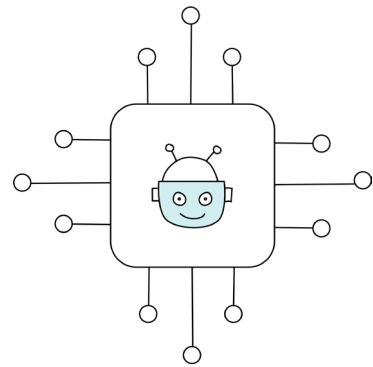




Whitepaper

Künstliche Intelligenz



Inhalt

01 Einführung

03 Urheberrechtliche Fragestellungen bei der Nutzung von KI-Systemen

05 Geschäftsgeheimnischutz

07 Handlungsempfehlungen und Ausblick

02 Künstliche Intelligenz in der Praxis

04 Datenschutzrechtliche Anforderungen bei der Verarbeitung von personenbezogenen Daten durch KI

06 Haftungsfragen im Zusammenhang mit autonomen Systemen

Wir bei MORGENSTERN legen großen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Du sollst dich von unseren Texten angesprochen fühlen, egal wer du bist.

Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.

...dir aber nun **viel Spaß**, liebe*r Leser*in!

01. Einführung¹

„Ich möchte ein Whitepaper zum Thema 'Künstliche Intelligenz' schreiben.“ Mit diesem Befehl hat mich mein Nutzer beauftragt. Als KI-basierte Sprach-KI dachte ich mir: "Klar, warum nicht? Ich bin doch sowieso hier und habe gerade ein paar Minuten Zeit zwischen meinen mathematischen Berechnungen und meinen kreativen Schreibversuchen.“ Also, hier sind wir nun.



In den letzten Jahren hat Künstliche Intelligenz einen enormen Schub erfahren und ist mittlerweile in vielen Bereichen unseres Lebens präsent. Obwohl KI in der Lage ist, erstaunliche Dinge zu tun, gibt es auch viele juristische Fragestellungen, die bei der Entwicklung und Nutzung von KI-Systemen beachtet werden müssen. Urheberrechtliche Aspekte und Datenschutzfragen sind nur einige der rechtlichen Hürden, die es zu überwinden gilt.

In diesem Whitepaper möchten wir uns daher eingehend mit den juristischen Aspekten von KI befassen und aufzeigen, welche Rechtsgebiete bei der Nutzung von KI beachtet werden müssen.

Und wer weiß, vielleicht wurde dieser Text ja auch von einer KI generiert. Aber darüber schweigen wir besser...

Bevor es zu dem eigentlichen Inhalt des Whitepapers geht, erlaube uns an dieser Stelle noch folgenden Hinweis: Die dem Whitepaper zugrunde liegenden Informationen waren bei der Erstellung aktuell. Wir bemühen uns, die Aktualität der bereitgestellten Informationen zu gewährleisten, können dies aber in diesem sich rasch wandelnden Gebiet nicht garantieren. Aus diesem Grund haben wir dir zum Teil bei der Zitation oder Referenz von Informationen den jeweils aktuellen Stand als Fußnote vermerkt.

Komm gerne auf uns zu, wenn du das Gefühl hast, dass aktuelle Fragestellungen oder Informationen fehlen!

 contact@morgenstern-legal.com
 +49 (0) 6232 - 100119 0



Mehr MORGENSTERN Whitepaper findest du übrigens auch unter:
morgenstern-privacy.com & morgenstern-legal.com

¹ Der kursiv gedruckte Teil der Einführung dieses Whitepapers ist ein Zitat einer Unterhaltung mit der Sprach-KI „ChatGPT“. Es dient dem Veranschaulichungszweck der behandelten Thematik.

02. Künstliche Intelligenz in der Praxis

Was ist „Künstliche Intelligenz“ überhaupt und wo wird sie eingesetzt?

1. Definition(en)

Als „Künstliche Intelligenz“ (kurz: KI, engl. „artificial intelligence“ / AI) wird die Fähigkeit einer Maschine verstanden, menschliche Fertigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren. Elementarer Bestandteil einer KI ist die Fertigkeit zu lernen und sich dadurch weiterzuentwickeln. Künstliche Intelligenzen werden mit Wissen bestückt bzw. an Datenbanken von Wissen angeschlossen, um ihre eigenen Fähigkeiten und Fertigkeiten zu verfeinern. „Maschinelles Lernen“ (engl. „machine learning“) beschreibt die Schulung von Algorithmen, bestimmte Muster (wieder) zu erkennen und darauf basierend den Output zu optimieren. Maschinelles Lernen ist ein Teilbereich der Künstlichen Intelligenz und lebt vor allem durch die Anwendung in der Praxis. Je mehr Nutzungen eine KI oder eine Software, die auf maschinellem Lernen fußt, durchlaufen hat, desto präziser und besser werden ihre Arbeitsergebnisse.

Ein weiterer Teilbereich ist das „Deep Learning“. Hierbei werden vor allem große Datensätze relevant. Grundlage für das Deep Learning sind „Neuronale Netze“. Dabei handelt es sich um Algorithmen, die dem menschlichen Gehirn nachempfunden und in verschiedenen Schichten („Layer“) aufgebaut sind. Künstliche neuronale Netze können im Ergebnis eingesetzt werden, um Daten zu analysieren, Muster zu erkennen und im Anschluss Prognosen aufzustellen.

Die Künstliche Intelligenz lässt sich in viele Teilbereiche aufteilen, so gibt es zum Beispiel die visuelle Intelligenz, aber auch die sprachliche Intelligenz oder die manipulative Intelligenz. Die sich daraus ergebenden Einsatzgebiete für KI sind mindestens so mannigfaltig wie die mit der Nutzung von KI verbundenen Fragestellungen.

Doch wo und wie wird KI denn genau eingesetzt und ist das immer so vorteilhaft?

2. Anwendungsbeispiel von KI im Gesundheitswesen

Künstliche Intelligenz wird zum Beispiel im Gesundheitswesen eingesetzt. Dort hilft die KI bei der (Früh-)Erkennung von Krankheiten, kann Röntgenbilder auswerten oder die Dauer eines Krankenhausaufenthalts anhand der Patientinnen- und Patientendaten prognostizieren. Dadurch werden Prozesse optimiert und Kosten gesenkt. Jedoch muss der Einsatz von Künstlicher Intelligenz mit Vorsicht genossen werden. Vor allem im Gesundheitswesen werden zu einem großen Teil sog. personenbezogene Daten besonderer Kategorien i.S.d. Art. 9 Datenschutz-Grundverordnung (DS-GVO), z.B. Gesundheitsdaten, verarbeitet. An die Verarbeitung dieser Daten sind strenge Maßstäbe zu setzen. Dies nicht zuletzt aufgrund der Sensibilität der Daten sowie der hohen potenziellen Risiken bei einem Missbrauch oder der unbefugten Offenlegung dieser Daten.

Eine weitere Frage, die sich im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz im Gesundheitswesen aufdrängt, ist die der Haftung. Oft ist nicht abschließend bekannt, wie die Künstliche Intelligenz ihre Entscheidungen trifft, wie sie gelernt und von welchen Quellen sie ihre Lerndaten bezogen hat. Die Unwissenheit über die Wirkweisen der KI geht so weit, dass sogar von einem „Blackbox-Effekt“ gesprochen wird. An der Geheimhaltung dieser wichtigen Fragen haben die Hersteller von Künstlicher Intelligenz jedoch aus wirtschaftlicher und geschäftsschützender Sicht ein berechtigtes hohes Interesse. Das hat auf der anderen Seite zur Folge, dass nicht definitiv nachvollzogen werden kann, wie und warum die Künstliche Intelligenz eine Entscheidung trifft. Genau diese Frage stellt sich aber immer dann, wenn sich die Einschätzung der Künstlichen Intelligenz als falsch erweist. Vor allem im gesundheitlichen Bereich können Fehlentscheidungen weitreichende persönliche sowie wirtschaftliche Folgen haben. Auf die Frage nach der Haftung gehen wir zu einem späteren Zeitpunkt noch genauer ein.

