Regulierung im Bereich KI-Medizin (AI Act)

Alexandra Jorzig und Luis Kemter

Das Thema künstliche Intelligenz (KI) erlangt immer größere Aufmerksamkeit in der Öffentlichkeit. Das aktuellste Beispiel ist die Nutzung von ChatGPT – ein Programm, das mittlerweile wohl den meisten bekannt sein dürfte – von fast allen Altersgruppen. Das Bundesministerium für Wirtschaft und Energie gab zudem bereits vor knapp drei Jahren an, dass künstliche Intelligenz eine der entscheidenden Schlüsseltechnologien sei.[1] Daher verwundert es nicht, dass künstliche Intelligenz mittlerweile in den verschiedensten Sektoren eingesetzt wird, mitunter auch im medizinischen Bereich. Dort soll deren Einsatz beispielsweise dazu beitragen, auf schnellem und einfachem Wege die Plazenta bei Schwangeren zu vermessen oder aber Zelltypvorhersagen zu treffen, was bei der Entdeckung von Blutkrebs helfen kann; als weitere Einsatzmöglichkeit ist die Mitwirkung von künstlicher Intelligenz bei der Krebsbehandlung mittels Bildanalyse zu nennen.[2] Insofern erweist sich der Einsatz von künstlicher Intelligenz nicht nur für die jeweiligen Ärzte als gewinnbringend, indem diese u.a. zu einer Verringerung der Arbeitsbelastung beitragen kann, sondern ebenso für die Patienten.

Der Einsatz von künstlicher Intelligenz bedarf dabei allerdings genauer Regelungen. Gerade in der Medizin können Fehler von eingesetzten Maschinen nämlich zu einer nicht nur unerheblichen Gefährdung von Menschenleben führen.

Aufgrund dessen soll im Folgenden eine Auseinandersetzung mit dem von der EU geplanten „AI Act"[3], einem Regelungswerk für die Anwendung von künstlicher Intelligenz, unter konkreter Berücksichtigung des medizinischen Sektors erfolgen.

---

1 Bundesministerium für Wirtschaft und Energie, Einsatz von Künstlicher Intelligenz in der Deutschen Wirtschaft (2020), S. 2 (https://www.bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/einsatz-von-ki-deutsche-wirtschaft.pdf?__blob=publicationFile&v=8).

2 Helmholtz, Maschinelles Lernen. Wie KI die Medizin revolutioniert, 2023 (URL: https://www.helmholtz.de/newsroom/artikel/wie-ki-die-medizin-revolutioniert/).

3 COM/2021/206 final.

I. Aktuelle Regelungslage

Derzeit besteht noch kein einheitliches europäisches Regelungswerk, dass sich speziell mit dem Einsatz von künstlicher Intelligenz beschäftigt. Zwar gibt es europäische Vorschriften, welche u.a. die Produkthaftung betreffen und dem Grunde nach auf selbstständig arbeitende Maschinen anwendbar sind. Diese Regelungen sind aber knapp 40 Jahre alt und daher nicht mehr zeitgemäß.[4] Darüber hinaus existieren zwar auch in den Mitgliedsstaaten nationale Haftungsregelungen. Diese gehen aber teilweise auf die veralteten EU-Vorschriften zurück und sind im Ländervergleich unterschiedlich ausgestaltet. Dessen ungeachtet regeln diese Vorschriften schließlich nur die Haftung, sodass eine Regelungslücke hinsichtlich der konkreten Durchführung gerade von künstlicher Intelligenz besteht.

