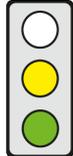


KERNPUNKTE

Ziel des Weißbuchs: Die Kommission schlägt verbindliche rechtliche Anforderungen für risikoreiche Anwendungen der künstlichen Intelligenz (KI) vor, die von KI-Entwicklern und -Nutzern in der gesamten EU einzuhalten sind.

Betroffene: KI-Entwickler und Betreiber, Unternehmen und Privatpersonen, die KI nutzen oder von ihr betroffen sind.



Pro: (1) Der vorgeschlagene risikobasierte Ansatz trägt der Tatsache Rechnung, dass die möglichen Folgen für die Nutzer von der spezifischen KI-Anwendung und dem Sektor abhängen, in dem diese eingesetzt wird.

(2) Zwingende gesetzliche Anforderungen für risikoreiche KI-Anwendungen und freiwillige Anforderungen für risikoarme KI-Anwendungen respektieren das Verhältnismäßigkeitsprinzip.

Contra: Die Definition von „risikoreich“ ist nicht klar genug, um Rechtssicherheit zu schaffen. Zu klären ist, wann die mit der Nutzung einer KI-Anwendung verbundenen Risiken als „erheblich“ anzusehen sind.

Die wichtigsten Passagen im Text sind durch einen Seitenstrich gekennzeichnet.

INHALT

Titel

Weißbuch COM(2020) 65 vom 19. Februar 2020: **Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen**

Kurzdarstellung

► Allgemeiner Hintergrund

- Künstliche Intelligenz [im Folgenden: „KI“] ist ein Bestand an Technologien, die Daten, Algorithmen und Rechenleistung kombinieren [S. 2].
- Der Zweck des Weißbuchs besteht darin, „politische Optionen“ darzulegen, wie die Nutzung von KI gefördert und gleichzeitig den mit KI verbundenen Risiken Rechnung getragen werden kann. Um diesen Zweck zu erreichen, plant die Kommission, in der EU
 - ein „Ökosystem für Exzellenz“ für KI, und
 - ein „Ökosystem für Vertrauen“ in KI zu entwickeln; zu diesem Zweck legt die Kommission die mit KI einhergehenden Risiken und ihren Plan zur Bewältigung dieser Risiken dar. In diesem Zusammenhang plant die Kommission, Folgendes vorzuschlagen:
 - Änderungen der bestehenden Gesetzgebung, und
 - neue KI-spezifische Gesetzgebung, insbesondere zusätzliche Anforderungen für risikoreiche KI-Anwendungen und ein freiwilliges Kennzeichnungssystem für risikoarme KI-Anwendungen.

► Maßnahmen zur Entwicklung eines „Ökosystems für Exzellenz“ für KI

- Die Kommission schlägt u.a. die folgenden Maßnahmen vor:
 - eine Neufassung des Koordinierten Plans für KI [s. [cepAnalysen 10/2019](#), [12/2019](#) und [13/2019](#)] bis Ende 2020 [S. 6], um u.a. sicherzustellen, dass mindestens ein digitales Innovationszentrum pro Mitgliedstaat auf KI hochspezialisiert ist [S. 7],
 - eine „Erleichterung“ der Einrichtung von Exzellenz- und Testzentren für KI, finanziert durch die EU, die Mitgliedstaaten und den Privatsektor, ggf. unter „Schaffung eines neues Rechtsinstruments“ [S. 7],
 - ein gemeinsames Pilotprogramm mit dem Europäischen Investitionsfonds mit einem Etat von 100 Mio. Euro zur Finanzierung innovativer KI-Entwicklungen [S. 8, vgl. [cepAnalyse 10/2019](#)],
 - einen Aktionsplan zur Erleichterung der Entwicklung, Erprobung und Einführung von KI durch Behörden und Anbieter von Dienstleistungen von öffentlichem Interesse, z.B. Versorgungs- und Verkehrsdienstleistungen. Die Kommission wird zuvor Dialoge mit Interessengruppen führen [S. 9] und
 - eine Verbesserung des Zugangs zu Daten und ihrer Verwaltung sowie eine Förderung von Cloud-Infrastrukturen, Hochleistungs- und Quanten-Rechnern, da die Entwicklung von KI-Anwendungen sowohl den Zugang zu Daten als auch maßgebliche Rechentechnologien und –infrastrukturen erfordert [S. 9].