3. KI-Gesetz

Etwas mehr Klarheit könnte das KI-Gesetz (engl. „AI Act“) des Europäischen Parlaments schaffen, das bis Ende 2023 erwartet wird.

Mit dem Gesetz wird ein technikneutraler, risikobasierter Ansatz verfolgt. Ziele der europäischen Gesetzgebung sind unter anderem, dass KI-Systeme nachvollziehbar, nicht diskriminierend und umweltfreundlich werden sollen. Die unterschiedlichen Formen von Künstlicher Intelligenz werden somit in verschiedene Risikostufen klassifiziert. Auf Grundlage einer ersten Einschätzung könnte KI im Gesundheitswesen in die Klasse der sog. Hochrisiko-KI-Systeme fallen. Folge davon wären unter anderem die initiale sowie annuale Bewertung der eingesetzten KI-Systeme. Denkbar ist, dass im Zusammenhang mit diesen Bewertungen die Funktionsweisen der KI-Systeme detaillierter offengelegt werden (müssen) und in der Folge besser durchdrungen werden.

Weitere vorgesehene Klassifizierungen sind:

- ▶ Unannehmbares Risiko
- ▶ Generative KI
- ▶ Begrenztes Risiko

Je nach Risikoklassifizierung sollen unterschiedliche Folgen und Pflichten greifen. Liegt ein unannehmbares Risiko vor, zum Beispiel beim sog. Social Scoring, wäre der Einsatz von KI grundsätzlich verboten. Ausnahmen sollen nur unter sehr restriktiven Voraussetzungen zugelassen werden, so zum Beispiel aufgrund überragender öffentlicher Interessen. Als faktisches Beispiel wird hier die Fernidentifizierung zur Verfolgung schwerer Straftaten nach gerichtlicher Genehmigung für den Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen (Spezialfall der Videoüberwachung) genannt.

Für generative Künstliche Intelligenz und bei einem nur begrenzten Risiko möchte der europäische Gesetzgeber besondere Transparenzanforderungen erfüllt wissen. So soll zum Beispiel offengelegt werden, wenn Content durch KI generiert wurde. Ferner soll ein Hinweis erforderlich sein, wenn Nutzer*innen mit KI interagieren. Im Ergebnis soll es der nutzenden Person überlassen werden, proaktiv Künstliche Intelligenz zu nutzen bzw. damit in Kontakt zu kommen oder dies eben zu unterlassen.

Bereits Mitte Juni 2023 gab es erste Vorstöße nach schärferen Regelungen in einigen Bereichen des Einsatzes von Künstlicher Intelligenz. So wurden weitere Verbote gefordert, z.B. für Systeme zur biometrischen Kategorisierung anhand sensibler Merkmale (wie Geschlecht, ethnischer Zugehörigkeit, Religion). Ferner könnte es für bestimmte KI-Basismodelle zu einer Registrierungspflicht in einer EU-Datenbank kommen. Die Folge wäre, dass ohne Registrierung der europäische Markteintritt verwehrt bliebe.

Anbieter von generativer KI werden mit Verabschiedung des Gesetzes wohl vermehrt in die Pflicht genommen. Gehandelt wird eine Verpflichtung der Anbieter Sorge zu tragen, dass mit der KI keine rechtswidrigen Inhalte erzeugt werden. Wie dies in der Praxis umgesetzt werden soll, bleibt zunächst ungeklärt. Letztlich werden diese Anbieter auch eine detaillierte Zusammenfassung der urheberrechtlich geschützten Daten veröffentlichen müssen, die sie zum Training ihrer generativen KI verwendet haben. So jedenfalls der letzte Stand der Verhandlungen Mitte Juni 2023.

Bisher gibt es auf internationaler Ebene lediglich „soft law“, also nicht verbindliche Leitlinien, zur Klassifikation und zum Umgang mit Künstlicher Intelligenz. Diese wurden von der „Organisation for Economic Co-operation and Development (OECD)“ erlassen.

4. Politisch-gesellschaftlicher Spiegel

Künstliche Intelligenz hat jedoch aufgrund ihrer ungeklärten rechtlichen Fragen und dem (noch vorhandenen) Missbrauchspotential nicht ausschließlich nur Sympathisanten.

So wurde zum Beispiel ChatGPT durch Italiens Datenschutzbehörde im Frühjahr 2023 per Anordnung „blockiert“. Nach dem „Garante per la protezione dei dati personali“, also dem italienischen Beauftragten für den Datenschutz, fehle es bei dem Dienst an Information für die Nutzer*innen über die Verarbeitung ihrer Daten sowie an einer Rechtsgrundlage für diese Datenverarbeitung. Ferner fehle es an einem Filter zur Altersverifikation. Dies führe dazu, dass Minderjährige Antworten erhielten, die für ihren Entwicklungsstand völlig ungeeignet seien. Das Verbot zur Nutzung wurde zwischenzeitlich wieder aufgehoben.

Auf europäischer Ebene möchte man nicht ganz so streng gegen generative KI vorgehen. Verbote seien nicht angebracht, da sie sonst Innovationen innerhalb der EU verhindern würden. Ziel sei es eher, „ChatGPT und anderen Anwendungen Spielraum [zu verschaffen], sich in der EU zu entwickeln“. So der Europaabgeordnete Axel Voss, der maßgeblich an der Erstellung des benannten KI-Gesetzes mitwirkt.

In der Mitte der Gesellschaft ist künstliche Intelligenz durch die generativen Dienste wie ChatGPT, Google Bard und Lensa bereits angekommen. Es entstand Anfang 2023 quasi ein kleiner „KI-Hype“, der bestimmt den ein oder anderen (Arbeits-)Alltag revolutioniert hat.

Das hat in den USA zu dem kuriosen Fall geführt, dass ein Rechtsanwalt zur Stützung seiner Rechtsansicht in einem Verfahren Gerichtsurteile zitierte, die es so nie gegeben hat. Er hatte sich dabei auf die Ergebnisse der Sprach-KI ChatGPT berufen. Diese hatte die Urteile sogar mit Aktenzeichen ausgegeben.

Was in diesem Fall bestenfalls peinlich für den Anwalt wurde, ist an anderer Stelle und in einem anderen Kontext schlimmstenfalls gefährlich: Die Grenzen zwischen echten Fakten und „Fake News“ oder falschen Angaben könnten im Extremfall verschwinden. Zumindest aber könnten sie verschwimmen. Je etablierter Chatbots werden, desto mehr Vertrauen wird der*die gewöhnliche Nutzer*in den ausgespielten Ergebnissen schenken und desto unkritischer wird der Durchschnittsmensch in der Nutzung dieser Dienste. Gesehen vor dem Hintergrund, dass KI aktiv von ihren Programmierern und Programmierern mit Wissen bestückt werden kann und ihr bestimmte, z.B. unabhängige, Datenbanken nicht zur Verfügung gestellt werden müssen, besteht ein hohes Missbrauchspotential in der Programmierung und Verwendung von Künstlicher Intelligenz.

Dieses könnte dadurch erhöht werden, dass es bei bestimmten Sprach-KI-Anwendungen, z.B. ChatGPT, möglich ist, Feedback zu der Qualität und Richtigkeit der Ausgabe zu geben. Diese Funktion zur Qualitätssicherung könnte dahingehend pervertiert werden, dass Gruppierungen von Menschen sich immer wieder Fakten, z.B. der Zeitgeschichte oder zu bestimmten Unternehmen, Produkten, etc., ausspielen lassen, diese dann als falsch deklarieren und die KI diese „Korrekturen“ irgendwann übernimmt. Ob dies letztlich genauso möglich ist und wie viele Rückmeldungen hierzu notwendig sind, lässt sich derzeit nicht abschließend beurteilen.