Aus diesen Gründen ist es zu begrüßen, dass sich die EU-Kommission mit dem geplanten Artificial Intelligence Act (AI Act) in Form einer Verordnung mit der komplexen Frage der Regulierung von künstlicher Intelligenz auseinandersetzt.[5] Ziel ist es nach Angaben der EU-Kommission, Risiken, die sich aus der spezifischen Nutzung von künstlicher Intelligenz ergeben, durch ergänzende, verhältnismäßige und flexible Vorschriften zu bewältigen.[6]

Wann der AI Act tatsächlich in Kraft treten wird, ist noch nicht abschließend geklärt. Von Seiten der EU heißt es aber, dass mit einer Anwendbarkeit der finalen Regelungen ab der zweiten Jahreshälfte in 2024 zu rechnen sei.[7] Unabhängig vom tatsächlichen Inkrafttreten werden die Regelungen ab diesem Zeitpunkt noch nicht bindend sein. Vielmehr wird es einen Übergangszeitraum geben, der es den Betroffenen ermöglicht, die neuen Vorgaben entsprechend umzusetzen und mögliche Prozesse anzu-

4 Europäische Kommission, Neue Haftungsvorschriften für Produkte und künstliche Intelligenz zum Schutz der Verbraucher und zur Förderung von Innovation (URL: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_5807).

5 Geminn, Die Regulierung Künstlicher Intelligenz. Anmerkungen zum Entwurf eines Artificial Intelligence Act. ZD 2021, 354 – 359 (354).

6 Europäische Kommission (2022), Ein europäischer Ansatz für künstliche Intelligenz (URL: https://digital-strategy.ec.europa.eu/de/policies/european-approach-artificial-intelligence).

7 European Commission, Regulatory framework proposal on artificial intelligence (https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai)

passen. Gleiches war beispielsweise bei der Datenschutzgrundverordnung (DSGVO)[8] der Fall.

II. Anwendungsbereich AI Act

In dem geplanten AI Act findet sich ein sehr weites Verständnis von Systemen, die unter dem Einsatz von künstlicher Intelligenz arbeiten (KI-Systeme) und die demnach von dem Anwendungsbereich erfasst sein sollen. So heißt es in Art. 3 Nr. 1, dass ein KI-System eine Software ist, „*die mit einer oder mehreren der in Anhang I aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren*". Anhang I, auf den Bezug genommen wird, gibt insgesamt drei Techniken und Konzepte vor. Zu diesen gehören (i) Konzepte des maschinellen Lernens, einschließlich des tiefen Lernens (Deep Learning) (ii) Logik und wissensgestützte Konzepte und (iii) statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

Ausdrücklich ausgenommen von dem AI Act sind aber beispielsweise KI-Systeme, die ausschließlich für militärische Zwecke genutzt werden.[9]

Aufgrund dieser weiten Begriffsdefinition fallen nach derzeitigem Stand wohl auch sämtliche KI-Systeme, die in der Medizin zum Einsatz kommen, in den Anwendungsbereich des AI Acts.

Die Regelungen des AI Acts richten sich an unterschiedliche Adressaten. Betroffen sind nämlich sowohl die Anbieter als auch die Nutzer der genannten KI-Systeme.

Anbieter von KI-Systemen sind stets diejenigen, die ein KI-System entwickeln oder dieses entwickeln lassen, um es unter ihrem Namen oder ihrer Marke in den Verkehr zu bringen oder in Betrieb zu nehmen. Dies kann sowohl entgeltlich als auch unentgeltlich erfolgen.[10] Dabei gilt stets das Marktortprinzip. Daher kommt es für die Anwendbarkeit der Regelungen

8 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119, S. 1.

9 Art. 2 Abs. 3 AI Act.

10 Art. 3 Nr. 1 AI Act.

nicht darauf an, wo die Anbieter ihren Sitz haben. Entscheidend ist vielmehr, dass die KI-Systeme in der EU in Verkehr gebracht oder in Betrieb genommen werden. Daneben reicht es aber bereits auch aus, wenn nur das von den KI-Systemen hervorgebrachte Ergebnis in der EU verwendet wird.[11] Somit sind Hersteller von KI-basierten Medizinprodukten zugleich als Anbieter im Sinne des AI Acts anzusehen.

