KI-Gesetze
Zusammenfassung des AIA im Angesicht der offiziellen Einführung im Sommer 2023

Alexander Ottl, HdM Stuttgart, SS23

Abstrakt

Im Angesicht der geplanten Einführung offizieller KI Regulierungen in Europa soll dieses Paper eine Zusammenfassung der Regelungen des AIA (Artificial Intelligence Act) vom 21. April 2021 liefern, welcher als Basis für den geplanten Gesetzesentwurf dient

Intro

Die Entwicklung und Anwendung von Künstlicher Intelligenz (KI) bringt zahlreiche Chancen und Herausforderungen mit sich. Auf der einen Seite kann KI Innovationen fördern, die Effizienz steigern und neue Möglichkeiten in verschiedenen Bereichen eröffnen. Auf der anderen Seite können unregulierte KI-Systeme erhebliche Risiken mit sich bringen, wie etwa Verletzungen der Privatsphäre, Diskriminierung oder unfaire Entscheidungsprozesse.

Der Einsatz von KI hat in den letzten Jahren weltweit erheblich zugenommen und damit die Notwendigkeit geschaffen, angemessene rechtliche Rahmenbedingungen für diese Technologie zu schaffen. In Europa erkennen Regierungen und Institutionen die Bedeutung von KI-Gesetzen an und haben in jüngster Zeit bedeutende Fortschritte gemacht, um den verantwortungsvollen und ethischen Einsatz von KI sicherzustellen. So wurden beispielsweise in Deutschland, Frankreich und Großbritannien spezifische Gesetze und Vorschriften erlassen, um den Einsatz von KI-Systemen in der Gesundheitsversorgung zu regulieren. In diesem Papier werden wir einen Überblick über die aktuellen KI-Gesetze in Europa geben und analysieren, warum solche Gesetze notwendig sind.

AIA (Artificial Intelligence Act)

Am 21. April 2021 hat die Europäische Kommission den Vorschlag für den Artificial Intelligence Act (AI Act) veröffentlicht. Dieser Akt stellt einen bedeutenden Schritt dar, um den Einsatz von Künstlicher Intelligenz (KI) in der Europäischen Union zu regulieren und sicherzustellen, dass sie ethisch und verantwortungsvoll eingesetzt wird. Bis heute wurden die dort vorgeschlagenen Regelungen jedoch nicht offiziell durchgesetzt, was sich ab Sommer 2023 ändern soll.
Der AI Act zielt darauf ab, einheitliche Regeln und Standards für den Einsatz von KI-Systemen in der EU festzulegen, um das Vertrauen der Bürger:innen in diese Technologie zu stärken und gleichzeitig potenzielle Risiken und Missbräuche zu minimieren. Der Akt deckt eine breite Palette von Anwendungen ab, von autonomen Fahrzeugen über Gesichtserkennungssysteme bis hin zu Chatbots und Robotern im Gesundheitswesen. Der AI Act definiert Künstliche Intelligenz als

"*eine Technologie, einschließlich Algorithmen, die dazu entwickelt wurde, in der Lage zu sein, bestimmte Funktionen auszuführen, die menschliche kognitive Fähigkeiten nachahmen oder automatisieren können.*" *[1]*

Diese Definition umfasst sowohl KI-Systeme, die auf maschinellem Lernen basieren, als auch solche, die auf symbolischer Logik oder anderen Ansätzen beruhen.

Der Akt legt verschiedene Anforderungen für KI-Systeme fest. Ein zentrales Element ist die Einteilung von KI-Systemen in vier Risikoklassen:
- inakzeptables Risiko,
- hohes Risiko,
- begrenztes Risiko
- minimales Risiko

KI-Systeme, die als inakzeptables Risiko eingestuft werden, werden vollständig verboten, während für KI-Systeme mit hohem Risiko strenge Anforderungen gelten, einschließlich umfassender Dokumentations-überprüfungen.

Unter die Kategorie „inakzeptables Risiko“ fallen z.B. biometrische Echtzeit-Identifikationssysteme in öffentlichen Räumen, biometrische Echtzeit-Kategorisierungssysteme basierend auf sensitiven Charakteristika (z.B. Herkunft, Geschlecht, ethnische Zugehörigkeit ivm.) und Emotionserkennungssysteme im Gesetzessektor.

Hochrisiko-KI-System werden in zwei Kategorien unterteilt. Zum Einen geht es um Systeme, die unter die Produktsicherheitsgesetzgebung der EU fallen (z.B. Spielzeuge, Autos und medizinische Geräte) und zum Anderen um KI-Systeme die unter die folgenden acht Kategorien fallen:

- biometrische Identifizierung und Kategorisierung natürlicher Personen (nicht echtzeit)
- Management und Betriebt kritischer Infrastruktur
- Lehre und berufliches Training
- Anstellungsverfahren, Personalmanagement und Zugang zu Selbstständigkeit
- Zugang zu und Genuss wesentlicher privater Dienstleistungen und öffentlicher Dienstleistungen und Vorteile
- Strafverfolgung
- Migrations-, Asyl- und Grenzkontrollmanagement
- Unterstützung bei der rechtlichen Auslegung und Anwendung des Gesetzes

Alle KI-Systeme, die unter diese Kategorien fallen werden vor der Markteinführung und während ihres gesamten Lebenszyklus durch Menschen bewertet.