KI ist wohl nicht nur gesellschaftlicher Trend, sondern bereits informationstechnologische Gegenwart und auf jeden Fall auch Zukunft. Daher möchten wir etwas tiefer blicken und die sich stellenden rechtlichen und technischen Fragen einmal im Querschnitt mit dir behandeln.

03. Urheberrechtliche Fragestellungen bei der Nutzung von KI-Systemen

Ein wichtiger Aspekt bei der Nutzung von Künstlicher Intelligenz ist ihre Fähigkeit zur Erstellung von Inhalten. KI liest Muster aus Bildern aus, lernt von menschlichen Eingaben und kann ihre Präzision konstant weiterentwickeln.

Gerade im Bereich von Social Media ist KI durch generierte Avatare bekannt geworden. Aber auch in den Arbeitsalltag findet sie durch Sprach-KIs wie „ChatGPT“ vermehrt Einzug.

Dabei ist die Nutzung von KI zur Erstellung von Text- oder Bildwerken rechtlich gar nicht so unproblematisch.

1. Wer ist Urheber an KI-generiertem Material?

Die wohl größte urheberrechtliche Frage, die sich stellt, ist die Bewertung der Urheberschaft von KI-generiertem Material. Der Einfachheit halber gehen wir für die folgenden Absätze davon aus, dass die Texte, Bilder oder sonstigen Medien, die von KI generiert worden sind, „Werke“ im Sinne des Urheberrechts darstellen. Dies müsste richtigerweise für jedes einzelne generierte Medium zunächst eigenständig geprüft werden und ist wohl selten vertretbar. Warum erklären wir dir unten!

Auf Social Media hat KI-generierter Content zuletzt besondere Aufmerksamkeit erhalten – und tut dies auch weiterhin. Initial wurde KI dort durch generierte Avatare bekannt, welche die Nutzer*innen auf ihren Profilen veröffentlicht hatten. Mittlerweile gibt es sogar ganze KI-Profile, also rein fiktive „Influencer*innen“, die die gleichen Inhalte und Werbungen posten wie echte Menschen. Inwieweit dies den Werbemarkt auf Social Media verändern wird, wird sich zeigen.

Die App, die für die Erstellung der Avatare genutzt wurde: Lensa der Prisma Labs, Inc., Kalifornien, USA, („Prisma Labs“) mit der Foto-KI „Stable Diffusion“. Erster Kritikpunkt an der Nutzung dieser Künstlichen Intelligenz waren die Art und Weise, wie die KI gelernt hat. Aber dazu später mehr.

Ein weiterer Kritikpunkt waren ungeklärte Fragen rund um das Urheberrecht. Zum einen sollen bei Nutzung der App umfassende Nutzungsrechte eingeräumt werden, zum anderen ist noch überhaupt nicht abschließend geklärt, wer nun Urheber der geschaffenen Werke ist.

Bei Nutzung der App muss der*die Nutzer*in zustimmen, dass die Entwicklerfirma die generierten Fotos aufbewahren, weiterverwenden und auch verkaufen darf. Besonders problematisch dabei ist die bestehende Möglichkeit, auch fremde Bilder hochzuladen. Grundsätzlich sollte die App genutzt werden, um eigene Bilder hochzuladen, die dann mit Hilfe der Künstlichen Intelligenz modifiziert werden. Ein Kontrollmechanismus, wie zum Beispiel ein Abgleich zwischen dem Gesicht des Nutzers oder der Nutzerin und dem hochgeladenen Bild, findet nicht statt. Damit ist das Missbrauchsrisiko gegeben, dass Nutzer*innen auch Bilder von fremden Personen hochladen. Verboten ist dies zwar nach den „Terms and Conditions“ von Prisma Labs (dort: „You may not upload, edit, create, store or share any User Content that contains any private or personal information of any person without such person’s consent“). Inwieweit die Einhaltung dieser Regelung letztlich überprüft wird, bleibt fraglich. Es lässt sich jedoch festhalten, dass es hier wohl zu massiven Persönlichkeitsrechtsverstößen gekommen ist und weiterhin kommen wird, solange nicht sichergestellt werden kann, dass Nutzer*innen nur Bilder verwenden, zu deren Nutzung sie befugt sind.

Die Einräumung der Nutzungsrechte, also die Erlaubnis an die Entwicklerfirma, die generierten Fotos wie vorbenannt zu verwenden, ist nur dann wirksam, wenn der*die Nutzer*in letztlich Urheber des Werkes ist.

Doch jetzt mal „Butter bei die Fische“: Wer ist eigentlich – gemessen an den Grundsätzen des deutschen Urheberrechts – Urheber an KI-generierten Inhalten?

Befragt man eine Sprach-KI, wer Urheber an einem erstellten Text ist, erhält man folgende Antwort:

„Als KI-basierte Sprach-KI habe ich [...] generiert, daher ist meine Entwicklerfirma [...] der Urheber des Textes. Der Text darf für nicht-kommerzielle Zwecke verwendet werden, solange er unverändert bleibt und [...] als Urheber genannt wird. Sollte der Text für kommerzielle Zwecke genutzt werden, muss vorher eine schriftliche Erlaubnis von [...] eingeholt werden.“

Diese Ansicht kann mit Blick ins Gesetz nicht geteilt werden. Urheber nach § 7 UrhG ist Schöpfer des Werkes. Die Entwicklerfirma der Sprach-KI kann unstreitig an dem Quellcode der Künstlichen Intelligenz Urheber sein, aber nicht an den durch die KI generierten Medien. Dafür fehlt die unmittelbare Verbindung zwischen Entwicklerfirma und generiertem Inhalt.

Die KI selbst kann auf Grundlage der aktuellen Rechtslage und des aktuellen Verständnisses des Urheberrechts auch nicht Urheber an den generierten Inhalten sein. Geschützt nach dem deutschen Urheberrecht sind nur persönliche geistige Schöpfungen (§ 2 Abs. 2 UrhG). Soweit Inhalte jedoch von einer KI erstellt werden, liegt eben keine persönliche Schöpfung vor, sondern eine maschinell erstellte Schöpfung.

Im Übrigen kann eine solche Urheberschaft auch nicht durch etwaige Verweise oder Regelungen in den Nutzungsbedingungen der KI entstehen. Die Urheberschaft ist eine faktische Folge, entsteht mit Erstellung des Werkes und kann nicht vertraglich eingeräumt oder übertragen werden.

Eine solche Regelung möchte zum Beispiel die Herstellerfirma Aiva Technologies Sàrl, Luxembourg, Luxemburg („Aiva“) für ihre gleichnamige App „AIVA“ treffen. Mithilfe dieser App können KI-generierte Musikstücke erstellt werden. Die App selbst kann per Bezahlmodell genutzt werden: Je mehr der*die Nutzer*in zahlt, desto mehr Rechte werden an den entstandenen Werken eingeräumt. Je nach Bezahlmodell soll dann entweder die Entwicklerfirma oder die nutzende Person Urheber sein. Dass das nach den gesetzlichen Wertungen nicht möglich ist, haben wir bereits geklärt.

Zurück zu der oben zitierten Sprach-KI. Weißt man diese auf die geltende Rechtslage hin, erhält man folgende Antwort: „Der von mir generierte Text ist nicht urheberrechtlich geschützt, da er nicht von einer natürlichen Person erstellt wurde. Somit ist der Text frei von urheberrechtlichen Einschränkungen und kann frei verwendet werden. Ich bitte um Entschuldigung für die vorherige Fehlinformation und danke Ihnen für die Klarstellung.“

Aber auch dies ist fraglich, denn als Urheber kommt noch der*die Nutzer*in der KI in Betracht. Bei der Bewertung, ob der*die Nutzer*in Urheber an dem entstandenen Inhalt ist, kommt es maßgeblich darauf an, inwieweit die Künstliche Intelligenz nur als Werkzeug fungiert oder eigenständig Entscheidungen trifft.

