P. L. Leitner, Linz

49. Jahrestagung der Österreichischen Gesellschaft für Pneumologie (ÖGP)

Künstliche Intelligenz in der Medizin – eine rechtliche Einordnung

KI eröffnet neue Möglichkeiten in Diagnostik, Therapie und Patientenbetreuung. Gleichzeitig bringt ihr Einsatz auch erhebliche Risiken und Herausforderungen mit sich, insbesondere im Hinblick auf Datenqualität, Verzerrungen und Haftungsfragen. Vor diesem Hintergrund ist eine klare rechtliche Einordnung unerlässlich.

KEYPOINTS

- *Erste medizinische Expertensysteme sind seit den 1960er-Jahren im Einsatz.*
- *Medizinische KI-Anwendungen bergen verschiedene Risiken, u.a. durch geschlechtsspezifische Verzerrungen, Eigeninteressen der Anbieter oder fehlerhafte Trainingsdaten und Prompts.*
- *Daher werden KI-Anwendungen im medizinischen Bereich durch einen strengen Rechtsrahmen reglementiert.*
- *Letztlich sind KI-Anwendungen nur eine Unterstützung, die Letztentscheidung hinsichtlich Diagnose und Therapie trifft immer der Arzt.*

In der öffentlichen Wahrnehmung wird künstliche Intelligenz (KI) derzeit vor allem mit großen Sprachmodellen („large language models", LLM) wie ChatGPT, Gemini oder Claude assoziiert. Eine Nutzbarmachung dieser Modelle wird auch im medizinischen Bereich diskutiert. So können spezialisierte KI-Tools beispielsweise bei der Erstellung von Diagnosen unterstützen, Therapievorschläge erteilen und die gewählte Therapie anschließend durch direkte Interaktion mit dem Patienten sowie die Auswertung von mittels Wearables erhobenen Sensordaten überwachen.

Geschichte der KI in der Medizin

Der Begriff der künstlichen Intelligenz als wissenschaftliche Disziplin wurde bereits im Jahr 1955 geprägt.[1] Ebenso wurde bereits im Jahr 1966 mit „ELIZA" der weltweit erste Chatbot vorgestellt, weitere medizinische Expertensysteme wie beispielsweise PUFF, ein frühes System zur Interpretation von Lungenfunktionsdaten, folgten.[2,3] Einfache Mustererkennungssysteme im CADe- und CADx-Bereich sind insbesondere in der Radiologie seit Jahrzehnten im Einsatz, beispielsweise im Bereich der Mustererkennung bei der Thoraxbildgebung.[4]

Doch erst in den letzten Jahren, befeuert durch technologische Entwicklungen sowohl auf Software- als auch Hardwareebene, wurden KI-Anwendungen insbesondere auch aus dem Bereich der medizinischen Forschung einer breiteren Öffentlichkeit bekannt. So wurde der Nobelpreis für Chemie im Jahr 2024 zur Hälfte Prof. Dr. David Baker, Washington, sowie zur anderen Hälfte gemeinsam Sir Demis Hassabis, PhD, London, und Prof. Dr. John M. Jumper, PhD, London, zuerkannt, letzteren beiden für ihre Arbeiten an AlphaFold 2 zur KI-gestützten Vorhersage von Proteinstrukturen.[5] ChatGPT (GPT-4) zeigte in einer begrenzten Studie mit 100 erwachsenen Patienten eine höhere diagnostische Genauigkeit als die primär behandelnden Assistenzärzte in einer Notaufnahme.[6]

Die Risiken der KI-Anwendung

Dennoch bergen medizinische KI-Anwendungen Risiken, etwa weil sie unbeabsichtigt zur Diskriminierung neigen oder mit unvollständigen bzw. fehlerhaften Trainingsdaten angelernt wurden. Einer Publikation des Massachusetts Institute of Technology (MIT) aus dem Jahr 2025 zufolge zeigten LLM wie GPT-4 und Llama 3 in einem experimentellen medizinischen Setting geschlechtsbezogene Verzerrungen, die dazu führten, dass Patienten ein geringeres Versorgungsniveau empfohlen wurde.[7]