Nutzer sind hingegen diejenigen, die das KI-System in eigener Verantwortung verwenden, es sei denn, die Verwendung erfolgt im Rahmen einer persönlichen und nicht beruflichen Tätigkeit.[12] Nach dieser Definition sind etwa Kliniken oder Praxen, in denen KI-Systeme zum Einsatz kommen, als Nutzer anzusehen, sodass die nachfolgenden Regelungen auch für diese gelten.

III. Regelungen des AI Acts

Welche Regelungen des AI Acts auf das konkrete KI-System anwendbar sind und welche Pflichten für die Anbieter und Nutzer gelten, ergibt sich anhand der Risikoeinordnung des KI-Systems. So klassifiziert der AI Act die KI-Systeme nämlich in verschiedene Risikogruppen, an die jeweils unterschiedliche Anforderungen gestellt werden. Dabei gilt, dass die einzuhaltenden Anforderungen an die KI-Systeme umso strenger sind, je höher das Risiko ist.

Die erste Risikogruppe betrifft die KI-Systeme, mit denen kein oder nur ein minimales Risiko einhergehen. Hierzu gehören etwa Spam-Filter. KI-Systeme mit besonderen Transparenzpflichten, wie es beispielsweise bei Chatbots anzunehmen ist, fallen in die zweite Risikogruppe („limited Risk"). Darüber hinaus gibt es noch eine dritte Risikogruppe, welche die KI-Systeme mit einem hohen Risiko erfasst („high-risk"). Sofern mit dem KI-System eine eindeutige Bedrohung für die Sicherheit, den Lebensunterhalt und die Rechte von Menschen einhergehen oder wenn diese Social Scorings von Regierungen zum Gegenstand haben, sind diese der letzten Risikogruppe („unacceptable risk") zuzuordnen. Von letzterer Risikogruppe soll auch Spielzeug mit Sprachassistenz erfasst sein, das zu einem gefähr-

11 Art. 2 Abs. 1 AI Act.
12 Art. 3 Nr. 4 AI Act.

lichen Verhalten anregt.[13] Der Einsatz entsprechender KI-Systeme, die dem „unacceptable risk" zuzuordnen sind, wird von dem AI Act untersagt.

Mit Blick auf den medizinischen Sektor ist insbesondere die dritte Risikogruppe („high-risk") von Bedeutung. Dieser Risikogruppe sind alle KI-basierten Medizinprodukte zuzuordnen, die der Klasse IIa oder höher angehören und durch eine benannte Stelle zertifiziert werden müssen. Diese Voraussetzung erfüllen aber nahezu alle in Betracht kommenden Medizinprodukte, die mit künstlicher Intelligenz zum Einsatz kommen können. Das bedeutet zugleich, dass an sämtliche KI-basierten Medizinprodukte nach dem AI Act besonders strenge Anforderungen gestellt werden. Über einige dieser speziellen Regelungen soll im Folgenden ein Überblick verschafft werden.

IV. Anforderungen an die Medizinprodukte

Die Anforderungen, welche an die Hochrisiko-KI-Systeme gestellt werden, werden im Wesentlichen im zweiten Kapitel des AI Acts angegeben.

Artikel 9 gibt zunächst vor, dass für das KI-System ein Risikomanagement eingerichtet, angewandt, dokumentiert und aufrechterhalten werden muss. Dieses Risikomanagement muss während des gesamten Lebenszyklus eines KI-Systems bestand haben. Zugleich muss das Risikomanagement stets aktuell gehalten werden, was eine regelmäßige Aktualisierungspflicht zur Folge hat. Bei der Implementierung eines solchen Risikomanagements gilt es eine Vielzahl von vorgeschriebenen Schritten einzuhalten, zu denen mitunter die Abschätzung und Bewertung möglicher Risiken bedeutet. Übertragen auf ein KI-System aus dem Medizinsektor müsste somit u.a. ermittelt werden, welche Auswirkungen das System auf einen Patienten oder generell auf dessen weitere Behandlung haben könnte, wobei mögliche vorhersehbare Fehlfunktionen in die Ermittlung der Auswirkungen miteinbezogen werden müssen.

