



Dr. Maximilian Poretschkin leitet die Abteilung „AI Assurance and Assessment“ am Fraunhofer IAIS und berät in dieser Funktion weltweit Unternehmen und Behörden zu vertrauenswürdiger KI. Seine Forschungsinteressen umfassen die informatische Operationalisierung rechtlicher Anforderungen, die Entwicklung von KI-Prüfmethoden, -kriterien und -werkzeugen sowie die Erarbeitung von KI-Governance Frameworks. Insbesondere hat er einen der ersten KI-Prüfkataloge entwickelt. Er studierte Physik und Mathematik in Bonn und Amsterdam.

Dr. Maximilian Poretschkin

Die Europäische KI-Verordnung: technische Realisierung rechtlicher Anforderungen

Mit dem Inkrafttreten der KI-Verordnung im August 2024 hat die Europäische Union einen neuen regulatorischen Rahmen für den Einsatz von künstlicher Intelligenz (KI) geschaffen. Die Versicherungsbranche ist dabei nicht nur am Rande betroffen – im Gegenteil: Einige ihrer digitalen Kernprozesse könnten künftig unter die Kategorie „Hochrisiko-KI-Systeme“ fallen.

Dazu zählen nach Anhang III der Verordnung insbesondere KI-Systeme, die für die Risikobewertung und Preisbildung in Bezug auf natürliche Personen im Falle von Lebens- und Krankenversicherungen eingesetzt werden. Weitere Hochrisikosysteme finden sich möglicherweise in den internen Prozessen von Versicherern, etwa im Recruiting oder der Personalentwicklung.

Ein risikobasierter Rechtsrahmen

Die KI-Verordnung verfolgt einen risikobasierten Ansatz. Systeme mit inakzeptablem Risiko – etwa manipulative KI zur Verhaltenssteuerung – werden verboten. Hochrisikosysteme sind grundsätzlich zulässig, müssen jedoch strenge Anforderungen erfüllen: Neben organisatorisch-prozessualen Anforderungen wie der Einrichtung eines Qualitäts-

management- und Risikomanagementsystems sind auch umfangreiche technische Anforderungen in den Bereichen Datenqualität, Genauigkeit, Robustheit und Cybersicherheit zu beachten.

Die Herausforderung: technische Operationalisierung rechtlicher Anforderungen

Insbesondere bei der technischen Operationalisierung der Anforderungen kommt Aktuaren eine besondere Mitverantwortung zu, denn sie sind etwa für die Wahl von Modelltypen oder die Festlegung von Schwellenwerten zuständig.

Das ist im Grundsatz für Aktuare nichts Neues. Schon mit der Datenschutz-Grundverordnung (DSGVO) oder Solvency II mussten komplexe regulatorische Anforderungen

in fachliche Prozesse und statistische Modelle überführt werden. Doch im Fall der KI-Verordnung ist die Unsicherheit bislang deutlich größer – nicht zuletzt, weil viele Begriffe offenbleiben oder Interpretationsspielräume lassen.

Unklare Begriffe und unscharfe Anforderungen

Ein zentrales Beispiel ist hier die Definition von „künstlicher Intelligenz“. Die KI-Verordnung orientiert sich an der Definition der OECD und hat die Fähigkeit zur Ableitung als zentrales Erkennungsmerkmal. Ein viel diskutierter Grenzfall ist in diesem Zusammenhang die logistische Regression

„Die KI-Verordnung verlangt von den Unternehmen, rechtliche Prinzipien wie Fairness, Transparenz und Nachvollziehbarkeit in technische Systeme zu übersetzen.“

– als konkretes Beispiel denke man etwa an die Vorhersage des Eintritts von Berufsunfähigkeit basierend auf der Versicherung vorliegenden Features der betreffenden Person. Je nach Perspektive kann diese als Machine-Learning Verfahren betrachtet werden (und fällt als solches in die Definition der KI-Verordnung) oder, da in vielen Fällen der funktionale Zusammenhang bereits grundsätzlich fixiert ist bzw. die Variablen durch menschliche Experten ausgewählt worden sind, als regelbasiertes System, das zudem nicht über einfache Datenverarbeitung hinausgeht, womit es nicht als KI im Sinne der KI-Verordnung zählen würde. Die im Februar 2025 von der EU-Kommission veröffentlichten (rechtlich nicht bindenden) „Guidelines on the definition of an artificial intelligence system established by AI Act“

haben durch unglückliche Formulierungen auch nicht die gewünschte Klarheit geschaffen.

Ein weiteres Beispiel sind die Anforderungen an die Datenqualität, wie sie in Artikel 10 formuliert sind: „Die Trainings-, Validierungs- und Testdatensätze müssen im Hinblick auf die Zweckbestimmung relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig sein.“

Unklar ist beispielsweise in diesem Zusammenhang, was genau mit Repräsentativität gemeint ist und unter welchen Umständen dies hinreichend erfüllt ist. Weiterhin müssen Trainings-, Validierungs- und Testdaten in Hinblick auf mögliche Verzerrungen geprüft werden, die zu einer verbotenen Diskriminierung führen könnten. Unklar ist aber noch, welche Fairnessmetrik bzw. das hiermit verbundene Fairnesskonzept geeignet sein könnten, um diese Anforderung zu erfüllen.

Ähnliche Unklarheiten findet man zudem für die Anforderungen an Transparenz (Artikel 13) sowie Genauigkeit und Robustheit (Artikel 15).