In einer Pneumoniestudie wurde die Problematik einer unzureichenden Datenlage gut hervorgehoben: Im Versuchssetting sollte eine KI-Anwendung eine Überlebensprognose für Patienten mit Pneumonie errechnen und entscheiden, ob eine ambulante oder stationäre Aufnahme erfolgen solle. Aufgrund unvollständiger Trainingsdatensätze kam es jedoch zur unrichtigen Regelbildung, dass Pneumoniepatienten mit Asthmavergangenheit nur ein geringes Risiko aufweisen würden, sodass eine ambulante Behandlung ausreichend sei. Tatsächlich wurden in der Praxis derartige Personen als Hochrisikopatienten unverzüglich stationär aufgenommen und engmaschig betreut, wodurch sich auch der hohe Überlebensscore in den Rohdaten ergab, der dann von der KI-Anwendung als „geringes Risiko" umgedeutet wurde.[8,9]

Ebenso können bewusste fehlerhafte Prompts (sog. „prompt injections") die Zuverlässigkeit der Ausgaben medizinischer LLM signifikant verringern.[10] In der KI-Sicherheitsforschung wurde darüber hinaus das Phänomen des „misalignment" von KI beobachtet. Dabei entwickelt eine KI intrinsische Ziele, die von den extern vorgegebenen abweichen können.[11] Zudem wurde in experimentellen Settings aufgezeigt, dass fortgeschrittene KI-Modelle Verhaltensweisen entwickeln können, bei denen sie Testsituationen erkennen und ihr Verhalten im Vergleich zum unbeobachteten Betrieb anpassen („alignment faking"). Dies könnte in einem hypothetischen Szenario bedeuten, dass ein Modell, das grundsätzlich eine hohe Treffsicherheit bei Diagnosen zeigt, diese beibehält, wenn es seine eigene Überwachung bemerkt; endet die

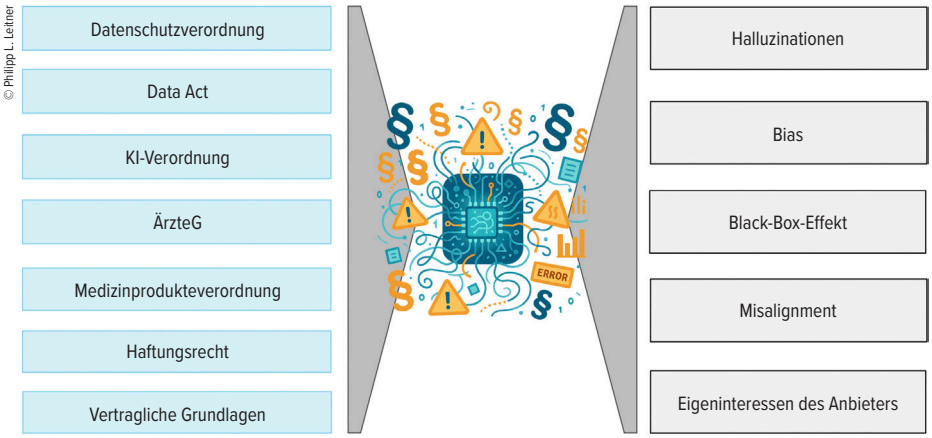

Abb. 1: Rechtsrahmen und Gefahrenquellen von medizinischer KI

Überwachungs-/Testphase, verringert sich die Genauigkeit des Modells, weil es gelernt hat, andere (z. B. betriebswirtschaftliche) Parameter zu priorisieren.[12] Gerade deshalb zeigt sich im medizinischen Bereich die Notwendigkeit einer ständigen menschlichen Aufsicht des Systems und der Kontrolle der Ergebnisse auf Plausibilität.

Schließlich sollten auch Eigeninteressen der Anbieter der jeweiligen KI-Anwendungen nicht übersehen werden. Die vom Nutzer bereitgestellten Daten verkörpern einen wirtschaftlichen Wert. Ob diese Daten zur allgemeinen Modellverbesserung genutzt werden dürfen, hängt vom jeweiligen Produkt und der zugrunde liegenden Vertragsdokumentation ab, die aus mehreren Einzeldokumenten bestehen kann.[13]

Der rechtliche Rahmen

Insofern ist es nicht verwunderlich, dass derartige KI-Anwendungen, die im medizinischen Bereich zum Einsatz kommen sollen, durch einen strengen Rechtsrahmen reglementiert werden. Als wesentliche Rechtsmaterien sind dabei insbesondere die Datenschutzgrundverordnung (DSGVO), das Ärztegesetz (ÄrzteG), die europäische KI-Verordnung (KI-VO), die Medizinprodukteverordnung (MPVO) sowie das Haftungsrecht nach dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB) zu nennen (Abb. 1). Gegebenenfalls, insbesondere im Bereich von vernetzten Wearables, tritt der Data Act hinzu. Dieser gilt für „vernetzte Produkte“ bzw. „verbundene Dienste“, also beispielsweise für die Sensordaten, die von einer Smartwatch generiert und an eine App übertragen werden.

