ZfRM
06.24
5. Jahrgang
Dezember 2024
S. 141 – 168

Zeitschrift für RISIKOMANAGEMENT

Praxiswissen risikobasierte Unternehmensführung

www.ZfRMdigital.de

Künstliche Intelligenz im Risk Management:

Technik, Praxis, Regulierung

ESV ERICH SCHMIDT VERLAG
100 Jahre

EU AI Act

KI-Gesetz erfasst Risikomodelle der Finanzbranche

Jan Esser · Dr. Ute Vellbinger

Jan Eßer
Managing Consultant bei PPI und spezialisiert auf Data & Analytics, KI-Anwendungen sowie auf Risikomanagement und die Entwicklung von Ratingmodellen

Dr. Ute Vellbinger
Managing Consultant bei PPI, Entwicklerin von Ratingmodulen aus methodischer und datentechnischer Sicht

Wo fängt Künstliche Intelligenz an? Laut der Europäischen Union bereits dort, wo einfache statistische Modelle Zinsen für die Kredite einer Bank oder Prämien für eine Versicherung berechnen. Da der EU AI Act diese Anwendungsbereiche in die Risikoklasse hoch einordnet, werden zukünftig auch logistische Regressionsmodelle als hochriskante KI-Systeme gewertet. Das ist die gleiche Kategorie, in die auch komplexe KI-Anwendungen fallen, wie etwa neuronale Netze. Auf die Finanzbranche kommen deshalb erhebliche Aufwände zu, die sich ironischerweise mit KI zumindest teilweise auffangen lassen.

Mit dem AI Act will die EU verhindern, dass Künstliche Intelligenz dafür verwendet wird, um Missbrauch zu betreiben oder jemanden zu diskriminieren. Beispielsweise soll es verboten sein, dass Unternehmen mithilfe von KI solche Modelle entwickeln, die ein gewünschtes soziales Verhalten honorieren (Social Scoring). Als besonders abschreckend gilt etwa das System, das in China dafür sorgen soll, dass sich die Bürger so verhalten, wie von der Staatsführung erwartet. Zwar hat das renommierte MIT Technology Revue inzwischen darauf hingewiesen, dass es so ein System gar nicht gibt. Vielmehr arbeite es ähnlich wie die Schufa hierzulande. Doch die Angst vor der Black Box ist groß, weil sich selten hundertprozentig nachvollziehen lässt, wie eine KI entscheidet.

Was jetzt gilt

Solche Risiken etwa, die sich nach Ansicht der EU kaum kontrollieren lassen, fallen künftig in die Kategorie „inakzeptabel“ und werden verboten. Bei einem hohen Risiko bleibt der KI-Betrieb zwar weiterhin erlaubt, unterliegt aber strengen Vorgaben. Eine KI, die Lebensläufe scannt und in eine Reihenfolge bringt, gehört etwa dazu, weil die Gefahr besteht, dass die KI einzelne Bewerber aufgrund ihrer Hautfarbe, ihres Namens oder ihrer Herkunft diskriminiert und andere Bewerber vorzieht. Dieses Risiko ähnelt dem, das sich ergibt, wenn eine KI mit darüber entscheidet, wie hoch die Zinsen für einen Kredit ausfallen oder wie viel jemand bezahlen muss, der sich versichern lassen möchte.

Ob und inwiefern ein Unternehmen vom EU AI Act betroffen ist, lässt sich auf der offiziellen Webseite der EU feststellen. Ein vereinfachter Onlinetest soll zeigen, in welche Kategorie — inakzeptabel, hoch oder unbedenklich — die eigenen Anwendungen fallen. Wer beispielsweise Spielzeug herstellt und vermarkten möchte, das KI enthält, gilt als „Provider“ und muss eine ganze Reihe von Vorschriften einhalten, weil er mit diesem Angebot als hochriskant im Sinne des EU AI Acts eingestuft wird. Das Unternehmen ist verpflichtet:

- Ein Risikomanagement einzurichten (gemäß Artikel 9)
- Hochwertige Daten einzusetzen, um das System zu trainieren, zu testen und zu validieren (gemäß Artikel 10)
- Dokumentationen durchzuführen und Protokolle zu den Designentwürfen zu führen (gemäß Artikel 11 und 12)
- Nutzer darüber zu informieren, was das System tut, und ein angemessenes Maß an Transparenz dafür zu gewährleisten (Artikel 13)
- Menschliche Kontrollen des KI-Systems zu ermöglichen und in das System zu integrieren und/oder sicherzustellen, dass diese Maßnahmen von den Nutzern umgesetzt werden können (Artikel 14)
- Das System daraufhin zu untersuchen, ob es robust, genau und sicher im Sinne von Cybersicherheit arbeitet (Artikel 15)
- Ein Qualitätsmanagement einzurichten (Artikel 17)