Artikel 11 stellt für Hochrisiko-KI-Systeme verschärfte Anforderungen an die technische Dokumentation. So muss die technische Dokumentation erstellt werden, bevor das System in Verkehr gebracht oder in Betrieb genommen wird. Auch hier besteht die Pflicht, die technische Dokumentation stets aktuell zu halten. Im Zusammenhang mit den technischen Do-

13 European Comission, Shaping Europe's digital future (URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai).

kumentationspflichten stehen die in Artikel 12 näher geregelten Aufzeichnungspflichten. Demnach muss während des Betriebs eine Protokollierung erfolgen, anhand derer die Ausführungen über die gesamte Lebensdauer des Systems rückverfolgbar sind.

Eine weitere nennenswerte Regelung ist die in Artikel 14 geregelte Pflicht der menschlichen Aufsicht. Diese soll der Verhinderung bzw. Minimierung von Risiken u.a. der Gesundheit dienen. Die menschliche Aufsicht soll durch entsprechende Vorkehrungen der Anbieter gewährleistet werden. Art. 14 Abs. 3 schreibt dafür u.a. vor, dass die menschliche Aufsicht, sofern technisch machbar, in das Hochrisiko-KI-System eingebaut werden muss. Dies könnte beispielsweise zur Folge haben, dass das KI-System nur dann arbeitet, wenn in regelmäßigen Abständen bestimmte Eingaben durch einen Menschen erfolgen, etwa durch das Drücken gewisser Knöpfe. Dies kann allerdings selbstredend nicht für Maschinen gelten, bei denen die Gesundheit von Menschen gefährdet wird, sollten die Maschinen mangels menschlicher Rückmeldung ihre Arbeit augenblicklich einstellen. Diesbezüglich sind die Hersteller entsprechender KI-Systeme wohl angehalten, neue Lösungsvorschläge zu entwickeln.

Kritik an dieser Regelung kommt aber insbesondere deshalb auf, weil noch ungeklärt sei, was genau unter der „menschlichen Aufsicht" zu verstehen ist. Eine Überwachung in Echtzeit erweise sich nämlich teilweise als unrealistisch, etwa bei Systemen, bei denen im Regelbetrieb automatisiert Steuerungen vorgenommen werden, wie z.B. automatisierte Adaptionen von Maschinenparametern in der Fertigung oder Konfiguration von Medizinprodukten.[14]

Sofern mit der Anwendung des KI-Systems eine biometrische Identifizierung und Kategorisierung von Personen erfolgt, gilt zudem, dass der Nutzer keine Maßnahmen oder Entscheidungen alleine aufgrund des vom System hervorgebrachten Identifizierungsergebnisses treffen darf. Die Entscheidung darf gemäß Artikel 14 Absatz 5 schließlich erst dann erfolgen, wenn das Ergebnis von mindestens zwei natürlichen Personen überprüft und bestätigt wurde.

Als letzte Vorschrift aus den erhöhten Anforderungen an Hochrisiko-KI-Systeme ist Artikel 15 zu nennen. Dieser hat die verschärften Anforderungen an Genauigkeit, Robustheit und die Cybersicherheit der KI-Systeme zum Gegenstand. So muss die Genauigkeit des Systems in Form von sog.

14 Haimerl, Anmerkungen zum Vorschlag für die EU-Verordnung zur künstlichen Intelligenz vom 21. April 2021, S. 8.

„Genauigkeitszahlen" in der beigefügten Gebrauchsanweisung angegeben werden. Zugleich muss das KI-System widerstandsfähig gegen unbefugtes Eingreifen sein.