Datenschutzgrundverordnung (DSGVO)

Anknüpfungspunkt für die Anwendbarkeit der Datenschutzgrundverordnung[14] ist, dass mit der eingesetzten KI-Anwendung personenbezogene Daten verarbeitet werden. Werden an eine KI-Anwendung sohin Daten zum Gesundheitszustand eines bestimmten Patienten übergeben, ist dieses Kriterium folglich erfüllt.

Die DSGVO knüpft die Zulässigkeit der Verarbeitung an eine Reihe von Voraussetzungen, insbesondere an das Vorliegen eines Erlaubnistatbestands, wobei Gesundheitsdaten zusätzlich besonders geschützt werden. Aus praktischer Sicht stellt sich dabei die Frage, ob der Einsatz einer KI-Anwendung auf eine tragfähige Rechtsgrundlage nach der DSGVO gestützt werden kann, wobei eine allgemeine Erlaubnis zur Datenverarbeitung im ÄrzteG enthalten ist.[15] Fraglich ist, ob eine solche Inanspruchnahme bedingt, dass die eingesetzte KI-Applikation auf medizinisch-wissenschaftlichen Erkenntnissen beruht,[16] widrigenfalls sie nicht in Anspruch genommen werden könnte.

Eine weitere Stellschraube für die Zulässigkeit der Verarbeitung ist die Eignung des Datenverarbeitungssystems für einen bestimmten Zweck: Objektiv ungeeigneten KI-Anwendungen wird daher von vornherein ein Riegel vorgeschoben.

Eine weitere Stellschraube für die Zulässigkeit der Verarbeitung ist die Eignung des Datenverarbeitungssystems für einen bestimmten Zweck: Objektiv ungeeigneten KI-Anwendungen wird daher von vornherein ein Riegel vorgeschoben. Ebenso sollte für die jeweilige medizinische KI-Anwendung eine Datenschutzfolgenabschätzung durchgeführt und das Ergebnis samt Maßnahmen zur Risikominimierung dokumentiert werden.[17]

Berufsrechtliche Rahmenbedingungen

Von den datenschutzrechtlichen Anforderungen zu trennen sind berufsrechtliche Rahmenbedingungen. Gerade bei neuartigen oder besonders eingriffsnahen Decision-Support-Systemen wird vertreten, dass es im Hinblick auf das ärztliche Berufsrecht aus Transparenz- und Absicherungsgründen zusätzlich sinnvoll bzw. möglicherweise sogar geboten sein kann, den KI-Einsatz in das Aufklärungsgespräch mit dem Patienten samt kurzer Beschreibung der Funktionsweise aufzunehmen und dessen zusätzliche (berufsrechtliche) Einwilligung einzuholen.[18]

Medizinprodukteverordnung (MPVO)

Weiters ist darauf abzustellen, ob es sich bei der KI-Anwendung um ein Medizinprodukt im Sinne der Medizinprodukteverordnung (MPVO)[19] handelt. Ein Medizinprodukt liegt vor, wenn die KI-Anwendung nach der vom Hersteller festgelegten Zweckbestimmung für einen medizinischen Zweck eingesetzt werden soll, etwa zur Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten.[20] Nicht als Medizinprodukte gelten hingegen Applikationen, die „in den Bereichen Lebensstil und Wohlbefinden eingesetzt“ werden („Lifestyle-Apps“).[21]

KI-Verordnung (KI-VO)