Derselbe Aufwand entsteht jedoch auch bei simplen Modellen, wie etwa der logistischen Regres-

sion. Hinter diesem Ausdruck verbergen sich Modelle, die beispielsweise zur Prognose eingesetzt werden, mit welcher Wahrscheinlichkeit ein Kredit ausfällt oder ein Schadenfall bei einer Versicherung eintritt. Davon wiederum hängt ab, welchen Preis die Kunden zu zahlen haben, also entweder der Zins für den Kredit oder die Prämie, um das Auto oder die Wohnung zu versichern. Die beiden wesentlichen Kennzahlen bei Krediten heißen PD (Probability of Default) und LGD (Loss given Default). Sie zeigen an, wie wahrscheinlich es ist, dass die Rückzahlung platzt und wie hoch der finanzielle Schaden wäre.

Etwas überspitzt formuliert, müssen die Banken und Versicherungen jetzt auch einfache statistische Modelle so behandeln, als hätten sie ein hochgradig komplexes IT-System geschaffen, das ähnlich zu Missbrauch neigen könnte wie eine KI-Anwendung. Allein die für ein KI-System geforderte Transparenz führt in diesem Fall dazu, dass die Finanzbranche weit mehr als bisher zu dokumentieren hat, repräsentative Datensätze nachweisen und eine Art KID (Kundeninformationsdokument) erstellen muss, das darüber aufklärt, dass die Nutzer womöglich mit einer KI interagieren. Sie müssen zudem die Hauptmerkmale, Funktionen und Einschränkungen ihrer Systeme dokumentieren, als handelte es sich um ein komplexes KI-System.

Enges Zeitfenster

Erschwerend kommt hinzu, dass der EU AI Act bereits am 1.8.2024 in Kraft getreten ist und schon nach zwei Jahren angewendet werden soll. Doch Vorsicht: Die Unternehmen sind auch dazu verpflichtet, einen Fahrplan zu entwickeln, der beschreibt, wie sie künftig mit KI umgehen wollen. Dieser Verhaltenskodex soll nach neun Monaten vorliegen, spätestens also am 2.4.2025. Das Problem: Viele Entscheider wird überraschen, dass sie sich damit beschäftigen müssen. Eine Umfrage des Branchenverbandes Bitkom zeigt, dass drei Viertel der Betriebe noch gar nichts unternommen haben, was den EU AI Act angeht. 69 Prozent der befragten Unternehmen gehen davon aus, dass sie Hilfe brauchen werden, um die Vorgaben umzusetzen.

Wie viel Unterstützung sie brauchen, legt eine Umfrage von Adesso nahe. Kaum ein Drittel der Entscheider kennen demnach die Inhalte aus dem EU AI Act. Sie laufen damit auch Gefahr, dass sie die KI-Systeme, die sie derzeit entwickeln, erst verspätet einsetzen können oder schlimmstenfalls, wenn sie als inakzeptables Risiko eingestuft werden, gar nicht mehr. Entsprechend unsicher reagieren die Unternehmen auf den neuen Gesetzvorstoß. Wie Deloitte ermittelt hat, glaubt jeder zweite Manager, dass der EU AI Act das eigene Unternehmen darin beeinträchtigt, sich mit KI zu beschäftigen und KI einzuführen. Darüber hinaus bestätigt sich, was Bitkom bereits herausgefunden hat: Zu wenige Unternehmen beschäftigen sich aktiv mit dem EU AI Act.

Wie riskant es ist, das Thema auf die lange Bank zu schieben, zeigt ein Blick auf die Strafen, die drohen, falls ein Unternehmen gegen den EU AI Act verstößt. Denn die fallen ähnlich drakonisch aus wie schon bei der DSGVO: Wer ein unerlaubtes KI-System einsetzt, muss mit bis zu 35 Millionen Euro Strafe oder sieben Prozent des Jahresumsatzes rechnen. Verstöße gegen die verschiedenen Anforderungen und Verpflichtungen können sich auf bis zu 15 Millionen Euro oder drei Prozent des weltweiten Jahresumsatzes summieren. Falsche, unvollständige oder irreführende Informationen schlagen mit 7,5 Millionen Euro oder 1,5 Prozent des Jahresumsatzes zu Buche. Hinzu kommen Kumulrisiken bei mehreren oder sich wiederholenden Verstößen.