Entwickler und Betreiber sogenannter Basismodelle werden durch den AI Act dazu verpflichtet, mögliche Risiken (z.B. in Bezug auf Gesundheit, Sicherheit, Grundrechte und Umwelt) zu bewerten und offenzulegen. Außerdem müssen diese Modelle vor Veröffentlichung offiziell in der EU Datenbank registriert werden und zusätzlich eine bestimmte Anforderung an transparenz erfüllen. Zu letzterem zählt unteranderem das warnen vor Deep Fakes und das Gewähren von Sicherheit vor illegalen Inhalten.
Zum Thema Transparenz steht im AI Act: "Ein hohes Maß an Transparenz sollte gewährleistet sein, um das Vertrauen in KI-Systeme zu stärken und eine wirksame Aufsicht zu ermöglichen“ [1]. Es wird festgelegt, dass die Nutzung von KI-Systemen den Nutzern gegenüber transparent sein muss, und dass bestimmte Kategorien von KI-Systemen immer erklärbar sein sollten. Es soll einsehbar sein, mit welchen Daten KI-Modelle trainiert worden sind. Der Akt enthält auch Vorschläge zur Haftung für KI-Systeme und legt fest, dass diejenigen, die KI-Systeme auf den Markt bringen oder nutzen, für etwaige Schäden oder Verletzungen verantwortlich sind, die durch diese Systeme verursacht werden. Endkunden soll es einfacher gemacht werden, Beschwerden gegen KI Systeme einzureichen. Eine genaue Umsetzung dieser Vorschläge ist jedoch noch nicht geklärt.
Darüber hinaus werden Ethikprüfungen für KI-Systeme mit hohem Risiko vorgeschrieben, um sicherzustellen, dass sie den Grundwerten der EU entsprechen und keine grundlegenden Rechte verletzen.

Neben vielen Regulierungen will der AI Act auch neue Möglichkeiten schaffen. So soll eine KI Sandbox entstehen, innerhalb dieser Unternehmen und Privatpersonen KI Modelle testen können bevor sie eingeführt werden. Diese Umgebungen geben Raum um Innovationen in realen Szenarien zu prüfen ohne dabei Risiken einzugehen. Auch im Bereich der Forschung und bei Open Source Projekten sieht der Gesetzesentwurf Möglichkeiten für Ausnahmeregelungen, vor Allem bei Hochrisiko-KI Systemen, vor um mehr Platz für Innovationen zu schaffen.

Nächste Schritte

Der Gesetzesentwurf ist noch nicht final und weitere Gespräche werden folgen. Im Rahmen des Trilog-Prozesses wird das Parlament mit dem EU-Rat und der Europäischen Kommission Mitte/Ende Sommer 2023 verhandeln. Das Hauptziel besteht darin, eine vorläufige Einigung über einen Legislativvorschlag zu erzielen, der sowohl für das Parlament als auch für den Rat als Mitgesetzgeber akzeptabel ist. Die Kommission spielt dabei eine Vermittlerrolle und unterstützt bei der Vereinbarung zwischen den Mitgesetzgebern. Diese vorläufige Einigung muss anschließend von jeder der beteiligten Institutionen formal angenommen werden.
Die Hauptgesprächsthemen umfassen die Definition von KI, die in die Kategorie der Hochrisiko Systeme fallenden KI Systeme und ob biometrische Scans gänzlich verboten werden sollen oder mit Ausnahmen Verwendung finden dürfen.
Ziel ist die Verabschiedung eines endgültigen EU-Gesetzes für KI Ende 2023 bevor im Jahr 2024 neue EU Parlamentswahlen anstehen.

Umsetzung

Das EU-Parlament sieht für die Marktüberwachung eine Nationale Überwachungsbehörde (NSA) pro Mitgliedsstaat vor. Dieser Ansatz hat den Vorteil, dass das sammeln von Talenten und das Aufbauen von internem Wissen innerhalb der NSAs effizient gestaltet werden kann und gleichzeitig die Kommunikation zwischen den einzelnen Staaten vereinfacht wird. Als Nachteil stellt sich die Finanzierung einer solchen Zentralisierung und die Kommunikation innerhalb des Staates zwischen KI-Experten und Fachkräften heraus. KI-Anwendungen können sehr komplex sein, weshalb eine Integration von KI-Experten innerhalb verschiedener Organisationen eines Staates von Vorteil sein könnte. Letzteren Ansatz verfolgen EU-Rat und Kommision, sodass die Marktüberwachung durch beliebig viele Organisationen erfolgen kann. Solch eine Umsetzung würde jedoch die Kommunikation zwischen den Staaten erheblich erschweren und gleichzeitig die Gleichheit der Überwachung einzelner Sektoren nicht mehr gewährleisten können.