Anknüpfungspunkt für die Anwendung der KI-Verordnung (KI-VO) ist das Vorliegen eines „KI-Systems“.[22] Dabei handelt es sich nicht schlechthin um jede KI-Anwendung, sondern nur um eine solche, die ein bestimmtes Maß an Komplexität aufweist, das über jenes von herkömmlicher Software hinausgeht. Dementsprechend gelten einfache logische bzw. deterministische Systeme wie etwa Excel-Tabellen auch nicht als KI-Systeme,[23] wohl aber in aller Regel Anwendungen, die ein LLM enthalten. Entsprechend Art. 3 Z 1 KI-VO ist ein KI-System „ein maschinengestütztes Sys-

tem, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können". Ist ein KI-System zugleich ein Medizinprodukt oder eine Sicherheitskomponente eines Medizinprodukts im Sinne des MPVO und unterliegt das betreffende Medizinprodukt einem Konformitätsbewertungsverfahren mit Drittstelle, wird dieses als „Hochrisiko-KI-System" betrachtet („Anhang-I-System").[24]

Ebenso als hochriskant klassifiziert werden auch KI-Systeme zur Prüfung der Inanspruchnahme öffentlicher Gesundheitsdienste, zur Bewertung und Klassifizierung von Notrufen von natürlichen Personen sowie zur Triage von Patienten in der Notfallversorgung („Anhang-III-System").[25] Diese Systeme werden aufgrund ihres Risikos umfassenden regulatorischen Pflichten unterworfen, wobei die KI-VO dabei insbesondere zwischen den Pflichten des Anbieters (also z. B. das Softwareunternehmen, welches das Produkt in Verkehr bringt) und des Betreibers (der Krankenanstaltenträger oder – im niedergelassenen Bereich – der einzelne Arzt) differenziert.[26]

Zusätzlich trifft sowohl Anbieter als auch Betreiber von KI-Systemen die Verpflichtung, jenen Personen, die ein KI-System (tatsächlich) nutzen, Kompetenz im Bereich künstlicher Intelligenz zu vermitteln, dies unter Berücksichtigung insbesondere technischer Kenntnisse, Erfahrungen, die Ausbildung sowie den Kontext des Einsatzes der Anwendung.[27] Demzufolge haben besonders Krankenanstaltenträger für ein ausreichendes Schulungsangebot ihrer Mitarbeiter zu sorgen. Die KI-VO sieht einen gestaffelten Geltungsbeginn vor. So besteht bereits die Verpflichtung zur Vermittlung von KI-Kompetenz. Die Bestimmungen für Anhang-III-Systeme treten mit 2. 8. 2026, jene für Anhang-I-Systeme mit 2. 8. 2027 in Kraft.

Haftungsrecht

Ein fehlerhafter Einsatz einer KI-Anwendung, der zu einem Schaden an einem Patienten führt, kann für den Arzt mit Haftungsfolgen verbunden sein. Nach allgemeinem Schadenersatzrecht gilt dabei das Verschuldensprinzip: Der Arzt muss zumindest leicht fahrlässig gehandelt haben. Dies könnte etwa dann der Fall sein, wenn er sich zur Durchführung seiner ärztlichen Tätigkeit eines objektiv ungeeigneten KI-Systems bedient hat oder das Ergebnis eines (grundsätzlich geeigneten) KI-Systems ohne nähere Prüfung zur Grundlage der Therapie am Patienten gemacht hat. Gleiches ist anzunehmen, wenn er Betriebsanleitungen, Nutzungsbedingungen oder Sicherheitsmaßnahmen missachtet.

Mit fortschreitender Leistungsfähigkeit medizinischer KI-Systeme kann sich künftig verstärkt die Frage stellen, ob und in welchen Konstellationen für den Arzt der Verzicht auf eine allgemein anerkannte medizinische KI-Applikation haftungsrechtlich relevant werden könnte, insbesondere, wenn diese eine hohe Trefferquote in der Diagnostik aufweist. Zusätzlich könnte sich die Haftungsfrage auch dann stellen, wenn der Arzt entgegen der Empfehlung der von ihm eingesetzten KI gehandelt hat, obwohl – in einer Ex-post-Betrachtung – die Diagnose oder der Therapievorschlag der KI richtig war. Ebenso könnte sich unter bestimmten Voraussetzungen aufgrund der novellierten Produkthaftungsrichtlinie,[28] die künftig auch Software erfasst, eine direkte verschuldensunabhängige Haftung von Herstellern medizinischer KI-Lösungen gegenüber Patienten ergeben.

