Vortrag „KI-Tools für den täglichen Einsatz“
Vom 07.10.24, Thomas Vehmeier

Zusammenfassung der Diskussionsrunde

Frage: Zur Höhe der Geldstrafen bei Verstößen gegen bestehende KI-Gesetze: Ich finde, Geldstrafen sollten so hoch gesetzt werden, dass sie die jeweilige Firma ruiniert – und eine neue Firma, die sich an das entsprechende Recht hält, dann eine Chance hat, groß zu werden. Man muss die Strafe größer setzen als der Effekt „Wer zuerst kommt, mahlt zuerst“.
Gibt es hierzu bereits Diskussionen?

Vehmeier: Mir sind keine solchen Diskussionen bekannt – ich bin aber auch, was das Strafmaß angeht, nicht mit Details vertraut; die Ideen an sich werden aber natürlich häufiger vorgebracht. Allerdings gibt es ja beispielsweise Facebook, trotz vielfacher Datenschutzverstöße, immer noch, obwohl die entsprechenden Strafen durchaus sehr hoch waren.
Ein Problem ist häufig, dass die Gerichtsbarkeit einfach einen sehr langen Atem hat und entsprechende Urteile erst zwei oder drei Jahre später durchgesetzt werden – und in dieser Zeit können Unternehmen dann so groß werden, dass sie die Strafen quasi aus der Portokasse bezahlen können. Und das Problem ist, dass einige Unternehmen genauso kalkulieren: Eine 10 Millionen Euro Strafe würde sie als Startup noch ruinieren, ihnen aber einige Jahre später, als riesiger, milliardenschwerer Konzern, kaum mehr schaden.

Frage: Eine weiterführende Frage: Wann ist es denn soweit, dass KI in der Gerichtsbarkeit eingesetzt wird? In Deutschland ist es wohl schwierig, aber in anderen Ländern könnte ich mir das gut vorstellen. Wenn die Gerichtsbarkeit durch den Einsatz von KI dann sehr schnell wird, haben die Menschen kaum mehr eine Chance, dagegen vorzugehen.

Vehmeier: KI wird auf jeden Fall zum Einsatz kommen, auch in der Gerichtsbarkeit; in einigen Bereichen ist sie ja auch schon fest im Einsatz. Beispielsweise werden lange Texte eigentlich nicht mehr wirklich durch den Menschen selbst gelesen – der Trend geht ja dahin, dass lange Texte durch eine KI gelesen werden, diese die Quintessenz daraus zieht, eine Zusammenfassung schreibt – und erst dann interagiert der Mensch wieder mit dem Text, indem er mit der KI über diesen schreibt oder spricht. Texte konsumieren, tatsächlich zu lesen, ist dann ein Kunstgenuss; und das wird dann natürlich auch bei juristischen Texten so sein. Es gibt auf jeden Fall spezialisierte und sehr fein getunte LLMs – bestimmt gibt es auch schon Startups, die solche LLMs bereits im Bereich der Gerichtsbarkeit einsetzen.

Meistens steckt hinter solchen spezialisierten Modellen übrigens ein Open Source Programm, da es hier einfach keine Lizenzprobleme geben kann.

Frage: Die KI-Modelle wissen ja nichts – oder nur ganz wenig. Jetzt ist es doch aber in der Juristerei so, dass in jedem Land hinter den Gesetzen ein gewisser Wille steht. Also: Was will das Land X mit einem gewissen Gesetz zum Thema Urheberrecht eigentlich erreichen, was ist die Philosophie dahinter? Und wenn eine KI nun ein rein statistisch operierendes Gerät ist, wie soll sie dann eine mögliche Logik einer Urteilssprechung auf Basis der philosophisch-ethischen Absicht eines Landes kennen und umsetzen?

Vehmeier: Das kann sie nicht, denn sie kann noch keine Kausalitäten erstellen. Sie kann nur Wahrscheinlichkeiten aufstellen – wie ein Hochstapler. Wenn man einem Hochstapler zuhört, hört sich alles fantastisch und überzeugend an – aber es macht eigentlich keinen Sinn. Das kann die KI jetzt. Sie ist im Moment ein stochastischer Papagei, der einfach das nachplappert, was wir ihm sagen.

Dabei ist aber natürlich auch manchmal viel Wissen enthalten, da ein Papagei sich ja viel merkt, indem er es reproduziert. Wenn wir uns jetzt anschauen, wie die Stufen davon aussehen, dass Menschen sich im Alltag an KI adaptieren, dann ist die erste Stufe ein einfaches Frage- Antwort-System. Als nächstes baut man sich vielleicht einen eigenen, spezialisierten Chatbot; danach kommt retrieval augmented generation – das bedeutet, dass parallel noch eine Wissensdatenbank aufgebaut wird, die vielleicht mit bestimmten Gesetzessammlungen abgeglichen werden. Der nächste Schritt wiederum wären spezifische Agenten, die jeweils spezifische Aufgaben übernehmen – einer würde dann beispielsweise die Quellen überprüfen, ein anderer nach Beweisen suchen und ähnliches. So beispielsweise im Rechtswesen.

