fieldfisher

Die EU-KI-Verordnung

14. Oktober 2021

Stephan Zimprich

Der Begriff „KI-System“

- **Konzepte des maschinellen Lernens**, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning)
- **Logik- und wissensgestützte Konzepte**, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme
- Statistische Ansätze, Bayessche Schätz-, **Such- und Optimierungsmethoden**.

Regulierungskonzept

Verbotene KI

Hochrisiko-KI

Umfangreiche Pflichten für Anbieter, Einführer und Nutzer!

Bestimmte KI

Transparenzpflichten

Regulierungskonzept

Verbotene KI

- Techniken der unbewussten **unterschwelligen Beeinflussung** in Schädigungsabsicht
- KI-Systeme, die **Schwächen einer Gruppe von Personen** (Alter, körperliche oder geistige Behinderung) in Schädigungsabsicht ausnutzen
- **Social Scoring**
- **Echtzeit-Biometrie** zu Strafverfolgungszwecken (Ausnahmen u.a. Opfersuche, Vermisstensuche, Gefahrenabwehr, Terrorabwehr)

Hochrisiko-KI

- **kritische Infrastrukturen** (z. B. im Verkehr), in denen das Leben und die Gesundheit der Bürger gefährdet werden könnten;
- **Schul- oder Berufsausbildung** , wenn der Zugang einer Person zur Bildung und zum Berufsleben beeinträchtigt werden könnte (z. B. Bewertung von Prüfungen);
- **Sicherheitskomponenten von Produkten** (z. B. eine KI-Anwendung für die roboterassistierte Chirurgie);
- **Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit** (z. B. Software zur Auswertung von Lebensläufen für Einstellungsverfahren);
- **wichtige private und öffentliche Dienstleistungen** (z. B. Bewertung der Kreditwürdigkeit, wodurch Bürgern die Möglichkeit verwehrt wird, ein Darlehen zu erhalten);
- **Strafverfolgung** , die in die Grundrechte der Menschen eingreifen könnte (z. B. Bewertung der Verlässlichkeit von Beweismitteln);
- **Migration, Asyl und Grenzkontrolle** (z. B. Überprüfung der Echtheit von Reisedokumenten);
- **Rechtspflege** und **demokratische Prozesse** (z. B. Anwendung der Rechtsvorschriften auf konkrete Sachverhalte).

Bestimmte KI

- Für **Interaktion** mit natürlichen Personen bestimmt
- **Emotionserkennung**
- Visuelle und akustische Manipulation („**deep fake**“)

Anbieter

- **Risikomanagementsystem**
- **Daten-Governance** (konzeptionelle Entscheidungen, Datenerfassung und -aufbereitung, Annahmen; Eignungsbewertung, Bias-Bewertung, Gap-Analyse)
- Daten müssen **relevant, repräsentativ, fehlerfrei** und **vollständig** sein
- **Technische Dokumentation** (Nachweisfunktion)
- **Aufzeichnungspflicht:** Protokollierung nach anerkannten Normen und Spezifikationen
- **Transparenzpflichten** u.a. Merkmale, Leistungsgrenzen, Risiken, Informationen über verwendete Trainings- oder Testdaten
- **Menschliche Aufsicht** muss u.a. „vollständiges Verständnis und ordnungsgemäße Überwachung“ ermöglichen
- **Konzeptionelle Anforderungen** – angemessenes Maß an Robustheit, Genauigkeit, Cybersicherheit; Widerstandsfähigkeit gegenüber Fehlern, Störungen, Unstimmigkeiten, Hacking etc.
- **Qualitätsmanagementsystem**
- Durchführung des **Konformitätsbewertungsverfahrens** und Erstellen der Konformitätserklärung
- **CE-Kennzeichnung**
- Bei Nicht-EU-Anbietern: **Ernennung EU-Vertreter**

Einführer und Nutzer

Einführer

- Stellen sicher, dass Anbieter **Konformitätsbewertungsverfahrens** durchgeführt hat
- Stellen sicher, dass Anbieter **Technische Dokumentation** erstellt hat
- Stellen sicher, dass System mit der erforderlichen **Konformitätskennzeichnung** versehen ist und ihm die erforderlichen Unterlagen und Gebrauchsanweisungen beigefügt sind.
- **Kooperationspflicht mit Behörde**
- **Prüfpflicht?**

Nutzer

- **Verwenden** ein System nur entsprechend der Gebrauchsanweisung
- Stellen sicher, dass Eingabedaten der **Zweckbestimmung entsprechen**
- **Überwachen** den Betrieb (entsprechend der Gebrauchsanweisung)
- **Bewahren** automatisch erzeugte Protokolle auf

Nutzer unterliegen den Anbieterpflichten, wenn sie

- Ein System unter **ihrem Namen oder ihrer Marke** in den Verkehr oder in Betrieb nehmen
- Zweckbestimmung eines bereits im Markt befindlichen Systems **verändern**
- Sie eine **wesentliche Änderung** an einem KI-System vornehmen

Diskussion

„Anlage III“

- EU-Kommission wird ermächtigt, Liste der Hochrisiko-Systeme per „**delegiertem Rechtsakt**“ zu ergänzen
  - Voraussetzung: **Vergleichbare Risiken** wie initiale Listenelemente
  - **Risiko,** dass Entscheidungen ohne ausreichende Rückkopplung mit Mitgliedsstaaten und Parlamenten getroffen werden
- Mangelnde **Abgrenzung/Bestimmtheit** der Definitionen

Offen Fragen

- Extrem **weitreichende Dokumentationspflichten**
  - Belastung für Anbieter?
- **Hohe Hürden** für White Label-Vertrieb
- AI-Nutzung innerhalb **globaler Konzerngesellschaften**?
- **Unklares Verhältnis** zur DSGVO

Kontakt

Stephan Zimprich
Partner

Fieldfisher
Am Sandtorkai 68
20457 Hamburg

+49 (0) 40 87 88 69 8 119
stephan.zimprich@fieldfisher.com
www.fieldfisher.com

Stephan Zimprich ist Anwalt im IP & Medien-Team im Hamburger Büro von Fieldfisher. Er ist spezialisiert auf die Prozessführung in Fällen mit Technologiehintergrund, und berät Mandanten hauptsächlich aus dem Digitalsektor in den Bereichen Datenschutz, Wettbewerbsrecht, Medienrecht und IT-Recht. Für den eco Verband der Internetwirtschaft leitet er die Kompetenzgruppe Blockchain.

Seine Mandanten sind globale Anbieter von Cloud-Lösungen, soziale Netzwerke und Bewertungsplattformen, führende europäische Ad-Tech-Anbieter sowie spezialisierte Softwareanbieter in hochregulierten Sektoren wie etwa der Versicherungswirtschaft. Stephan Zimprich ist erfolgreicher Prozessanwalt und vertritt seine Mandanten regelmäßig vor Gericht, einschließlich des Europäischen Gerichtshofs und dem Europäischen Gerichtshof für Menschenrechte.