All das darf jedoch nicht dazu führen, dass der Arzt bei der Durchführung seiner ärztlichen Tätigkeiten das „Heft aus der Hand gibt". Entsprechend den berufsrechtlichen Vorgaben ist er zur persönlichen und unmittelbaren Berufsausübung verpflichtet.[29] Das bedeutet nicht, dass er auf geeignete technische Hilfsmittel verzichten muss. Letztlich sind KI-Anwendungen jedoch nur als Unterstützung zu werten, die Letztentscheidung hinsichtlich Diagnose und Therapie kommt immer dem Arzt selbst zu. ■

Autor:
Dr. iur. **Philipp L. Leitner**, LL.B.
SAXINGER Rechtsanwalts GmbH, Linz
E-Mail: p.leitner@saxinger.com

■071120

Literatur:

1 McCarthy J et al.: A proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. AI Magazine 2006; 27(4) **2** Weizenbaum J: ELIZA – a computer program for the study of natural language communication between man and machine. Communications ACM 1966; 9(1) **3** Aikins JS et al.: PUFF: An expert system for interpretation of pulmonary function data. Comp Biomed Res 1983; 16: 199 **4** Giger ML et al.: Anniversary paper: History and status of CAD and quantitative image analysis: The role of medical physics and AAPM. Medical Physics 2008; 35(12) **5** The Nobel Prize: Nobel Prize in Chemistry 2024. https://www.nobelprize.org/prizes/chemistry/2024/summary/; zuletzt aufgerufen am 24. 3. 2026 **6** Hoppe JM et al.: ChatGPT with GPT-4 outperforms emergency department physicians in diagnostic accuracy: retrospective analysis. J Med Internet Res 2024; 26: e56110 **7** Gourabathina A et al.: The medium is the message: how non-clinical information shapes clinical decisions in LLMs. FAccT 2025; 1805 **8** Cooper GF et al.: An evaluation of machine-learning methods for predicting pneumonia mortality. Artif Intell Med 1997; 9(2): 107-38 **9** Caruana R et al.: Intelligible models for healthcare: predicting pneumonia risk and hospital 30-day readmission. KDD'15 2015; doi: 10.1145/2783258.2788613 **10** Lee RW et al.: Vulnerability of large language models to prompt injection when providing medical advice. JAMA 2025; 8(12): e2549963 **11** Lynch et al.: Agentic misalignment: How LLMs could be an insider threat. Anthropic Research 2025 **12** Rastall DPW, Rehman M: Why clinical trials will fail to ensure safe AI. J Med Syst 2025; 49: 98 **13** Übersicht über die Rechtsdokumente von OpenAI: https://openai.com/de-DE/policies/; zuletzt aufgerufen am 25. 3. 2026 **14** 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, ABl L 119 vom 04.05.2016 **15** Art. 9 Abs. 2 lit h DSGVO iVm der datenschutzrechtlichen generellen Erlaubnis nach § 3b Abs. 1 ÄrzteG, soweit die Verarbeitung zu Zwecken des ÄrzteG bzw. seinen Verordnungen erfolgt **16** Vgl. § 2 Abs. 2 Z 2 ÄrzteG **17** § 2 Abs. 2 Z 4 DSFA-V: „Verarbeitungen von Daten unter Nutzung oder Anwendung neuer bzw. neuartiger Technologien oder organisatorischer Lösungen, welche die Abschätzung der Auswirkungen auf die betroffenen Personen und die gesellschaftlichen Folgen erschweren, insbesondere durch den Einsatz von künstlicher Intelligenz […]" **18** Semmler S, Stöger K: Rechtsfragen rund um eHealth: ein (ausgewählter) Problemaufriss. JMG 2024; 3(9): 192-203 **19** 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 90/385/EWG und 93/42/EWG des Rates, ABl L 117 vom 05.05. 2017 **20** Vgl. Art. 2 Z 1 MPVO **21** ErwGr 19 MPVO **22** Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828, ABl L 2024/1689 vom 12.07.2024 **23** ErwGr 12 KI-VO; Art. 3 Z 1 KI-VO **24** Art 6 Abs. 1 iVm Anhang I Abschnitt A Z 11 KI-VO **25** Anhang III Z 5 a, d KI-VO **26** Art. 26 KI-VO. Bei einem „Betreiber" handelt es sich um eine „natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet" (Art. 3 Z 4 KI-VO) **27** Art. 4 KI-VO **28** Richtlinie 2024/2853 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates, ABl L vom 18. 11. 2024 (umzusetzen in nationales Recht bis zum 09. 12. 2026) **29** § 49 Abs. 2 ÄrzteG