Woche 10 Recht: Der AI Act der Europäischen Union

Skript

Erarbeitet von
Dr. Ann-Kathrin Selker

Die Inhalte dieses Videos stellen keinesfalls eine Rechtsberatung in irgendeiner Form dar oder rechtliche Leitlinien. Ziels dieses Videos ist es, ein Problembewusstsein im Umgang mit KI zu schaffen und für rechtliche Fragen in diesem Kontext zu sensibilisieren. Vor dem Einsatz von KI-Systemen im Rahmen deines Projekts oder deiner Arbeit wende dich an die jeweiligen Fachstellen deiner Universität oder deines Unternehmens, um die rechtlichen Rahmenbedingungen für den Einsatz von KI zu besprechen.

Lernziele

- Die wichtigsten Grundlagen des AI Acts wiedergeben können
- KI-Modelle den Risikostufen des AI Acts zuordnen können

Projekt „KI für alle"
HeiCAD – Heine Center for Artificial Intelligence and Data Science

Inhalt

Einstieg

Die Unsicherheiten im Bereich Künstliche Intelligenz sind groß. Nimmt KI uns unsere Arbeitsplätze weg? Was ist mit sogenannten Social-Scoring-Systemen, bei denen anhand von berechneten Verhaltenswerten bestimmt wird, wer einen Job oder eine Wohnung erhält? Werden wir durch KI dauerhafter Überwachung unterworfen, oder gar in unserer Position als Letztentscheidende verdrängt?

Regulierung von KI

Die Vergangenheit hat bereits gezeigt, dass von KI Gefahren ausgehen können. So wurde z.B. ab dem Jahre 2013 in den Niederlanden ein KI-System zur Aufdeckung von Sozialbetrug eingesetzt. Dieses System markierte allerdings während seiner Einsatzzeit fälschlicherweise etwa 20.000 Eltern als Betrüger im Bereich von Kinderbeihilfen, was viele Familien in existenzielle finanzielle Notlagen versetzte.

Quelle [1]

Dabei handelt es sich nicht um einen tragischen Einzelfall, wie etwa der australische Robodebt-Skandal belegt.

Quelle [2]

Um die Verletzung von Rechtsgütern zu vermeiden, ist es also wichtig, dass der Einsatz von KI reguliert wird. Das kann natürlich alles heißen – zum Beispiel auch den Einsatz von KI komplett zu verbieten. Aber nicht von jedem KI-System geht dieselbe Gefahr bzw. dasselbe Risiko aus. So sollte zum Beispiel eine KI, die medizinische Entscheidungen trifft und damit direkten Einfluss auf deine Gesundheit hat, weitaus rigoroser geprüft und überwacht werden als eine KI, die mit dir Schach spielt.