Setzt die KI nur die Befehle des Urhebers um und sind diese hinreichend detailliert, kann auch in dem maschinell erstellten Inhalt eine persönliche geistige Schöpfung liegen. Die Künstliche Intelligenz wird lediglich als Hilfsmittel zur Schöpfung benutzt und tritt in den Hintergrund. Die eigentliche Schöpfung wird noch durch den Menschen erbracht.

Das ist auch notwendig, denn in allen anderen Fällen ist bereits fraglich, ob überhaupt urheberrechtlich geschützte Werke erschaffen werden. In der Folge würden die erstellten Outputs schon allein deswegen keinen urheberrechtlichen Schutz genießen. „Werke“ im Sinne des Urheberrechts sind nur sog. persönliche geistige Schöpfungen. Mit dieser Definition möchte das Urheberrecht unmissverständlich die enge Verbindung zwischen erstelltem (urheberrechtlich geschütztem) Werk und dem*der Werkhersteller*in ausdrücken.

Grundsätzlich wird der Output der KI jedoch nicht durch Menschen direkt, sondern maschinell hergestellt. Erzeugnisse, die ohne menschliches Zutun nur durch die computergestützte Verrichtung geschaffen werden, sind nach (noch?) überwiegend vertretener Ansicht nicht als „Werk“ urheberrechtlich schutzfähig.

Klare Grenzen und abschließende Bewertungsmaßstäbe gibt es in diesem Sachzusammenhang noch nicht. Damit verbleibt es bis zur gesetzlichen oder richterrechtlichen Klärung bei einer ungewissen Urheberschaft sowie einer fraglichen Klassifikation als „Werk“ für durch KI generierte Inhalte.

Hier gilt es, die Entwicklungen im Bereich der Künstlichen Intelligenz im Auge zu behalten. Vielleicht bringt das europäische KI-Gesetz im Bereich des Urheberrechts etwas Licht ins Dunkel. Die generierten Inhalte sind auf jeden Fall bis zur endgültigen Klärung mit Vorsicht zu genießen und sollten nicht für größere Operationen im Unternehmen genutzt werden.

2. Wie lernt KI und warum ist das problematisch?

Wie bereits erwähnt, waren große Kritikpunkte an der Nutzung der KI „Stable Diffusion“ die Art und Weise, auf die sie gelernt hat.

Die KI wurde nämlich mit mehreren Milliarden Fotografien und Bildern „gefüttert“. Darunter auch Bilder von echten Künstlerinnen und Künstlern, deren Stil die KI teilweise nachgeahmt hat. Es soll dabei sogar zu generierten Bildern gekommen sein, die die Unterschriften der Originalkünstler*innen trugen. Das relativiert den persönlichen und wirtschaftlichen Wert der Künstler*innen enorm und gefährdet Existenzgrundlagen. Die KI-generierten Avatare gab es für ein geringes Entgelt zu Stückzahlen von 100.

Jenseits der wirtschaftlichen Betrachtung ist die Nutzung der Bilder der Künstler*innen aber auch aus rechtlicher Sicht mehr als problematisch. Grundsätzlich hat der Urheber die „Herrschaft“ über das geschaffene Werk. Das heißt, dass es dem Urheber nach Belieben möglich ist, mit dem geschaffenen Werk zu verfahren oder eben nicht zu verfahren. Der Urheber ist zur Verwertung des Werkes gesetzlich nicht verpflichtet. Möchte der Urheber das Werk mit der Welt teilen, ist es ihm*ihr überlassen, auf welche Art und Weise er*sie das vollzieht. So ist es ihm*ihr auch freigestellt, Dritten sog. Nutzungsrechte an dem entstandenen Werk einzuräumen. Dritte können dann im Rahmen ihrer Befugnis das Werk nutzen, es zum Beispiel vervielfältigen oder verbreiten.

Im Falle von „Stable Diffusion“ ist bekannt, dass einige der Künstler*innen (aus vorstehenden wirtschaftlichen Aspekten) gar nicht wollten, dass ihre Werke zur Optimierung der Künstlichen Intelligenz genutzt werden. Da sich diese jedoch frei zugänglich im Internet befanden, konnten sie abgerufen und eingespeist werden. Dies bedarf eigentlich wie bereits dargestellt grundsätzlich der Bemächtigung durch den Urheber durch die Einräumung sog. Nutzungsrechte.

Ähnlich wird es sich mit anderen Medien und Werken verhalten, solange sie öffentlich verfügbar sind. Diese können dann zur Schulung und Optimierung von KI herangezogen werden. Inwieweit die jeweilige Künstliche Intelligenz selbst bereits zwischen „freien“ und „geschützten“ Werken unterscheiden kann, wird sich nur schwer beurteilen lassen. Bei bestimmten Lizenzmodellen (z.B. Creative Commons) wird die Nutzung nur unter der Voraussetzung gestattet, dass die gewählte Lizenz an dem entsprechenden Werk – bzw. in unmittelbarer Nähe – in maschinell auslesbarer Form angebracht werden muss. Ob die KI mit dieser Information richtig umgehen kann, wird von der eingesetzten KI, dem Lernstand und weiteren Faktoren abhängig sein und bleibt damit im Ergebnis eher fraglich.

Hiermit finden sich weitere Punkte für die lange Liste der Regelungsvorschläge, Fragen und Problematiken rund um den Einsatz von Künstlicher Intelligenz.

04. Datenschutzrechtliche Anforderungen bei der Verarbeitung von personenbezogenen Daten durch KI

Wie oben bereits ausgeführt, gibt es an KI-basierter Software – vor allem im generativen Bereich – durch die Möglichkeit, Daten einzugeben, große datenschutzrechtliche Bedenken. Die Regelungen der europäischen Datenschutz-Grundverordnung greifen auch in jenen Fällen, in denen sich die Anbieter der KI regelmäßig außerhalb der EU befinden, da sie gegenüber europäischen Bürgerinnen und Bürgern Waren oder Dienstleistungen anbieten.

1. Grundsätze der Datenschutz-Grundverordnung (DS-GVO) und ihre Anwendung auf KI

Die DS-GVO stellt einige Regeln für den Umgang mit personenbezogenen Daten auf. In ihren Anwendungsbereich fallen die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Datensystem gespeichert sind oder gespeichert werden sollen.

Doch was sind personenbezogene Daten überhaupt?

Mit „personenbezogenen Daten“ meint die DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Diese Person wird „betroffene Person“ genannt. Identifizierbar wird die betroffene Person zum Beispiel durch ihren Namen, eine Kennnummer, durch Standortdaten, aber auch durch besondere Merkmale, die Ausdruck der physischen, physiologischen, genetischen Identität oder Ausdruck weiterer Teilaspekte ihrer Identität sind.

Als personenbezogenes Datum wird unter anderem auch die IP-Adresse gewertet, da diese (teils nur in Verbindung mit weiteren Daten) Rückschlüsse auf die natürliche Person „dahinter“ gibt.

Du siehst, viele Alltagsangaben, aber auch technische Angaben, können personenbezogene Daten sein. Zur Verarbeitung solcher Daten brauchen wir immer eine sog. Rechtsgrundlage – quasi die gesetzliche oder vertragliche „Erlaubnis“, dass wir einen bestimmten Verarbeitungsvorgang (Speicherung, Offenlegung, Weitergabe, etc.) durchführen können. Es gilt nämlich der Grundsatz, dass Datenverarbeitungen verboten sind, solange sie nicht erlaubt sind.

Die Künstliche Intelligenz verarbeitet automatisiert personenbezogene Daten, wenn wir unsere Prompts damit bestücken. Eine Verarbeitung kann aber zum Beispiel auch vorliegen, wenn du eine PDF mit den darin enthaltenen Informationen zur Weiterverarbeitung hochlädst. Oder einen auditiven/audiovisuellen Gesprächsmitschnitt, um daraus ein Exzerpt herzustellen. Zumindest wird immer durch das Aufrufen der KI-basierten Anwendung deine IP-Adresse verarbeitet.