Konkretisierung der KI-Verordnung durch weitere Dokumente

Die KI-Verordnung wird zurzeit durch weitere Dokumente zur Operationalisierung ergänzt: Allen voran sind die harmonisierten Normen zu nennen, die von der EU-Kommission beauftragt worden sind und aktuell vom JTC 21 erarbeitet werden. Im Fall der harmonisierten Normen gilt die Konformitätsvermutung, das heißt, es wird angenommen, dass KI-Anwendungen, die mit diesen Normen übereinstimmen, die Anforderungen der KI-Verordnung erfüllen. Neben den harmonisierten Normen werden weitere Begleitdokumente erarbeitet, welche die KI-Verordnung zusätzlich konkretisieren. Herausfordernd ist in diesem Zusammenhang, dass



Weiterführende Literatur

(Auswahl mit Fokus auf Datenqualität):

Bundesamt für Sicherheit in der Informationstechnik, QAIDAL – Qualitätskriterien für Trainingsdaten im KI-Lebenszyklus, 2025: stellt einen Bewertungsrahmen für Qualitätskriterien von Trainingsdaten im KI-Lebenszyklus vor.

Feldkamp/Kappler/Poretschkin/Schmitz/Weiss, Rechtliche Fairnessanforderungen an KI-Systeme und ihre technische Evaluation, Zeitschrift für Digitalisierung und Recht, 2024: stellt eine juristisch-informatischen Analyse zur Interpretation und Operationalisierung der fairnessbezogenen Anforderungen an die verwendeten Daten gem. Art. 10 KI-VO für den konkreten Fall von Kredit-scoring-Systemen vor.

Schmitz/Poretschkin, Analyzing the baseline for harmonized standards – a systematic review of standards on bias and data quality, Proceedings of AICOM International Workshop on AI Value Engineering and AI Compliance Mechanisms, 2024: führt eine systematische Analyse aller internationalen Standards zu Datenqualität durch und diskutiert die Konsequenzen für die Operationalisierung der KI-Verordnung.

Wahlster/Winterhalter (Hrsg.), Deutsche Normungsroadmap Künstliche Intelligenz (Ausgabe 2), DIN, DKE, 2022: bietet einen Überblick über die KI-Standardisierungslandschaft und diskutiert insbesondere die Bedarfe des Finanzsektors.



↑ Eingang Fraunhofer IAIS

Foto: Fraunhofer_IAIS

viele dieser Dokumente aktuell noch nicht verfügbar sind, während Unternehmen sich bereits jetzt in der Umsetzung befinden. Zudem zeigt das obige Beispiel der KI-Definition, dass auch die zusätzlichen Dokumente nicht immer die erforderliche Klarheit schaffen. Dies wirft erneut die Frage auf, wie die Operationalisierung der rechtlichen Anforderungen auf technischer Ebene gelingt.

„Ein zentraler Erfolgsfaktor zur Herstellung einer holistischen Perspektive ist das Finden einer gemeinsamen Sprache.“

Lösungsansätze zur weiteren Konkretisierung

Im Folgenden stellen wir vor, wie die Vorgaben der KI-Verordnung weiter konkretisiert werden können:

Zahlreiche technische ISO/IEC-Normen konkretisieren Begriffe aus der KI-Verordnung, etwa Repräsentativität oder Relevanz im Bereich der Datenqualität, und können daher zur Konkretisierung herangezogen werden. Zudem plant auch das JTC 21 eine Adaption einiger bestehender internationaler Standards.

Eine Analyse bestehender bzw. sich in Entwicklung befindender Normen und Standards kann daher bei der Operationalisierung der KI-Verordnung hilfreich sein. Während prozessual-organisatorische Normen, wie etwa die 27000er-Reihe zur Etablierung von Informationssicherheitsmanagementsystemen bereits heute in Versicherungen etabliert sind, ist die Anwendung technischer Normen anders als in Branchen, die beispielsweise Safety-Vorgaben umsetzen müssen, weniger verbreitet. Ein diesbezüg-

licher Kompetenzaufbau scheint daher sinnvoll. Darüber hinaus haben viele Organisationen und Aufsichtsbehörden Guidelines und Whitepaper veröffentlicht, die oben angesprochene Konzepte mit Leben füllen und wertvolle Hilfestellung für die Praxis liefern.

Dort, wo die in den Guidelines und Standards zur Verfügung gestellten Informationen nicht für eine vollständige Operationalisierung ausreichen, können interdisziplinäre Untersuchungen von konkreten Use Cases an der Schnittstelle von Recht, Informatik und Statistik Abhilfe schaffen. Ein zentraler Erfolgsfaktor zur Herstellung dieser holistischen Perspektive ist das Finden einer gemeinsamen Sprache, da Informatik und Statistik stark quantitativ getrieben sind und die Qualität von KI-Systemen mit Metriken beurteilen, während die Rechtswissenschaft vor allem sprachliche Beschreibungen des Regulierungsgegenstands bevorzugt und sich oftmals mit quantitativen Anforderungen schwer tut, weswegen die Fokussierung auf möglichst konkrete Beispiele in diesem Fall hilfreich ist.



Fazit

Die KI-Verordnung markiert den Beginn einer neuen regulatorischen Ära – auch und gerade für die Versicherungsbranche. Sie verlangt von den Unternehmen, rechtliche Prinzipien wie Fairness, Transparenz und Nachvollziehbarkeit in technische Systeme zu übersetzen. Wichtig ist, rechtzeitig mit der Analyse zu beginnen, Standards und Guidelines sinnvoll zu nutzen und interdisziplinäre Zusammenarbeit zu fördern – zwischen Aktuariat, IT, Data Science, Recht und Compliance. Wer diesen Weg frühzeitig einschlägt, wird nicht nur regulatorisch gut aufgestellt sein, sondern kann auch das Vertrauen in KI-gestützte Prozesse nachhaltig stärken.