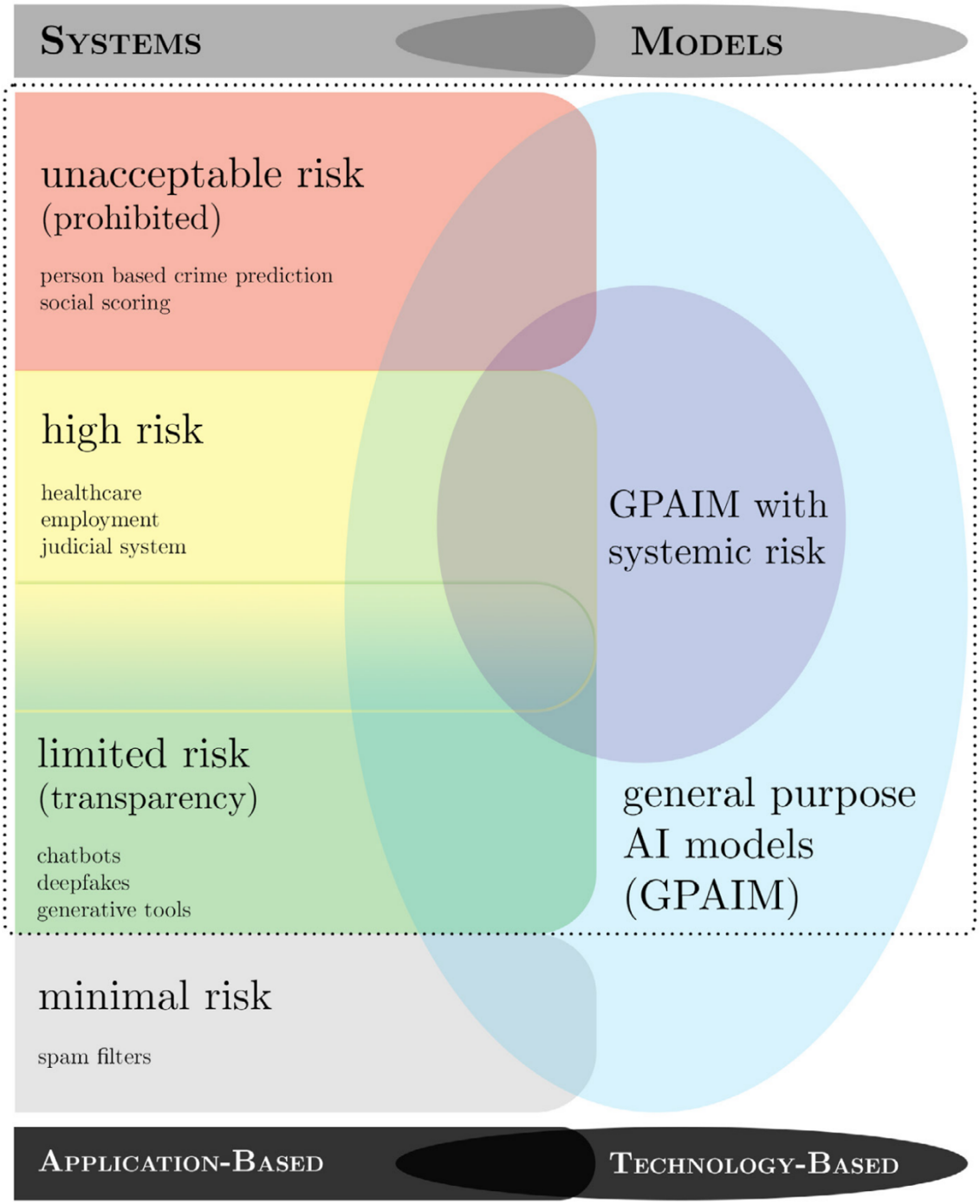
Genau einen solchen risikobasierten Ansatz legt auch die Europäische Union zugrunde. Diese schuf den sogenannten AI Act, der am 01. August 2024 in Kraft trat. Ziel dieser in der ganzen EU geltenden Verordnung ist es, mögliche Gefahren beim Einsatz von KI durch frühzeitige und weitreichende Vorgaben abzuschirmen.

Quelle [3]

Im AI Act werden KI-Systeme nach ihrem Risiko bewertet und dementsprechend gruppiert. Hier ist zu beachten, dass der AI Act auf im Grunde jede nicht-private Nutzung von KI-

Systemen anwendbar ist. Ausnahmen gibt es beim Einsatz von KI in der Forschung, beim Militär und im Bereich der nationalen Sicherheit.