► Risiken von KI-Anwendungen

- Die Nutzung von KI-Anwendungen erhöht die Risiken für Grundrechte (z.B. Nichtdiskriminierung), Sicherheit und das wirksame Funktionieren des Haftungssystems. Dies ist u.a. zurückzuführen auf

- Voreingenommenheiten (*biases*) in einer KI-Anwendung, die größere Auswirkungen haben könnten als Voreingenommenheiten in der menschlichen Entscheidungsfindung, weil der KI die sozialen Kontrollmechanismen fehlen, die das menschliche Verhalten steuern,
- die mangelnde Transparenz (Opazität) vieler KI-Anwendungen, die die Überprüfung der Einhaltung von Rechtsnormen erschwert, weil es schwierig oder gar unmöglich ist, zurückzuerfolgen, wie eine Entscheidung getroffen wurde [S. 12-15]; Opazität erhöht daher die Schwierigkeiten bei der Feststellung
- des Vorliegens der Haftungs Voraussetzungen, wenn ein Schaden angeblich durch einen Fehler in einem mit KI ausgestatteten Produkt verursacht wurde [S. 14-15], und
- eines Verstoßes gegen das geltende nationale und EU-Sicherheitsrecht [S. 15].

► **Mögliche Anpassungen der für KI geltenden Rechtsvorschriften**

- Die EU-Vorschriften – wie die Produktsicherheitsrichtlinie und die Produkthaftungsrichtlinie – gelten zwar grundsätzlich auch für KI; die Kommission identifiziert jedoch fünf Mängel, die behoben werden sollten [S. 16-17]:
 - Die geltenden EU-Vorschriften adressieren im Wesentlichen Sicherheitsrisiken, die zum Zeitpunkt des Inverkehrbringens bestehen. Eine KI-Anwendung kann jedoch ihre Funktionsweise verändern und neue Risiken verursachen, insbesondere wenn sie auf maschinellem Lernen beruht oder häufige Updates erfordert.
 - Aufgrund der Opazität von KI könnte es notwendig sein, bestehende Sicherheits- und Haftungs Vorschriften anzupassen oder zu präzisieren, um ihre wirksame Anwendung zu gewährleisten.
 - Der Anwendungsbereich der EU-Sicherheitsgesetzgebung ist begrenzt; sie gilt aktuell nur für Produkte. Daher
 - fallen KI-basierte Dienstleistungen nicht unter die EU-Sicherheitsvorschriften und
 - ist unklar, ob eigenständige Software ein „Produkt“ im Sinne der EU-Produktsicherheitsvorschriften ist.
 - Die bestehenden EU-Vorschriften erfassen neue Risiken – z.B. solche, die sich aus Cyber-Bedrohungen oder dem Verlust der Konnektivität ergeben – nicht ausdrücklich, unabhängig davon, ob diese Risiken zum Zeitpunkt des Inverkehrbringens vorhanden waren oder während der Nutzung des Produkts auftreten.
 - Die Verantwortlichkeitsverteilung zwischen den verschiedenen Wirtschaftsakteuren ist unklar. Das EU-Produkthaftungsrecht regelt nur die Haftung der Hersteller, nationales Recht die Haftung anderer in der Lieferkette. Die Haftung ist z.B. unklar, wenn ein Dritter einem Produkt nach dessen Inverkehrbringen KI hinzufügt.