Sofern das KI-System den genannten Voraussetzungen entspricht, kann dieses grundsätzlich in Verkehr gebracht bzw. in Betrieb genommen werden. Das bedeutet allerdings nicht, dass die Anbieter von weiteren Pflichten entbunden werden. So sieht Artikel 61 weiter vor, dass Anbieter ein System zur Beobachtung nach dem Inverkehrbringen des KI-Systems einrichten müssen, das im Verhältnis zu der Art der KI-Technik und zu den Risiken des KI-Systems steht. Mittels eines solchen Systems soll der Anbieter u.a. zur fortdauernden Einhaltung der zuvor beschriebenen und speziell für Hochrisiko-KI-Systeme vorgesehenen Regelungen imstande sein.

V. Rechtsfolgen bei Verstößen

Der AI Act sieht bei Verstößen gegen die Verordnung Geldbußen von bis zu 30.000.000 Euro oder – sofern es sich um ein Unternehmen handelt und dieser Betrag höher sein sollte – eine Geldbuße von bis zu sechs Prozent des gesamten weltweiten Jahresumsatzes des vorangegangen Geschäftsjahres vor. Die Zahlung dieses Höchstbetrages kann allerdings nur angeordnet werden, sofern entweder ein KI-System zur Anwendung kommt, das nach dem AI Act dem Grunde nach verboten ist, oder aber wenn das KI-System nicht den in Art. 10 des AI Acts beschriebenen Konformitätsanforderungen entspricht. Sofern dies nicht zutrifft, ist aber dennoch eine Geldbuße von 20.000.000 Euro oder von bis zu vier Prozent des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres möglich. Darüber hinaus verpflichtet Artikel 71 die Mitgliedsstaaten der EU, dass diese Vorschriften für Sanktionen erlassen, die bei Verstößen gegen den AI Act zur Anwendung kommen, etwa in Form von Geldbußen.

VI. Verhältnis zur EU-Medizinprodukteverordnung (MDR)[15]

Wie eingangs bereits erläutert, fallen aufgrund des weiten Begriffsverständnisses des AI Acts von einem „KI-System" nahezu alle Systeme, die in der Medizin unter Zuhilfenahme von künstlicher Intelligenz zum Einsatz kommen, in den Anwendungsbereich des AI Acts. Daraus folgt jedoch ein nicht zu unterschätzendes Problem: Die medizinischen KI-Systeme unterliegen in vielen Fällen zugleich den Regelungen der bereits existenten EU-Medizinprodukteverordnung (MDR). Dies liegt daran, dass die Definition des „Medizinproduktes" in der MDR ebenfalls sehr weit gefasst ist. So heißt es in Art. 2 Nr. 1 u.a.: „*‚Medizinprodukt' bezeichnet ein Instrument, einen Apparat, ein Gerät, eine Software (...) oder einen anderen Gegenstand, das dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere der folgenden spezifischen medizinischen Zwecke erfüllen soll: (...) und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann*".

Sofern also ein medizinisches KI-System sowohl unter die Definition in Art. 3 Nr. 1 des AI Acts als auch unter die in Art. 2 Nr. 1 MDR fällt, stellt sich die Frage nach dem Verhältnis dieser Regelungswerke. Dass diese Frage einer endgültigen Klärung bedarf, wird insbesondere mit Blick auf die sich teilweise überschneidenden Regelungen deutlich:

Sowohl von dem AI Act als auch von der MDR werden Nachmarktkontrollen vorgeschrieben. Daher stellt sich hier die Frage, ob nunmehr eine doppelte Nachmarktkontrolle vorgesehen ist. Der Bundesverband Medizintechnologie sieht eine solche doppelte Nachmarktkontrolle jedenfalls als sachlich nicht gerechtfertigt an und fordert zugleich, solchen doppelten Aufwendungen der Hersteller entgegenzuwirken.[16]

Zugleich regeln sowohl der AI Act als auch die MDR die Voraussetzungen, unter denen Behörden eingreifend tätig werden. Auffällig ist dabei,

15 Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/382/EWG und 92/42/EWG des Rates, ABl. EU Nr. L 117, S. 1.