Mehr und mehr Banken und Versicherungen werden sich vor diesem Hintergrund kurzfristig mit dem EU AI Act auseinandersetzen müssen und sich fragen, wie sich die Regeln auf ihre IT und die eingesetzte Software auswirkt. Sollten sie dabei entdecken, dass sie verbotene KI-Tools nutzen, müssen sie diese bereits innerhalb von sechs Monaten — also bis zum 2.3.2025 — abschalten, um sich möglichen Strafzahlungen zu entziehen. Viel Zeit bleibt also nicht mehr, zumal sich die betroffenen Finanzkonzerne auch überlegen müssen, wie sie mit dem zusätzlichen Aufwand umgehen wollen, den das Gesetz ihnen auferlegt.

Die Unternehmensberatung zeb geht bereits davon aus, dass Banken und auch die Schwesterbranche Versicherungen bis 2030 bis zu 30 Prozent ihrer Mitarbeitenden verlieren, vor allem deshalb, weil sie in den Ruhestand gehen und wenig Nachwuchs bereitsteht. Demnach wird sich diese Entwicklung auch nicht linear abspielen, sondern zunehmend beschleunigen, bis schließlich jede 14. Stelle unbesetzt bleibt. Diese „Effizienzlücke“ müssen Banken und Versicherungen schließen,

wenn sie weiterhin wettbewerbsfähig bleiben wollen. Ausgerechnet KI könnte sich als Rettungsanker erweisen, um die bestehenden Fachkräfte von Fleißarbeiten zu entlasten, die durch die regulatorischen Vorgaben entstehen.

Wie KI doch hilft

Einige Fintechs machen es vor, wie es gehen kann. Klarna beispielsweise hat erst vor Kurzem verkündet, dass KI bereits zwei Drittel der Kundenanfragen eigenständig bearbeitet. Mehr als zehn Millionen US-Dollar will das Unternehmen zudem jährlich im Marketing einsparen, indem es stärker auf KI setzt. In einem Podcast hat die DZ Bank bereits klargestellt, dass auch für die großen Institute kein Weg an KI vorbeiführt. Die ING analysiert etwa mit KI, was die Kunden der Bank an Feedback geben. Bei den Sparkassen soll ein „KI-Pilot" entstehen, um die Kunden zu unterstützen. Es ist also keinesfalls so, dass sich die Branche erst noch wachküssen lassen muss. Es geht derzeit vor allem darum, geeignete Use Cases zu finden, die sich für KI eignen. Drei Regeln zeichnen sich dabei ab.

1. KI wird vor allem dort helfen, wo es darum geht, massenhaft auftretende und vor allem wiederkehrende Aufgaben zu lösen, etwa im Kundenservice.
2. KI wird – unter anderem wegen der Regulatorik – nur nach besonderer Prüfung in den Kernprozessen einer Bank oder einer Versicherung eingesetzt werden können. Jedenfalls dann, wenn dort sensible Daten verarbeitet werden.
3. KI kann als Sparringspartner für bestehende Verfahren eingesetzt werden und diese unterstützen.

KI eignet sich beispielsweise, um erforderliche Dokumentationen durchzuführen, Testdaten zu generieren und damit zusammenhängende Tests abzuwickeln sowie als Schnittstelle gegenüber dem Kunden, um Self-Service-Angebote zu schaffen, die sonst von knappen Fachkräften ausgeführt werden müssten. Insbesondere für solche Aufgaben lassen sich bereits trainierte Modelle nutzen, was es deutlich leichter macht, KI zu erproben. Wenn es darum geht, KI in bestehenden Prozessketten einzusetzen, sollten Banken und Versicherungen eigenes Know-how aufbauen und ein passendes Vorgehensmodell einsetzen. AVE ist ein solches Modell, das sich vor allem darauf konzentriert, den Prozess im Risikocontrolling teilweise zu automatisieren und somit Mitarbeitende effizient zu unterstützen (Abbildung 1).

Das Vorgehensmodell berücksichtigt, wie sich KI in jedem einzelnen Schritt eines typischen Modellrisikomanagements einsetzen lässt. Moderne Sprachmodelle, die Large Language Models (LLM), helfen Mitarbeitenden etwa dabei, zeitintensive Aufgaben, die zudem häufig wiederkehren, mög-

KI-Unterstützung im automatisierten Risikocontrolling mit AVE, der Automatisierungsprozess für Validierung und Entwicklung