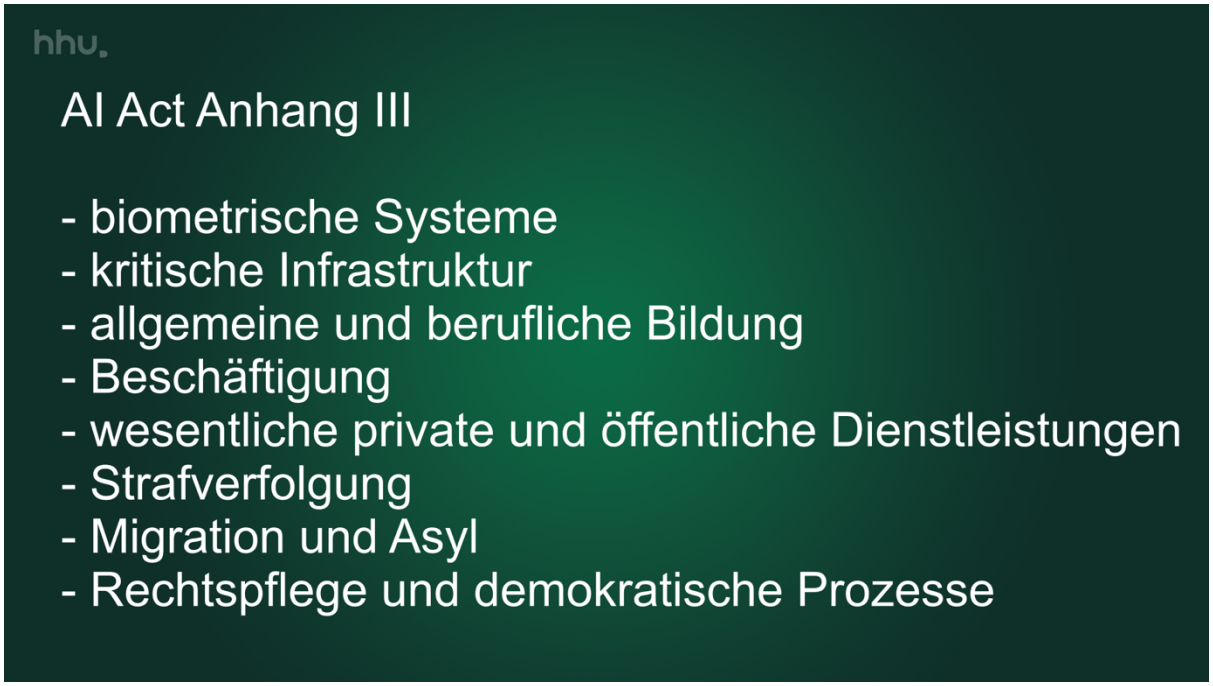
Die Risikogruppen des AI Acts



Risikogruppen des AI Acts (**Quelle [4]**)

Schauen wir uns doch einmal die Risikogruppen des AI Acts und ihre Einschränkungen genauer an. Für die höchste Risikogruppe, also für KI-Systeme mit inakzeptablem Risiko, wird sogar ein Verbot ausgesprochen. Dies betrifft alle KI-Anwendungen, die Menschen unterbewusst manipulieren oder ihnen schaden, und deckt damit viele Szenarien ab, die du aus dystopischen Filmen und Büchern kennst. In diese Kategorie fällt übrigens auch der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen im öffentlichen Raum zu Zwecken der Strafverfolgung, also z.B. Gesichtserkennung durch Videoüberwachung auf öffentlichen Plätzen, was in manchen Ländern von der Polizei eingesetzt wird – wobei es jedoch eine große Anzahl an Ausnahmen und Rückausnahmen gibt.

Als Nächstes kommen die hochriskanten KI-Systeme. Diese Systeme schaden den Menschen bei korrektem Einsatz nicht, werden aber in Szenarien eingesetzt, bei denen das Potential zu vergleichsweise schwerwiegenden Schädigungen besteht, ob aus Böswilligkeit oder auch "nur" aus Fahrlässigkeit. Werden in diesen Systemen z.B. mit Bias behaftete Trainingsdaten verwendet, können, wie in dem Kinderbeihilfe-Fall, Rechtsgüter verletzt werden, ohne dass die Nutzer:innen des Systems dies tatsächlich so vorsehen. Bei den hochriskanten KI-Systeme handelt es sich unter anderem um Systeme, die in Bereichen wie (kritischer) Infrastruktur, im Gesundheits- oder im Finanzwesen eingesetzt werden. Beispiele dafür sind Systeme, die den Luftraum überwachen, medizinische Geräte steuern oder Bonitätsprüfungen für Kredite durchführen. Aber auch Systeme, die ein Risiko für die Grundrechte einer Person darstellen, fallen in diese Kategorie. Biometrische Identifikation von Personen (sofern der jeweilige Einsatz nicht bereits in die inakzeptable Risikogruppe gehört), das Ausfiltern von Bewerbungen und das automatische Bewerten von Prüfungsleistungen sind einige Beispiele dafür.