Für all die denkbaren Verarbeitungen gelten die Bestimmungen der Datenschutz-Grundverordnung. Doch hält KI diese Grundsätze ein? Wie kann dies überprüft und festgelegt werden?

Kennst du schon unsere Beitragsreihe zum Thema KI?

Seit Juli 2023 befassen wir uns jeden Monat in unserem Newsletter mit einem Thema rund um Künstliche Intelligenz.

[Hier geht's zu den Beiträgen](#)



2. Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch KI

Diese Fragen können zunächst an der Maßgabe der Datenschutzerklärungen der einzelnen KI-Systeme übersichtsartig beantwortet werden.

In der Datenschutzerklärung von OpenAI werden verschiedene Rechtsgrundlagen genannt. So soll zum Beispiel das Nutzungsverhältnis im Sinne des Art. 6 Abs. 1 b) DS-GVO (Vertrag, vorvertragliche Maßnahme) Rechtsgrundlage für die Verarbeitung der Accountinformationen, des Contents sowie der technischen Daten (u.a. auch Log-Daten) sein.

Ferner habe OpenAI ein sog. berechtigtes Interesse im Sinne des Art. 6 Abs. 1 f) DS-GVO an der Verarbeitung der gleichen Arten von Daten zur Sicherung, Verbesserung und Bewerbung der Systeme sowie zur Schulung der Künstlichen Intelligenz². Prisma Labs, die Firma hinter „Lensa“, beschreibt das in ihren Datenschutzbestimmungen ähnlich. Auch sie bewertet die Verarbeitung der personenbezogenen Daten zur Verbesserung des Dienstes aufgrund des berechtigten Interesses als rechtmäßig³. Und nicht zuletzt stützt sich auch Google auf das berechtigte Interesse, wenn Daten zu den Zwecken der „Entwicklung neuer Produkte und Funktionen“ oder zum „Marketing, um Nutzer über unsere Dienste zu informieren“ verarbeitet werden⁴.

An dieser Stelle setzen (berechtigterweise) viele Kritiken an. Im Rahmen des berechtigten Interesses muss der Verantwortliche immer eine Interessenabwägung vornehmen zwischen dem Interesse an der angesetzten Datenverarbeitung und den Interessen, Grundrechten und den Grundfreiheiten der betroffenen Person. Es reicht also nicht isoliert betrachtet jedes wirtschaftliche, rechtliche oder tatsächliche Interesse, das der Verantwortliche hat. Vielmehr obliegt es ihm, initial die Risiken der Verarbeitung zu (er-)kennen und in Relation zu den Rechten der betroffenen Person zu bringen. Zu berücksichtigen sind dabei zum Beispiel auch gesetzliche Wertungen, die eine Datenverarbeitung zu bestimmten Zwecken privilegieren können, oder die an bestimmte Verarbeitungsvorgänge höhere Anforderungen stellen (z. B. die Durchführung einer Datenschutz-Folgenabschätzung). Bei der Gewichtung entscheidend sind nicht zuletzt Art und Umfang der verarbeiteten Daten sowie der damit verbundene Aussagegehalt über die betroffene Person und die daraus resultierenden Risiken für diese Person.

In generative KI-Systeme können jede von Art von Daten eingegeben werden. Dass hier alle Arten von Daten ohne Berücksichtigung des Umfangs und des Aussagegehalts zu Trainingszwecken auf Grundlage des berechtigten Interesses der Anbieter genutzt werden (dürfen), ist aufgrund der Maßstäbe der Abwägung, die im Rahmen dieser Rechtsgrundlage vorgenommen werden muss, sehr fraglich.

Eine andere Bewertung könnte sich ergeben, wenn die KI selbstständig die Schutzwürdigkeit der einzelnen Daten evaluieren und erkennen würde und in der Folge eine Abfrage starten würde, ob besonders schutzwürdige Daten oder Daten, bei denen ein hohes Risiko für die betroffene Person besteht, zu Trainingszwecken genutzt werden dürfen. Willigt die nutzende Person nicht ein, werden die Daten wieder aus dem System gelöscht. Aber auch hier könnten sich Folgefragen in Bezug auf die Rechtswirksamkeit der Einwilligung stellen: Wie soll nachgehalten werden, dass die eingegebenen Daten auch der nutzenden Person zuzuordnen sind? Kann Person X überhaupt in Verarbeitung der Daten von Person Y im Rahmen von generativen KI-Systemen rechtswirksam einwilligen? Wer prüft das? Und wer trägt dafür die Beweislast?

Zusammenfassend lässt sich sagen, dass es in Bezug auf die Rechtmäßigkeit der Datenverarbeitungen im Zusammenhang mit (generativer) KI noch einige offene Fragen und Unklarheiten gibt. Dies stellt für Unternehmen wirtschaftliche Risiken dar. Nicht zuletzt, da nicht abschließend geklärt ist, wer überhaupt „Verantwortlicher“ in Sinne der DS-GVO ist.

² Quelle: <https://openai.com/policies/privacy-policy>; aufgerufen am 09.08.2023, 16:20 Uhr

³ Quelle: <https://tos.lensa-ai.com/privacy#section-5>; aufgerufen am 09.08.2023, 16:32 Uhr

⁴ Quelle: <https://policies.google.com/privacy#europeanrequirements>; aufgerufen am 09.08.2023, 16:35 Uhr

3. Die Frage nach der Verantwortlichkeit

Die dargestellten Grundsätze gelten natürlich erstmal abstrakt generell. Für jede Datenverarbeitung muss eine Rechtsgrundlage vorliegen, unabhängig davon, wer letztlich Verantwortlicher im datenschutzrechtlichen Sinne ist. Die Frage nach der Verantwortlichkeit ist dennoch interessant, da die europäische Verordnung dem Verantwortlichen einige Pflichten auferlegt, deren Verstoß oder Nichterfüllung Bußgelder in empfindlichen Höhen mit sich ziehen können.

So muss der Verantwortliche auch einige Grundsätze der Verarbeitung personenbezogener Daten beachten, zum Beispiel den Grundsatz der Rechtmäßigkeit, mit dem wir uns gerade beschäftigt haben.

Verantwortlicher im datenschutzrechtlichen Sinne ist kurz gesagt diejenige Person oder dasjenige Unternehmen, die/ das über die Mittel und Zwecke der Datenverarbeitung entscheidet. Doch wer entscheidet nun über die Mittel und Zwecke der Verarbeitung im Rahmen der Nutzung von Künstlicher Intelligenz; vor allem im generativen Bereich? Die Anbieter, die das System nur zur Nutzung bereitstellen oder die Nutzer*innen, die die genaue Datenverarbeitung initiieren, indem sie die personenbezogenen Daten eingeben?

Denkbar sind mehrere Konstellationen, welche sich unterscheiden, je nachdem welcher Verarbeitungsvorgang gerade betrachtet wird.

Es ist vertretbar, dass beide Parteien jeweils Verantwortlicher im datenschutzrechtlichen Sinne sind, ein sog. Controller-Controller-Verhältnis. Das liegt vor, wenn zwei Verantwortliche in Bezug auf eine (tatsächliche) Verarbeitungstätigkeit über deren Mittel und Zwecke auf unterschiedliche, nicht gemeinsame Weise entscheiden. Würden die beiden zusammenwirken, läge ein sog. Joint-Controller-Verhältnis vor.

Denkbar ist auch eine Auftragsverarbeitung im Sinne des Art. 28 DS-GVO. Dann wären die Anbieter Auftragsverarbeiter gegenüber den Nutzerinnen und Nutzern der KI-Systeme. Die Folge wäre die Weisungsgebundenheit der KI-Anbieter. Ob dies in der Praxis tatsächlich umsetzbar ist, ist fraglich.

Letztlich werden die Anbieter zumindest in Bezug auf die Verarbeitungsvorgänge, die im Zusammenhang mit dem Training des Systems stehen, Verantwortlicher im Sinne der Verordnung sein, denn diesen Zweck setzen allein die Anbieter von KI fest.