Ein weiterer zu klärender Mechanismus ist das Ernennen von unabhängigen Organisationen zu sogenannten Bekanntstellen durch die Benachrichtigungsbehörde. Bekanntstellen sind Organisationen, die KI-Systeme mit Hohen Risiko überprüfen und zertifizieren dürfen. Solch eine Überprüfung ist jedoch nicht verpflichtend für Unternehmen, weshalb im Trilog die Frage geklärt werden sollte, ob die Einführung eines solchen Ökosystems den Aufwand wirklich wert ist oder mehr Fokus auf die NSA gelegt werden sollte.

Es ist immer noch nicht ganz klar, inwieweit Beschwerden, Wiedergutmachung und zivilrechtliche Haftung von Personen, die durch KI-Systeme geschädigt worden sind, umgesetzt werden. Eine neue KI-Haftungsrichtlinie soll diese offenen Fragen ein wenig klären. Zunächst will die vorgeschlagene Richtlinie Richtern die Offenlegung von Beweisen durch Anbieter und Benutzer relevanter KI Anwendungen ermöglichen. Des Weiteren soll ein Beschuldigter in Fall mit KI-Anwendungen für Schuldig erklärt werden, wenn:

- die Nichteinhaltung des AI-Gesetzes nachgewiesen werden kann
- diese Nichteinhaltung wahrscheinlich das Ergebnis des KI-Systems beeinflusst hat
- dieses Ergebnis (oder dessen Fehlen) zu Schäden des Klägers geführt hat

Es ist noch unklar, welche Auswirkungen die rechtliche Umsetzung der KI-Gesetze auf in der EU ansäßige Unternehmen mit sich bringen wird und in welchem Maße Endkonsumenten über ihre Rechte informiert sein werden und Unterstützung durch Gemeinnützige Interessenvertretungen erhalten werden. Diese Fragen können jedoch nicht durch den Trilog geklärt werden, sondern stellen sich in den Kommenden Jahren nach Einführung des Gesetzes heraus.

Aussichten

Über 150 europäische Unternehmen und CEOs haben als Antwort auf die geplante Einführung des Gesetzesentwurf im Sommer 2023 eine Forderung an die EU gestellt, die Änderungen zu überdenken, da diese die Wettbewerbsfähigkeit Europas gegenüber dem Rest der Welt stark einschränken würden. Der neue AI Act würde die technologischen Möglichkeiten, welche Künstliche Intelligenz bietet, unterdrücken. Die größte Gefahr sieht man in den Regelungen zu generativen KIs bzw. Basismodellen. Man befürchtet, Unternehmen könnten sich aufgrund zu starker Regelungen komplett aus der EU zurückziehen.
Um solche Gesetze besser einschätzen zu können fordern die Unternehmen eine Expertengruppe innerhalb der KI Industrie, welche sich auf KI Gesetze und deren Anwendung in der Industrie spezialisieren soll.

Allgemein ist die Debatte über die geplanten Gesetze noch lange nicht vorbei und wird auch in Zukunft bei weiteren Änderungen weitergehen. Es ist eine klare Schere zwischen der Wahrung der eigenen Vorteile und dem Schutz vor KI zu sehen. Staaten mit KI Regelungen können im globalen Wettbewerb tendenziell häufiger hinterherhinken als Staaten ohne Regelungen, wobei ein Schutz von Daten und Endkonsumenten ein notwendiges Gut im Umgang mit KI darstellen. Der AI-Act stellt einen bedeutenden ersten Schritt in der KI-Gesetzgebung dar und unabhängig von Vor- und Nachteilen der Erneuerungen gilt ein besonderes Augenmerk dem wahrscheinlich wichtigsten Aspekt des Themas: Der Anregung zur Diskussion und der tatsächlichen Umsetzung von Gesetzen und Regelungen.

Quellen

- *Europäische Kommission. "Vorschlag für einen Künstliche-Intelligenz-Act." 21. April 2021. URL: https://ec.europa.eu/commission/presscorner/detail/de/ip_21_1681*
- *https://www.theverge.com/2023/6/30/23779611/eu-ai-act-open-letter-artificial-intelligence-regulation-renault-siemens (last visited: 02.07.23 12:43)*
- *https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai (last visited: 02.07.23 15:30)*
- *https://www.artificial-intelligence-act.com (last visited: 03.07.23 11:30)*
- *https://www.brookings.edu/articles/key-enforcement-issues-of-the-ai-act-should-lead-eu-trilogue-debate/ (last visited: 03.07.23 12:07)*
- *https://chat.openai.com*