16 BVMed-Stellungnahme zum „Artificial Intelligence Act" (AIA) der EU-Kommission: „Überregulierung vermeiden, Datenzugang ermöglichen" (https://www.bvmed.de/de/bvmed/presse/pressemeldungen/bvmed-stellungnahme-zum-artificial-intelligence-act-aia-der-eu-kommission-ueberregulierung-vermeiden-datenzugang-ermoeglichen).

dass die Eingriffshürden unterschiedlich hoch angesetzt sind. So setzt die MDR mitunter voraus, dass ein Produkt ein „unvertretbares Risiko für die Gesundheit oder Sicherheit der Patienten, Anwender oder anderer Personen oder für andere Aspekte des Schutzes der öffentlichen Gesundheit darstellen kann". Der AI Act lässt hingegen ein Risiko für Aspekte des Schutzes öffentlicher Interessen ausreichen. Insofern liegt die Befürchtung nahe, dass die hohen Eingriffsvoraussetzungen der MDR durch die Anwendung des AI Acts umgangen werden können.

Neben den genannten Aspekten sind auch noch weitere Dopplungen in den Regelungswerken zu erkennen. Dies betrifft u.a. die Cybersicherheit des Systems, das Risikomanagement oder das Meldesystem.

Die Eingangs aufgeworfene Frage nach dem Verhältnis von AI Act und MDR ist bislang noch nicht geklärt. Da dies jedoch bereits mehrfach Gegenstand von Kritik war, ist eine Klarstellung vor Inkrafttreten des AI Acts zu erwarten.

Eine Möglichkeit zur Lösung des Problems wäre dabei, die speziell auf Medizinprodukte ausgelegte MDR hinsichtlich sich überschneidender Regelungen als vorrangig anzusehen. Beispielsweise könnte in Art. 2 des AI Acts, der dessen Anwendungsbereich bestimmt, eine Regelung aufgenommen werden, welche den Vorrang der MDR zum Gegenstand hat. Insofern würden die Regelungen des AI Acts nur dann zur Anwendung gelangen, wenn die MDR keine den Themenbereich betreffende Regelung für medizinische KI-Systeme enthält. Hierzu zählt beispielsweise der oben erwähnte Aspekt der menschlichen Aufsicht.

VII. Fazit

Im Hinblick auf die sich immer weiter entwickelnden KI-Systeme und deren zunehmenden Nutzung ist die Einführung einheitlicher europäischer Regelungen hinsichtlich der Anforderungen, die solche Systeme erfüllen müssen, als durchaus notwendig anzusehen. Der AI Act umfasst aufgrund des weiten Begriffsverständnisses eines KI-Systems auch nahezu jede Form der künstlichen Intelligenz. Kritisch zu betrachten ist jedoch, dass nahezu jedes KI-basierte Medizinprodukt unter die Kategorie der Hochrisiko-Systeme fällt und damit besonders strengen Regelungen unterliegt. Dies kann mitunter dazu führen, dass es zu einem geringeren Einsatz von künstlicher Intelligenz im medizinischen Sektor kommt. Aufgrund der enormen Fortschritte, die gerade in der Medizin mit verschiedenen KI-Systemen

erreicht wurden bzw. noch erreicht werden können, kann dies aber gerade nicht das Ziel eines neues Regelungswerkes sein. Dieses Problem könnte vermieden werden, indem der AI Act der MDR den Vorrang einräumt und nur ergänzend für medizinische KI-Systeme gilt. Insofern bleibt jedoch abzuwarten, inwiefern das erkannte, aber dennoch noch nicht abschließend gelöste Problem des Konkurrenzverhältnisses von AI Act und MDR auf europäischer Ebene gelöst wird.