Hochriskante Systeme sind zwar erlaubt, müssen aber strenge Anforderungen erfüllen, um in der EU benutzt werden zu können. Dazu gehören etwa Sicherheit, Robustheit und Datenqualität sowie Verständlichkeit. Außerdem müssen in diesen Bereichen die Vorgänge protokolliert und die Systeme von Menschen beaufsichtigt werden.

Unter die Kategorie der KI-Systeme mit beschränktem Risiko fallen die Systeme, die zur Interaktion mit Menschen bestimmt sind. Ein Beispiel hierfür sind Chatbots. In diesen Fällen sieht der AI Act vor, dass jederzeit klar sein muss, dass gerade mit einer KI und nicht mit einem Menschen interagiert wird. Ein Chatbot mit Namen und Bild einer realen oder real wirkenden Person ist unter dem AI Act also verboten, wenn der Kontext nicht offensichtlich macht, dass nicht mit einer „echten“ Personen interagiert wird.

Bot-Bild by Alexandra_Koch from pixabay.com

Auch generative KI-Systeme, also Systeme, die z.B. Texte oder Bilder erzeugen, werden im AI Act bestimmten Vorgaben unterworfen. Für diese von ihnen erstellten Inhalte ist unter gewissen Umständen eine Kennzeichnungspflicht zu beachten. So müssen sogenannte Deepfakes gekennzeichnet werden, also durch KI erzeugte Bilder, Videos oder Audio, die realistisch wirken und von einem “Durchschnittsmenschen” auch tatsächlich für realistisch gehalten werden könnten. Außerdem gilt die Kennzeichnungspflicht auch für KI-generierte oder KI-manipulierte Texte, die die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse informieren sollen. Ganz wichtig: Alle Kennzeichnungen müssen maschinenlesbar sein, z.B. in Form von Klartext oder speziellen Wasserzeichen.

Auf der untersten Risiko-Ebene befinden sich KI-Systeme mit minimalem Risiko, z.B. Spamfilter oder KI in Videospielen, solange diese nicht mit Menschen interagiert. Diese können ohne Einschränkungen benutzt werden.

Die eben vorgestellten Risikoeinstufungen sind natürlich nicht fest. Der AI Act sieht vor, dass die Kategorien regelmäßig überprüft und angepasst werden können, wenn neue Entwicklungen es nötig machen. Der AI Act ist unmittelbar in der gesamten EU rechtswirksam. Einige Teile der Verordnung gelten aber erst später, um einen reibungslosen Übergang für KI-Systeme, die sich bereits im Betrieb befinden, zu gewährleisten. Es ist übrigens nicht relevant, welchen Sitz ein Unternehmen hat, das ein KI-System herausbringen möchte: Der AI Act muss beachtet werden, sobald das entsprechende System in der EU auf den Markt kommt oder dessen Anwendung sich auf EU-Bürger:innen auswirkt.