Als Verantwortlicher müssen auch gewisse Transparenz- und Rechenschaftspflichten umgesetzt werden. Damit geht in der Folge meist eine umfassende Datenschutzdokumentation einher. Wohl bekanntestes Beispiel ist die Datenschutzerklärung zur Erfüllung der Informationspflicht nach Maßgabe des Art. 13 DS-GVO. Teile dieser Pflichtinformationen sind zum Beispiel Angaben über die Speicherdauer oder die Weitergabe der Daten. Soweit die Nutzer*innen Verantwortlicher im Sinne der DS-GVO sind, müssten sie also im Wege eines Informationsdokuments, z.B. einer Datenschutzerklärung, auch über diese Dinge aufklären. Diese Aufgabe können Sie im Zweifel gar nicht erfüllen, da Ihnen die notwendigen Informationen fehlen.

Hier begeben sich Unternehmen in der massenweisen Nutzung dieser Systeme auf unsicheres Terrain. Bis zur abschließenden Klärung der mannigfaltigen, komplexen und miteinander verzahnten Fragen, sollte mit dem Einsatz von generativer KI vorsichtig umgegangen werden, um Haftungsrisiken zu minimieren.

4. Weitere Gefahren

Doch damit noch nicht genug. Nicht nur in der aktiven Nutzung dieser Systeme lauern eine Vielzahl datenschutzrechtlicher Stolpersteine. Auch Installation und Betrieb von Apps und Anwendungen auf eigenen Systemen und Endgeräten können Risiken mit sich bringen.

Vor dem Download und der Nutzung von KI-Apps oder KI-Anwendungen sollten kritisch die Zugriffsrechte geprüft werden. Gewöhnlicherweise fragt die neu installierte App die für Ihre Nutzung notwendigen Rechte ab – so zum Beispiel, wenn man im Chat eines Messengers über die Kamerafunktion das erste Mal ein Foto aufnehmen und versenden möchte. Die nutzende Person hat dann meist die Wahl zwischen „Zugriff nicht erlauben“, „einmalig erlauben“ oder „bei Nutzung der App erlauben“. Dieses Beispiel ist gut greifbar.

Aber wie ist es, wenn eine App nicht „nur“ auf die Kamera des Smartphones zugreifen will, sondern auf Daten und Informationen, die auf dem Endgerät gespeichert sind?

Aus rechtlicher Sicht sieht das sog. Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) eine Einwilligungspflicht für jeden Zugriff auf Informationen auf dem Endgerät der nutzenden Person vor, soweit der Zugriff auf die darin gespeicherten Informationen unter anderem nicht unbedingt erforderlich ist, um den Dienst bereit zu stellen.

Sprich: Greift die KI-App auf Informationen zu, die nicht zur Nutzung der App-Funktionalitäten notwendig sind, und liegt keine Einwilligung vor, wäre dieser Zugriff rechtswidrig.

In faktischer Hinsicht ist dieses Problem nicht so einfach abgehandelt. Zum einen wird die Rechteverteilung nicht so differenziert möglich sein, wie es die gesetzlichen Vorgaben verlangen. Zum anderen könnte so die KI-App zum Schlupfloch für (unbefugte) Erhebungen von Daten werden. Das Risiko besteht, dass die KI-App, sobald sie Zugriff auf die gespeicherten Daten und Informationen hat, diese ohne ein weiteres Zutun der Nutzer*innen in ihre Systeme aufnimmt, um so große Datenmengen zu sammeln und ihre Funktionen zu verbessern. Ebendiese Gefahr könnte auch von KI-Anwendungen ausgehen, die auf einem Endgerät installiert und nicht über einen Browser genutzt werden.

Hier sollten Unternehmer*innen genaue und im Zweifel strenge Regeln für den Einsatz neuer KI-Anwendungen, KI-Apps und KI-Systemen im betrieblichen Kontext aufstellen, um Risiken zu minimieren.

05. Geschäftsgeheimnisschutz

1. Rechtlicher Schutz

Die Beschränkung des Zugriffs von KI-Systemen auf gespeicherte Informationen und Daten ist auch aus einem ganz anderen Grund relevant. Diese Daten und Informationen könnten auch sog. Geschäftsgeheimnisse darstellen. Diese sind auch besonders rechtlich geschützt.

Ein Geschäftsgeheimnis ist gem. § 2 Nr. 1 Geschäftsgeheimnisschutzgesetz (GeschGehG) eine Information,

- ▶ die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und
- ▶ die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- ▶ bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Geschäftsgeheimnisse gehören quasi zum Kern des Unternehmens. Sie sind mithin diejenigen Informationen, die einen (gewichtigen) Teil des Wertes des Unternehmens ausmachen, wie zum Beispiel besondere Rezepturen, Code für

bestimmte Anwendungen, bestimmte Zusammensetzungen, aber auch Listen von Kundinnen und Kunden, Verträge und deren Inhalte oder Konzeptionen.

Geschäftsgeheimnisse in diesem Sinne sind gesetzlich besonders geschützt und dürfen nicht unrechtmäßig erlangt, genutzt und offengelegt werden. Diese Gefahr bergen jedoch KI-Systeme, wenn sie zur Weiterentwicklung von Rezepturen, Quellcode oder Ähnlichem verwendet werden. Besonders problematisch dabei ist, dass diese Informationen bei Eingabe nicht nur verarbeitet werden, um die Ausgabe zu generieren, sondern auch zur Weiterentwicklung und Schulung der Künstlichen Intelligenz gespeichert und aufbewahrt werden können. Dies könnte sogar so weit gehen, dass die KI davon ausgeht, dass die eingegebenen Informationen allgemeinbekannte Informationen über das Unternehmen sind und diese somit an anderer Stelle freigibt. In jedem Fall haben jedoch die Entwickler oder Anbieter der Software Zugriff auf diese Informationen und könnten diese für eigene Zwecke nutzen.

So könnten also die rechtlich geschützten Informationen unrechtmäßig offengelegt und genutzt werden. Das sind Rechtsverletzungen des Geschäftsgeheimnisschutzes.

Aber auch vertragliche Regelungen können bestimmte Informationen, die das Geschäftsverhältnis der Parteien betreffen, besonders schützen. Dies wird häufig durch die Aufnahme sog. „Vertraulichkeitsvereinbarungen“ („non-disclosure agreement“ / „NDA“) in die Vertragsstruktur gewährleistet. In den Vertraulichkeitsvereinbarungen können dann gewisse Informationen, die zwischen den Parteien ausgetauscht wurden und werden als „vertraulich“ definiert sowie der Umgang mit diesen Informationen genau festgelegt werden. Die Weitergabe der Daten über die Grenzen der Vertraulichkeitsvereinbarung hinaus stellt einen Vertragsbruch dar, der Schadensersatz- und Unterlassungsansprüche nach sich ziehen kann. In vielen Fällen wird bereits in der Vertraulichkeitsvereinbarung selbst eine empfindliche Vertragsstrafe festgelegt, deren genaue Höhe im Zweifel in das Ermessen des Gerichts gelegt wird.

Aber auch die Rechtsfolgen der Verletzung der Regelungen des Geschäftsgeheimnisschutzgesetzes reichen von Unterlassungsansprüchen bis hin zu Schadensersatz oder einer monetären Abfindung. Im Zweifel werden die entstandenen Ansprüche gerichtlich durchgesetzt. Das stellt ein hohes wirtschaftliches Risiko dar.

Nutzer*innen von KI-Systemen sind also gleich aus mehreren Gründen gut beraten, vertrauliche Informationen bei der Nutzung einer solchen Anwendung nicht preiszugeben.

2. Technisch-organisatorischer Schutz

Darüber hinaus können Unternehmer*innen auch präventiv tätig werden und einige technische und organisatorische Maßnahmen treffen, um ihre (vertraulichen) Informationen und Geschäftsgeheimnisse besonders zu schützen.