► **Neue KI-spezifische Vorschriften**

- Neben der Aktualisierung des bestehenden EU-Rechts erwägt die Kommission auch den Erlass neuer KI-spezifischer Rechtsvorschriften.
- Dies erfordert eine klare Definition von KI, die sowohl flexibel sein muss, um dem technischen Fortschritt Rechnung zu tragen, als auch präzise genug, um die notwendige Rechtssicherheit zu gewährleisten [S. 19].
- Um die Verhältnismäßigkeit zu gewährleisten, schlägt die Kommission einen risikobasierten Ansatz vor: KI-Anwendungen sollten als „risikoreich“ oder „risikoarm“ kategorisiert werden, wobei erstere strengeren zusätzlichen Anforderungen unterliegen sollen [S. 20].
- Eine KI-Anwendung soll als risikoreich gelten, wenn sie die beiden folgenden Kriterien kumulativ erfüllt [S. 20f.]:
 - sie wird in einem Sektor verwendet, in dem typischerweise mit erheblichen Risiken zu rechnen ist, z.B. im Gesundheitswesen; dieser Sektor muss in einer abschließenden Liste von Sektoren aufgeführt sein, und
 - sie wird in einem solchen Sektor so eingesetzt, dass mit erheblichen Risiken zu rechnen ist, z.B. wenn
 - die KI-Anwendung „rechtliche oder ähnlich erhebliche Auswirkungen“ auf die Rechte einer natürlichen Person oder eines Unternehmens haben könnte, oder
 - von ihr Verletzungs- oder Lebensgefahr oder die Gefahr eines erheblichen Schadens ausgeht, oder
 - die KI-Anwendung Auswirkungen hat, die „realistischerweise nicht vermieden werden können“.
- Unabhängig vom Sektor sollte der Einsatz von KI-Anwendungen ausnahmsweise „grundsätzlich“ als risikoreich angesehen werden, wenn damit spezifische Risiken verbunden sind, z.B. wenn KI-Anwendungen bei Einstellungsverfahren oder zur biometrischen Fernidentifizierung verwendet werden [S. 21].
- Die zusätzlichen Anforderungen für risikoreiche KI-Anwendungen sollten für alle relevanten Wirtschaftsakteure gelten, die KI-gestützte Produkte oder Dienstleistungen innerhalb der EU anbieten, unabhängig vom Ort ihrer Niederlassung [S. 27].
- An KI-Anwendungen sind viele Akteure beteiligt, darunter Entwickler, Betreiber, Nutzer, Hersteller und Dienstleister. Die Pflichten gemäß der neuen KI-spezifischen Gesetzgebung sollten denjenigen Akteuren obliegen, die „am besten in der Lage“ sind, potenzielle Risiken zu bewältigen [S. 26f.].

► **Zusätzliche Anforderungen für risikoreiche KI-Anwendungen**

- Die Kommission erwägt die folgenden zwingenden rechtlichen Anforderungen für risikoreiche KI-Anwendungen:
 - Pflichten, KI-Anwendungen mit Datensätzen zu trainieren, die umfassend und ausreichend repräsentativ sind, oder andere Anforderungen, um sicherzustellen, dass [S. 22f.]
 - KI-Anwendungen sicher sind und nicht zu diskriminierenden Ergebnissen führen, und
 - personenbezogene Daten und die Privatsphäre angemessen geschützt werden.
 - Anforderungen, die gewährleisten sollen, dass [S. 24f.]