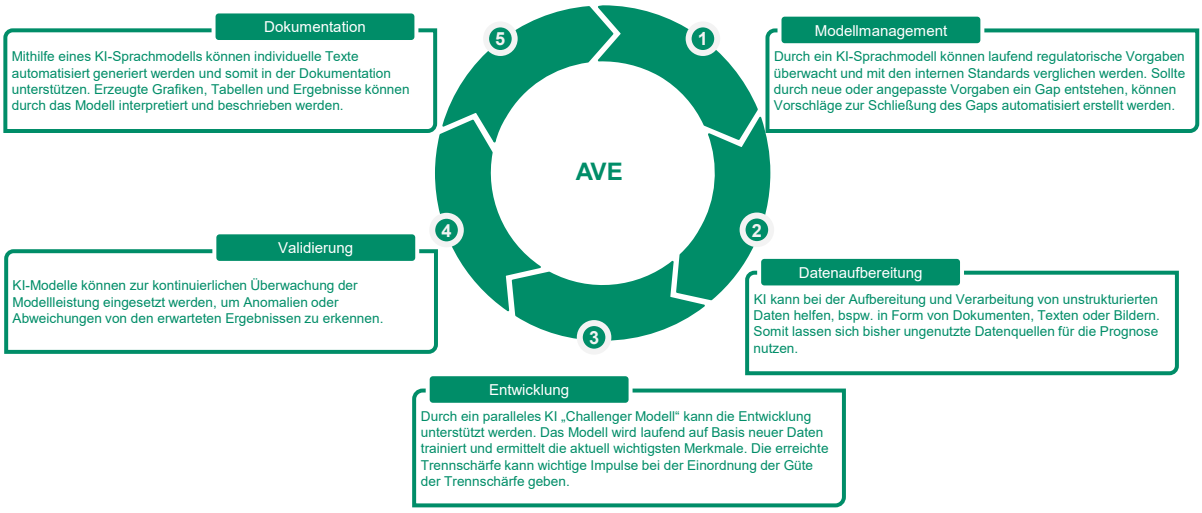

Abbildung 1: AVE-Vorgehen für Teilautomatisierung im Risikocontrolling. Quelle: PPI AG

lichst zu automatisieren. Dazu zählt vor allem die Dokumentation, weil sie bei Modellneuentwicklungen, -kalibrierungen sowie -validierungen regelmäßig erstellt werden muss. Nicht nur vorgegebene Abschnitte der Dokumentation können durch die Modelle erstellt werden, auch Ergebnisse aus den vorherigen Schritten, wie Grafiken oder Tabellen, lassen sich automatisch integrieren.

Sprachmodelle eignen sich auch, um im Unternehmen verwendete KI-Systeme und die übrigen statistischen Verfahren daraufhin zu überwachen, ob sie immer noch den jeweils gültigen Vorschriften entsprechen. Je nach Güte des KI-Systems kann es darüber hinaus Vorschläge entwickeln, wie sich die aufgedeckten Lücken schließen lassen. Schließlich hilft KI auch dabei, unstrukturierte und deshalb meist wenig oder gar nicht genutzte Datenquellen zu erschließen.

Die verwendeten Sprachmodelle werden in der Regel nicht eigenständig trainiert, sondern lediglich für den eingesetzten Use Case parametrisiert. Dies verringert die Eintrittshürde für einen ersten Einsatz der Modelle im Vergleich zu klassischen Modellen enorm. Für den Betrieb solcher Sprachmodelle gibt es zwei unterschiedliche Ansätze. Zum einen können Unternehmen auf Open Source zurückgreifen, deren Nutzung meist kostenfrei möglich ist, und welche auf eigens bereitgestellter Hardware betrieben wird. Da dies jedoch höhere anfängliche Investitionskosten zur Folge hat, greifen die Unternehmen stattdessen häufig zu den Cloudangeboten der Hyperscaler. Als eines der größten Hindernisse galt lange Zeit der Datenschutz, doch der DSGVO-konforme Betrieb stellt heutzutage kein Problem mehr dar, das sich nicht lösen ließe.

Fazit

Der EU AI Act soll KI beherrschbar machen, legt den Begriff KI jedoch sehr streng aus, sodass auch einfache Rechenmodelle davon erfasst werden. Auf die Banken, beziehungsweise alle Unternehmen, die beispielsweise logistische Regression einsetzen, um sensible Entscheidungen zu treffen, kommen deshalb zusätzliche Aufwände zu. Vor allem, was die Dokumentationen und Erläuterungen der eingesetzten Modelle angeht, muss jetzt viel Zeit investiert werden, um zu ermitteln, inwieweit welche Berichtspflichten einschlägig sind und wie die Unternehmen ihnen gerecht werden wollen. Ausgerechnet KI erweist sich als dafür willkommener Assistent, um diese zusätzlichen Aufgaben zu bewältigen.

Ein geeignetes Vorgehensmodell stellt AVE dar, welches nicht nur die nötigen Fleißaufgaben übernehmen kann. Verschiedene KI-Assistenten erlauben sogar, große Teile einer Prozesskette zu automatisieren. In einem Markt, in dem stetig neue Anforderungen auf einen grassierenden Fachkräftemangel treffen, sind das gute Nachrichten, die sich die Unternehmen zunutze machen und sich das dafür notwendige Know-how erschließen sollten.