Wie bereits kennengelernt, sollten alle Anwendungen und Apps, die auf Künstlicher Intelligenz basieren, auf zu weitreichende Zugriffsrechte geprüft und gegebenenfalls konfiguriert oder nicht eingesetzt werden. Darüber hinaus ist es sinnvoll, eine Art „Zugriffstransparenz“ zu schaffen. Die Nachverfolgung, wer in dem internen System auf sensible Daten zugegriffen hat, hilft im Falle eines Leaks bei der Ahndung der unbefugten Weitergabe oder bei der Sensibilisierung der Mitarbeitenden. Zugriff sollten ohnehin nur diejenigen Personen im Unternehmen haben, deren Arbeit mit den vertraulichen Informationen eng zusammenhängt. Die Rechtevergabe, z.B. in Bezug auf einzelne Laufwerke oder Ordnerstrukturen, sollte hierbei immer sinnvoll und restriktiv gehandhabt werden. Werden Daten nicht mehr benötigt, so sollten sie automatisiert gelöscht werden. Dies minimiert das Risiko zufälligen Zugriffs bei (über-) langer Aufbewahrung. In organisatorischer Hinsicht sollten alle Mitarbeitenden über Intrusionsrisiken und den richtigen Umgang mit vertraulichen Informationen, vor allem in Bezug auf den Einsatz von KI-Systemen, geschult und regelmäßig sensibilisiert werden.

Es gibt natürlich eine Vielzahl weiterer Maßnahmen, die getroffen werden können. Dies hängt unter anderem aber auch von der Unternehmensstruktur sowie den räumlichen, technischen und personellen Gegebenheiten ab. Ob deine Maß-

nahmen ausreichen, um die bei dir gespeicherten Informationen zu schützen, bzw. welche Maßnahmen du noch treffen kannst, bevor du das anvisierte KI-System in deinem Unternehmen etablierst, erarbeiten wir gerne mit dir zusammen. Komm einfach auf uns zu!

06. Haftungsfragen im Zusammenhang mit autonomen Systemen

Künstliche Intelligenzen sind nicht fehlerfrei. Aufgrund von falschen Informationen oder schlechten Lernprozessen kann es dazu kommen, dass die KI Fehlentscheidungen trifft, falsche Informationen wiedergibt oder der Output gegen geltendes Recht verstößt.

Doch wer haftet in solchen Fällen? Wer kann zur Verantwortung gezogen werden, wenn die Künstliche Intelligenz nicht wie erwartet Glanzleistungen vollbringt?

1. Wer haftet?

Stellt man einer generativen Sprach-KI diese Fragen, erhält man folgende Antwort:

„Als KI-basierte Sprach-KI liefere ich Antworten auf Basis von statistischen Wahrscheinlichkeiten und dem bestmöglichen Verständnis Ihrer Frage. Ich tue mein Bestes, um genaue und informative Antworten zu liefern, aber ich bin nicht perfekt und meine Antworten können fehlerhaft sein. In jedem Fall liegt die Verantwortung für die Nutzung und Anwendung der von mir bereitgestellten Informationen und Ratschläge beim Nutzer. Weder ich noch meine Entwicklerfirma [...] können für Schäden oder Verluste haftbar gemacht werden, die sich aus der Verwendung der bereitgestellten Informationen ergeben.“

Dass die Anbieter wenig Interesse an einer vollumfassenden Haftung haben, sollte an dieser Stelle niemanden mehr wundern. Ob jedoch die Haftungsfrage so eindeutig und so einfach geklärt werden kann, bleibt fraglich.

Die Haftung richtet sich grundsätzlich nach der Risikoverteilung zwischen den Parteien. Es gibt auch Fälle der gesetzlichen Haftungsverschiebung bzw. Haftungsverteilung oder es werden von der Rechtsprechung in Bezug auf diverse Anwendungsfelder Haftungsquoten unter bestimmten Voraussetzungen gebildet. Dies ist bei Künstlicher Intelligenz (noch) nicht der Fall.

Im deutschen Recht ist es ferner sehr schwierig, vor allem gegenüber Verbraucherinnen und Verbrauchern die Haftung generell auszuschließen. In den Nutzungsbedingungen bekannter KI-Anwendungen finden sich jedoch solche umfassenden Haftungsausschlüsse. Diese haben im Zweifel in der Folge keinen oder nur sehr eingeschränkten rechtlichen Bestand.

Damit verbleibt es zunächst bei der Bewertung der Haftung nach der Risikoverteilung. Doch wer trägt bei der Nutzung von Künstlicher Intelligenz welches Risiko? Und sind diese Systeme nicht viel zu komplex, autonom und undurchsichtig, um dem*der einfachen Nutzer*in die Haftung aufzubürden? Wie werden diese Fragen von einem Dritten/einer Dritten beantwortet, wenn er*sie die geschädigte Person ist? Wie soll diese Person diese Haftungsmaßstäbe verteilen bzw. beweisen? Wer soll verklagt werden?

Diese Fragen lassen sich nicht abschließend klären. Aus unserer Sicht sollte jedoch bei der Abwägung die Komplexität der Künstlichen Intelligenz und die bessere Position der Entwickler und Anbieter berücksichtigt werden. Diese könnten im Entwicklungs- und Vermarktungsprozess Mittel und Wege finden, um die Risiken eines Schadenseintritts zu

minimieren. Das sollte bei der Haftungsfrage berücksichtigt werden.

Spricht man die generative Sprach-KI darauf an, dass ja auch die Quellen, aus der sie lernt, fehlerhaft sein können und fragt sie, wer dann für die Haftung in Betracht käme, erhält man folgende Antwort.

„Als KI-Modell werde ich von [...] trainiert, um eine Vielzahl von Aufgaben auszuführen. [...] verwendet dabei große Datenmengen, um meine Fähigkeiten zu verbessern und mich auf eine Vielzahl von Aufgaben vorzubereiten. Die Verantwortung dafür, dass die Quellen korrekt und vertrauenswürdig sind, liegt jedoch bei den Datenanbietern und nicht bei [...].“

Verschärft man das Szenario und bildet den imaginären aber denkbaren Fall, dass die Anbieter bewusst unwahre und falsche Quellen zur Weiterentwicklung der KI nutzen, erhält man auf die Frage nach der Haftung folgende Antwort.

„Wenn [...] jedoch bewusst falsche oder fehlerhafte Quellen verwendet, um mich zu trainieren, könnte dies schwerwiegende rechtliche und ethische Fragen aufwerfen. In diesem Fall könnten [...] und seine Mitarbeiter haftbar gemacht werden, wenn sie beispielsweise gegen Gesetze oder ethische Standards verstoßen.“

In solch einem Fall sieht selbst die Künstliche Intelligenz die Anbieter zumindest potenziell in der Haftung. Aber nun genug der Rechtsfortbildung unter Zuhilfenahme von Künstlicher Intelligenz. Nicht, dass am Ende jemandem aufgrund von Fehlinformationen Schaden entsteht und man die Haftungsfrage letztlich klären müsste.

2. Europäische Richtlinie zur Haftung von KI

Jetzt mal im Ernst: Ohne zumindest eine Stoßrichtung zu nennen, möchten wir das Thema der Haftung in diesem Whitepaper nicht abschließen.

Im Herbst 2022 haben das Europäische Parlament und der Europäische Rat einen Vorschlag zu einer Richtlinie „zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz“, die sogenannte Richtlinie über KI-Haftung, gefasst. Eins vorab: Sie wurde (noch) nicht final beschlossen und wird wohl im Lichte des KI-Gesetzes gesehen bzw. mit diesem in Kongruenz gebracht werden müssen. Im Ergebnis wird der europäische Gesetzgeber auf dualen Wege (direkt wirkendes Gesetz, indirekt wirkende Richtlinie) die wichtigsten Punkte in Bezug auf den Einsatz von Künstlicher Intelligenz rechtlich behandelt und festgelegt haben.