Agenten könnten aber auch im allgemeinen Alltag eingesetzt werden – so dass man als Privatperson nicht mehr selbst die DB-App öffnen und dort ein Ticket kaufen müsste, sondern dass ein KI-Agent das übernimmt. Dieser würde dann beispielsweise kommunizieren, dass er ein gutes Sparpreis Angebot gefunden hat, und fragen, ob er es kaufen soll. Wenn der Mensch das dann bestätigt, kauft der Agent das Ticket dann auch tatsächlich selbst. Diese Agenten werden also unser ganzes App Erlebnis verändern – die Oberflächen, mit denen wir dann in ein paar Jahren arbeiten werden, werden wahrscheinlich nicht mehr nur ChatGPT und ähnliches sein. Die werden wir, so wie Google, zwar auch weiterhin benutzen, aber zusätzlich werden wir eben Agenten haben, die im Hintergrund für uns das Surfen übernehmen.

Kommentar: Da wird mir aber angst und bange, wenn ich daran denke, dass Elon Musk jetzt Donald Trump im Wahlkampf unterstützt und Donald Trump sehr viele Strafprozesse aktiv hat – die Angst, die ich habe, ist ja nicht, dass Elon Musk seinen Programmierern über die Schultern schaut – sondern dass hier schon eine massive Einflussnahme passieren könnte.

Frage: Sie haben gesagt, KI ist keine Wissensdatenbank, sondern eine Wahrscheinlichkeitsmaschine. Ich kann mir das nicht wirklich vorstellen, können Sie das ein bisschen erklären? Denn letztendlich haben Sie ja auch gezeigt, dass die KI auf Webseiten zurückgreift und mit Informationen gefüttert wird. Ich stelle es mir ganz simpel so vor, dass etwas vorhanden ist, worauf die KI zurückgreift – deshalb muss es ja so gesehen eine Wissensdatenbank geben.

Vehmeier: Ja, das stimmt natürlich ein Stück weit. Diese retrieval Fähigkeiten, also die Suche über das Internet, das ist nicht Teil des KI-Modells, sondern Teil der App. Man muss dabei klar unterscheiden: ChatGPT ist die App, die einerseits Zugriff auf eine KI hat, und andererseits noch andere Fähigkeiten hat, wie beispielsweise ein Eingabefenster, eine bestimmte Darstellung, aber auch die Suchfähigkeit im Internet. Das bedeutet: Wenn die KI aus dem bestehenden Wissen, das in den Trainingsdaten vorgegeben ist, keine guten Ergebnisse erzielen kann, beginnt die App – nicht die KI – im Internet zu suchen. Und dieses Wissen wird dann einfach über die App präsentiert und den KI-Ergebnissen vorgeschoben. Das ist aber neu recherchiert und nicht das Wissen der KI selbst.

Was ich mit Wahrscheinlichkeitsmaschine oder Wahrscheinlichkeitsdatenbank meine: ChatGPT kann zum Beispiel auf Grundlage der Trainingsdaten erraten, welche Buchstaben und Worte der Wahrscheinlichkeit nach aufeinander folgen.
Diese Wörter sind außerdem sozusagen Anker im neuronalen Netz – wenn zum Beispiel das Wort „Humanismus“ eingegeben wird, wird die entsprechende thematische „Ecke“ der Trainingsdaten angezapft. Die Trainingsdaten sind per se nicht kategorisiert oder sortiert – und so ist natürlich auch viel Unbrauchbares dabei, alleine schon, weil ja sozusagen das ganze Internet darin steckt.

Frage: Wenn ich eigene oder firmenspezifische Daten bei ChatGPT eingebe, gehören diese Daten dann ChatGPT? Es gab ja in der Vergangenheit eine Diskussion über frühre WhatsApp-Versionen, dass – wenn ich über WhatsApp Bilder versende – diese WhatsApp gehören und zur Werbung verwendet werden können. Das ist inzwischen aufgelöst und es wurden entsprechende Richtlinien festgelegt.
Wie ist es bei ChatGPT?

Vehmeier: Nach aktuellem Stand sollte man davon ablassen, nachvollziehbare Unternehmensdaten oder private Daten in ein KI-System einzugeben, da hier die Richtlinien noch nicht genau festgelegt sind. Deshalb hat beispielsweise die Sparkasse ihr eigenes LLM – allerdings ist das sehr aufwändig und teuer.

Hier muss man einfach vorsichtig und aufmerksam bleiben – es ist schon möglich, sich dieser Gefahr zu entziehen. Man kann auch bei vielen Programmen und Apps die entsprechenden

Datenschutz Einstellungen genauer durchlesen und sein Einverständnis über die Verwendung der Daten zu Trainingszwecken entziehen.

Aber insgesamt ist es aktuell noch eine unbefriedigende Situation und oft können sich Kleinunternehmen die notwendigen Schritte zur absoluten Sicherheit einfach nicht leisten.

Frage: Bis wann kann man denn mit der Entwicklung solcher Agenten rechnen, die einem beispielsweise im Internet Reisen buchen?

Vehmeier: Das passiert eigentlich genau jetzt – dafür werden gerade Startups gegründet. Natürlich ist der Ausgang aktuell nicht einzuschätzen, aber in zwei Jahren wird man sicher die ersten Ergebnisse sehen – vielleicht auch schon in den nächsten Monaten.
Es wird auf jeden Fall im Moment daran gearbeitet und ist keine Zukunft mehr.