Quelle [3]

Überwachung des AI Acts

Neue Regeln aufzustellen ist ja schön und gut, aber wie werden diese Regeln eigentlich durchgesetzt? Grundsätzlich sind Anbieter:innen und Betreiber:innen von KI-Systemen erst einmal selber dafür verantwortlich, das angebotene KI-System in die entsprechende Risikokategorie einzustufen und die Vorgaben einzuhalten. Manche Regelungen des AI Acts wie zum Beispiel die Kennzeichnungspflicht betreffen aber auch die Endnutzer:innen, sodass auch du mit den groben Regelungen des AI Acts vertraut sein solltest. Auf Regierungsebene werden Behörden eingerichtet, die den AI Act umsetzen sollen, sowohl auf EU- als auch auf nationaler Ebene. Bis August 2025 wird voraussichtlich eine deutsche KI-Aufsichtsbehörde ernannt werden. Diese Behörden und auch andere Gremien sind damit betraut, die praktische Umsetzbarkeit des AI Acts zu sichern. Es steht zu erwarten, dass Leitfäden herausgegeben werden, die sich insbesondere mit der technischen Implementation der weitreichenden Vorgaben befassen. Die Entwicklungen in diesem Bereich sind rapide, sodass es sich lohnt, sich auf dem neuesten Stand zu halten.

Quelle [5,6,7]

Verstößt jemand gegen Pflichten aus dem AI Act, besteht die Möglichkeit der Sanktionierung. Im schlimmsten Fall kann sogar eine Sanktion von 35 Millionen Euro oder — im Falle von Unternehmen — 7 % des weltweiten Jahresumsatzes verhängt werden, je nachdem, welche Zahl höher ist. Davon geht eine beachtliche Abschreckungswirkung aus, sodass eine Einhaltung der Vorgaben anzuraten ist.

Quelle [3]

Abschluss

Kommen wir noch einmal zurück zum Anfang: KI ist überall, und auch die Angst vor KI begleitet viele Menschen ständig. Der AI Act ist aber hoffentlich ein Schritt in die richtige Richtung, um die realen Risiken, die KI mit sich bringt, zu minimieren.

Quellen

Quelle [1] Dachwitz, I. (2021, 29. Dezember). *Kindergeldaffäre: Niederlande zahlen Millionenstrafe wegen Datendiskriminierung*. netzpolitik.org. https://netzpolitik.org/2021/kindergeldaffaere-niederlande-zahlen-millionenstrafe-wegen-datendiskriminierung/

Quelle [2] Mao, B. F. (2023, 7. Juli). *Robodebt: Illegal Australian welfare hunt drove people to despair*. https://www.bbc.com/news/world-australia-66130105

Quelle [3] Artificial Intelligence Act, Regulation (EU) 2024/1689. http://data.europa.eu/eli/reg/2024/1689/oj

Quelle [4] G'sell, F. (2024). Regulating under Uncertainty: Governance Options for Generative AI. *SSRN*, S. 238. https://doi.org/10.2139/ssrn.4918704

Quelle [5] Commission Decision Establishing the European AI Office. (2024). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office

Quelle [6] Gesetz über künstliche Intelligenz (Verordnung (EU) 2024/1689), Artikel 65 https://artificialintelligenceact.eu/de/article/65/

Quelle [7] Steiner, F. (2024, 26. September). Künstliche Intelligenz: Wie die Bundesnetzagentur die Aufsicht übernehmen soll. *Heise Online*. https://www.heise.de/news/KI-Verordnung-Bundesregierung-verraet-Aufsichtsregime-Plan-9954083.html

Weiterführendes Material

D. Becker/D. Feuerstack, Die EU-KI-Verordnung, KIR 2024, 62

K. Chibanguza/H. Steege, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769

C. Krönke, Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten, NVwZ 2024, 529

J. Möller-Klapperich, Die neue KI-Verordnung der EU, NJ 2024, 337

E. Hilgendorf/D. Roth-Isigkeit (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, 2. Aufl. 2025 (pro futuro)

M. Martini/C. Wendehorst (Hrsg.), Kommentar KI-VO, 2024

Disclaimer

Transkript zu dem Video „Woche 10 Recht: Der AI Act der Europäischen Union“, Ann-Kathrin Selker.