- KI-Anwendungen über ihren gesamten Lebenszyklus hinweg robust, genau, widerstandsfähig gegen Angriffe und in der Lage sind, Fehler und Unstimmigkeiten angemessen zu bewältigen, und
 - ihre Ergebnisse reproduzierbar sind.
 - Verschiedene Formen menschlicher Aufsicht über bestimmte KI-Anwendungen, u.a. indem [S. 25]
 - die Ergebnisse der KI-Anwendung erst nach menschlicher Überprüfung und Validierung wirksam werden,
 - eine menschliche Überprüfung nach Wirksamwerden der Ergebnisse der KI-Anwendung sichergestellt wird,
 - KI-Anwendungen während des Betriebs durch einen Menschen überwacht werden, der in Echtzeit eingreifen und sie deaktivieren kann, oder
 - einer KI-Anwendung betriebliche Einschränkungen auferlegt werden, z.B. dass ein fahrerloses Auto bei schlechter Sicht anhält.
 - Die Pflicht, genaue Aufzeichnungen über verwendete Datensätze, Programmierungs- und Trainingsmethoden zu führen und diese – sowie „in bestimmten begründeten Fällen“ die Datensätze selbst – Behörden auf Anfrage zur Verfügung zu stellen, um die Transparenz der KI zu erhöhen [S. 23].
 - Pflichten, proaktiv Informationen über die Fähigkeiten und Grenzen der KI-Anwendung sowie ihren erwarteten Genauigkeitsgrad bereitzustellen, sowie eine allgemeine Pflicht, Personen darüber zu informieren, dass sie mit einer KI-Anwendung interagieren, falls dies nicht unmittelbar ersichtlich ist [S. 23f.].
 - Der Einsatz biometrischer Fernidentifikationssysteme – z.B. zur Gesichtserkennung – ist nach dem EU-Datenschutzrecht und der EU-Grundrechtecharta nur zulässig, wenn er begründet und verhältnismäßig ist und geeignete Garantien vorliegen. Die Kommission will eine breite Debatte über deren Nutzung einleiten [S. 26].
 - Die Kommission will obligatorische Ex-ante-Konformitätsbewertungen einführen, um die Einhaltung der Anforderungen zu überprüfen, bevor risikoreiche KI-Anwendungen auf den Binnenmarkt gebracht werden, und erwägt in bestimmten Fällen auch wiederholte Bewertungen während deren gesamter Lebensdauer [S. 27f.].
- **Freiwilliges Kennzeichnungssystem für risikoarme KI-Anwendungen**
- Für risikoarme KI-Anwendungen überlegt die Kommission, ein freiwilliges Kennzeichnungssystem einzuführen. Interessierte Parteien könnten sich in dessen Rahmen zur Einhaltung bestimmter Anforderungen verpflichten und ein Qualitätslabel erhalten, das die Vertrauenswürdigkeit ihrer KI-Anwendungen signalisiert [S. 29].
 - Bei den Anforderungen könnte es sich um die oben genannten Anforderungen an risikoreiche KI-Anwendungen oder um ähnliche, speziell für das jeweilige Kennzeichnungssystem festgelegte Anforderungen handeln [S. 29].

Politischer Kontext

Das Weißbuch zur KI ist Teil der Kommissionsstrategie zur Gestaltung der digitalen Zukunft Europas, neben der europäischen Datenstrategie [cepAnalysen folgen] und anderen in der Begleitmitteilung COM(2020) 67 dargelegten Aktionen. Sie baut auf der KI-Strategie der EU von 2018, dem Koordinierten Plan für KI und auf der Mitteilung COM(2019) 168 betreffend Ethik-Leitlinien für KI [vgl. cepAnalyse Nr. [16/2019](#)] auf. Das Europäische Parlament forderte die Kommission in seiner Entschließung [P9 TA-PROV\(2020\)0032](#) auf, ein Risikobewertungssystem für KI zu entwickeln. Mangels Regelungen auf EU-Ebene haben einige Mitgliedstaaten bereits begonnen, KI zu regulieren [S. 12].

BEWERTUNG

Ökonomische Folgenabschätzung

Insgesamt gesehen ist der Ansatz der Kommission zur KI-Regulierung aus folgenden Gründen angemessen:

Erstens: **Der vorgeschlagene risikobasierte Ansatz trägt der Tatsache Rechnung, dass die möglichen Folgen für die Nutzer von der spezifischen KI-Anwendung und dem Sektor abhängen, in dem diese eingesetzt wird.** Denn die Festlegung strenger Anforderungen an KI-Anwendungen kann zwei negative Auswirkungen haben: Europäische Start-ups, die KI-Anwendungen entwickeln, werden benachteiligt, wenn die Kosten für die Einhaltung der Anforderungen unverhältnismäßig höher sind als z.B. in den USA, wo Start-ups schnell wachsen können und die strengeren EU-Anforderungen erst später beim Eintritt in den EU-Markt erfüllen müssen. Darüber hinaus würden die Vorteile der KI-Nutzung – z.B. die Automatisierung langwieriger und mühsamer Aufgaben – geschmälert, wenn die Unternehmen stets strenge Anforderungen erfüllen müssten, z.B. menschliche Aufsicht und Rechtsmittel gewährleisten. **Die negativen Auswirkungen einer strengen Regulierung, die auch die Entwicklung eines Ökosystems der Exzellenz schwächen könnten, werden reduziert, wenn die Anforderungen nur für risikoreiche KI-Anwendungen gelten.**

