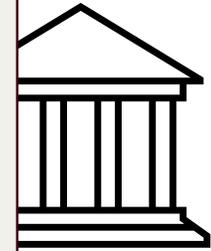
Sanktionierung von
Verstößen

Verpflichtende Selbstregulierung unter Beteiligung des Parlaments



gesetzliche Vor-
von Leitplanke
die Regulierung

Das beschriebene Vorgehen hat den Vorteil, dass das Europäische Parlament die Grundentscheidungen zur Regulierung von Foundation Models trifft, während Spezifikationen durch die Modellanbieter im Austausch mit der Kommission und unter Berücksichtigung technologischen Fortschritts vorgenommen werden können. Der Regelungstechnik liegt insofern der Grundgedanke der aus der DS-GVO bekannten delegierten Rechtsakte zugrunde, wobei das Initiativrecht zur Erarbeitung delegierter Rechtsakte nach dem vorliegenden Vorschlag nicht bei der Kommission, sondern im Sinne einer Regulierung beim Parlament und im Sinne einer Selbstregulierung bei den Modellanbietern liegt.



Genehmigung der
Spezifikationen
durch die
Kommission

Die Regulierung von GPAI-Modellen nach der politischen Einigung zur KI-Verordnung



hierzu eingehend: DataAgenda Datenschutz Podcast, Folge 48 ab Minute 13:00