Zweitens: Da KI-Anwendungen ihre Funktionsweise verändern können, müssen risikoreiche KI-Anwendungen robust, genau und ihre Ergebnisse über ihren Lebenszyklus reproduzierbar sein. Dadurch wird gewährleistet, dass z.B. das Risiko erheblicher Schäden oder Verletzungen als unvorhergesehene Folge eines Software-Updates minimiert wird. Daher schlägt die Kommission zu Recht vor, wiederholte Konformitätsbewertungen auch nach dem Inverkehrbringen der KI-Anwendungen durchzuführen.

Drittens: Für risikoreiche KI-Anwendungen sollten – wie von der Kommission vorgeschlagen – verschiedene Formen der menschlichen Aufsicht vorgesehen werden. Da KI-Anwendungen auch beim Einsatz im gleichen Hochrisikosektor

zu unterschiedlich großen Risiken führen können, sollte über die bestgeeignete Art der Aufsicht jeweils einzelfallbezogen entschieden werden. Während z.B. das Ergebnis einer KI-Anwendung, die tödliche Risiken birgt, ohne Zustimmung eines Menschen nicht wirksam werden sollte, könnte bei anderen KI-Anwendungen eine nachträgliche menschliche Kontrolle ausreichen.

Viertens: Die Einführung eines freiwilligen Kennzeichnungssystems für risikoarme KI-Anwendungen achtet die unternehmerische Freiheit. Wenn Verbraucher das Siegel wertschätzen, wäre dies dennoch ein Anreiz für Unternehmen, an dem freiwilligen System teilzunehmen, um die Verbraucher von ihrer „Vertrauenswürdigkeit“ zu überzeugen.

Juristische Bewertung

Kompetenz

Die EU kann in Ausübung ihrer Binnenmarktkompetenz zur Gewährleistung eines hohen Verbraucherschutzniveaus [Art. 114, Art. 169 Abs. 1 AEUV] auch bereits harmonisiertes Recht wie die Produkthaftungsrichtlinie und die Produktsicherheitsrichtlinie an neue technische Entwicklungen und Risiken anpassen und ihre Anwendung auf KI-basierte Produkte und Dienstleistungen klarstellen oder ausweiten: Zum einen wird der freie Handel mit letzteren durch die Rechtsunsicherheit behindert, inwieweit die geltenden Regelungen auf KI anwendbar sind; zum anderen besteht die wahrscheinliche Gefahr der Rechtszersplitterung und Wettbewerbsverzerrung, wenn die Mitgliedstaaten eigene Haftungs- und Sicherheitsregeln für KI erlassen, z.B. die von den Richtlinien nicht erfasste Haftung für Dienstleistungen regeln. Die Beurteilung der Kompetenz für neue KI-spezifische Rechtsvorschriften hängt vom Inhalt des künftigen Vorschlags ab. Deren Erlass kann aber grundsätzlich auf Art. 114 gestützt werden, um der Entstehung neuer Handelshemmnisse infolge einer heterogenen Entwicklung der nationalen Rechtsvorschriften vorzubeugen, falls die Entstehung solcher Hemmnisse wahrscheinlich ist und die neuen Regeln ihre Vermeidung bezwecken [vgl. EuGH, Rs. C-376/98, Rn. 86].

Subsidiarität

Abhängig von der Ausgestaltung der Folgemaßnahmen. Das übergeordnete Ziel, das Vertrauen in KI-Anwendungen und die Marktakzeptanz von KI EU-weit zu stärken und eine dynamische und wettbewerbsfähige europäische KI-Industrie zu schaffen, kann durch nationale Initiativen nicht ausreichend erreicht werden.

Sonstige Vereinbarkeit mit EU-Recht

Abhängig von der Ausgestaltung der Folgemaßnahmen. Technologien zur biometrischen Fernidentifikation – insbesondere zur Gesichtserkennung – bergen sehr hohe Risiken für die Grundrechte der überwachten Personen und werden daher von der Datenschutzgrundverordnung (DSGVO) generell verboten. Ihr Einsatz darf nur unter strengen Einschränkungen erlaubt werden, z.B. aus Gründen „erheblichen öffentlichen Interesses“ oder der nationalen Sicherheit; es ist jedoch unklar, wann diese Voraussetzungen erfüllt sind. Da einige Mitgliedstaaten bereits beginnen, die öffentliche Nutzung solcher Technologien zu regulieren, ist es sinnvoll, dass die Kommission eine Debatte anstrebt, um zu einem gemeinsamen Verständnis über die Umstände, die eine solche Nutzung rechtfertigen könnten, und die notwendigen Schutzmaßnahmen zu gelangen.

Zwingende gesetzliche Anforderungen für risikoreiche KI-Anwendungen und freiwillige Anforderungen für risikoarme KI-Anwendungen – wie vorgeschlagen – **respektieren das Verhältnismäßigkeitsprinzip**. Es könnte unverhältnismäßig sein, die zwingenden gesetzlichen Anforderungen auch auf risikoarme KI-Anwendungen zu erstrecken.

Im Weißbuch fehlt eine umfassende Definition von KI; ein künftiger EU-Rechtsakt muss eine solche Definition aber enthalten. Wie das Weißbuch zu Recht hervorhebt, muss diese Definition sowohl präzise genug sein, um Rechtssicherheit zu gewährleisten, als auch flexibel genug, um dem technischen Fortschritt Rechnung zu tragen. **Die im Weißbuch vorgeschlagene Definition von „risikoreich“ ist zwar flexibel, aber nicht klar genug, um Rechtssicherheit zu schaffen.** Insbesondere sollte nicht jede Nutzung einer KI-Anwendung in einem der genannten Sektoren, die eine Rechtswirkung erzeugt, als „risikoreich“ angesehen werden, was die Kommission jedoch zu sagen scheint. Dies sollte nur dann der Fall sein, wenn die Rechtswirkung erheblich genug ist, um sowohl unnötige Belastungen für die Unternehmen als auch eine Diskrepanz mit dem parallelen Kriterium der „Verletzungs- oder Lebensgefahr oder der Gefahr eines erheblichen Schadens“ zu vermeiden. **Zu klären ist, wann mögliche Rechtswirkungen oder Schäden – und damit die mit der Nutzung einer KI-Anwendung verbundenen Risiken – als „erheblich“ anzusehen sind**, weil die Anwendung in diesem Fall u.U. als risikoreich einzustufen wäre. Unklar ist auch, wer über die Einstufung einer KI-Anwendung als risikoreich oder risikoarm entscheidet.

Zusammenfassung der Bewertung

Der vorgeschlagene risikobasierte Ansatz trägt der Tatsache Rechnung, dass die möglichen Folgen für die Nutzer von der spezifischen KI-Anwendung und dem Sektor abhängen, in dem diese eingesetzt wird. Die negativen Auswirkungen einer strengen Regulierung werden reduziert, wenn die Anforderungen nur für risikoreiche KI-Anwendungen gelten. Zwingende gesetzliche Anforderungen für risikoreiche KI-Anwendungen und freiwillige Anforderungen für risikoarme KI-Anwendungen respektieren das Verhältnismäßigkeitsprinzip. Die Definition von „risikoreich“ ist nicht klar genug, um Rechtssicherheit zu schaffen. Zu klären ist, wann die mit der Nutzung einer KI-Anwendung verbundenen Risiken als „erheblich“ anzusehen sind.