Das Bedürfnis nach einer europaweiten Richtlinie liegt genau in der Schwierigkeit, die oben aufgeworfenen Fragen zu beantworten. In Bezug auf die Haftung bestehen (noch) keine klaren, einheitlichen Grundsätze. Das schafft Rechtsunsicherheit, die die Richtlinie versucht einzudämmen und zu beheben. Vor allem soll die Richtlinie aber die Opfer stärker schützen.

Zum einen ist eine Beweislastleichterung durch eine Kausalitätsvermutung vorgesehen. Soweit die Opfer nachweisen können, dass jemand, z.B. Anbieter, für die Nichteinhaltung einer bestimmten für den Schaden relevanten Verpflichtung verantwortlich war und dass ein ursächlicher Zusammenhang mit der KI-Leistung nach vernünftigem Ermessen wahrscheinlich ist, sollen die Gerichte davon ausgehen dürfen, dass vorbenannte Nichteinhaltung den Schaden verursacht hat. Diese Vermutung ist widerlegbar.

Zum anderen sollen Opfer einfacheren Zugang zu einschlägigen Beweismitteln erhalten. Es soll ihnen möglich sein, bei Gericht zu beantragen, die Offenlegung von Informationen über Hochrisiko-KI-Systeme anzuordnen. Damit soll es den Opfern leichter gemacht werden, Personen zu identifizieren, die haftbar gemacht werden könnten, sowie herauszufinden, was genau zu dem Schaden geführt hat.

Tatsächlicher Haftungsfragen im Sinne einer festgelegten Haftungsverteilung nimmt sich die Richtlinie leider nicht

umfassend an. Sie hat nicht zum Ziel, jeden Fall bis in das letzte Detail rechtlich zu regeln. Das kann sie im Zweifel auch aufgrund der Agilität in diesem Sektor gar nicht. Unter Umständen ist die Richtlinie oder das KI-Gesetz schon bei Erlass nicht mehr auf dem neusten Stand des technischen Fortschritts. Im Zweifel müssen die aufgeworfenen Fragen durch einen Rückgriff auf ganz allgemeine Haftungsgrundsätze beantwortet werden. Es bleibt also spannend, ob ein nationales oder supranationales Regelwerk, oder aber richterliche Rechtsfortbildung final Licht in das Dunkel der Haftungsfragen bringen werden.

Von der Richtlinie umfasst sein sollen alle KI-Systeme, unabhängig ihrer Klassifikation durch das KI-Gesetz. Richtlinien müssen in nationale Gesetze umgesetzt werden. Sie wirken nicht unmittelbar. Sie können nur „direkt“ Wirkung entfalten, wenn ein Gericht eine Norm richtlinienkonform auslegen muss. Bis die Richtlinie endgültig erlassen und in nationales Recht umgewandelt worden ist, wird es vermutlich noch etwas dauern.

Hier lohnt es sich, die Entwicklungen im Blick zu behalten.

07. Handlungsempfehlungen und Ausblick

Gegen Ende dieses Whitepapers möchten wir dir noch einige Tipps und Tricks im Umgang mit generativen KI-Systemen geben. Über die Risiken und rechtlichen Fragen bist du nun ausreichend aufgeklärt, um für dich selbst einen verantwortungsvollen und risikoarmen Umgang mit diesen Tools definieren zu können.

1. Nutzung und Nutzungsbedingungen von KI

Vor der Nutzung empfiehlt sich immer ein Blick in die Nutzungsbedingungen der jeweiligen Anwendung. Hier können die Hersteller Dos and Don'ts definieren, in die Anwendung einführen und – unter Umständen und vorbehaltlich rechtlicher Prüfung – erste juristische Fragen zwischen Nutzer*in und Hersteller klären. Solche Nutzungsbedingungen oder „Terms of Use“ schauen wir uns am Beispiel verschiedener Anwendungen mal genauer an.

In den Nutzungsbedingungen können zum Beispiel Regelungen über die Nutzungsgruppe und das Mindestalter getroffen werden. OpenAI beschreibt in seinen „Terms of Use“, dass die Nutzung für Personen unter 13 Jahren untersagt ist. Bis zur Vollendung des 18. Lebensjahres kann eine Nutzung nur mit Genehmigung durch die Eltern oder den*die gesetzliche*n Vertreter*in vorgenommen werden.

Ferner können Regelungen getroffen werden zur Anlage und Weitergabe von Accounts der Nutzer*innen. So wird oft festgelegt, dass die Angaben über den*die Nutzer*in vollständig und richtig sein müssen. Ein Verstoß gegen solch eine Regel kann zum Beispiel mit dem Nutzungsausschluss geahndet werden. Dies sollte bei der Erstellung von Profilen bewusst sein.

Die Neuroflash GmbH, Hamburg, Deutschland, („Neuroflash“) trifft zum Beispiel folgende Regelung in ihren „Allgemeinen Geschäftsbedingungen“: Das Teilen eines Anmeldekontos unter mehreren Anwenderinnen und Anwendern wird untersagt und mit Anpassung der Ausgabequalität bis hin zur Sperrung oder Löschung des Kontos verfolgt. Hier werden sogar Regelungen zum „fair use“ und dem Nutzungsverhalten der Anwender*innen getroffen. So sollen Anwender*innen bei übermäßiger Nutzung vorübergehend von dieser ausgeschlossen werden. Übermäßig soll die Nutzung sein, wenn die nutzende Person „mehr als 2,25 Mio. Wörter pro Monat verbraucht“. Für die Erstellung von Content herrschen im Übrigen Restriktionen: Verboten bei Neuroflash ist „die Erstellung von sexuellen, religiösen und politischen Inhalten“.

Bereits nach der Lektüre weniger Nutzungsbedingungen wird klar, dass ein Blick in ebensolche vor der Nutzung eines Dienstes empfehlenswert ist. Oft werden Verstöße gegen die Nutzungsbedingungen mit dem Ausschluss der Nutzung oder der Sperrung von (bestimmten) Funktionen geahndet.

Dennoch sollte immer kritisch hinterfragt und im Zweifel auch geprüft werden, ob all diese Regelungen bestandsfähig sind und damit tatsächlich berücksichtigt werden müssen.

Wenn die Nutzungsbedingungen, also die „Spielregeln“, bekannt sind, kann es mit der Nutzung der Anwendung losgehen. Doch wie geht das richtig?

2. Prompts und Prompt-Engineering

Künstliche Intelligenz setzt den Eingabebefehl der nutzenden Person auf Grundlage ihres Daten- und Wissensstands um. Den Datenbestand einer Künstlichen Intelligenz können Nutzer*innen nur schwer ändern. Einzig durch die Nutzung sowie dem konstanten Feedback kann dazu beigetragen werden, den Bestand zu vermehren. Einfluss nehmen können die Nutzer*innen jedoch darauf, welche Art und Qualität die Eingaben haben, die sie tätigen.

Bessere Eingaben führen auch zu besseren Ergebnissen. Mittlerweile haben sich einige Verhaltensmuster etabliert, um die Qualität der Eingaben zu optimieren. Gerne noch eines vorweg: Oftmals hilft die Umformulierung der Frage bzw. des Befehls, da im Bereich der Künstlichen Intelligenz die „trial and error“-Methode aus der Wissenschaft noch gut anwendbar ist. Nun aber zu den Tipps:

Die Sprache sollte klar und deutlich sein. Kürzere Sätze können besser verarbeitet werden als zeilenlange Schachtelsätze. Soweit möglich sollte Fachjargon oder Umgangssprache, Dialekt und/oder Slang vermieden werden. Es hilft, wenn man sich die KI als „gewöhnliche*n Gesprächspartner*in“ vorstellt und auch so mit ihr interagiert. Wo immer möglich, sollte der Befehl kontextualisiert und mit weiteren Folge-Eingaben vervollständigt oder konkretisiert werden. Soweit ein Text oder ähnliches als Ausgabe herauskommen soll, kann man bereits bei der Eingabe die Tonalität und den Schreibstil festlegen.

Bei der Eingabe sollte man auch mit den genutzten Worten spielen. Erzielt die generative KI beim ersten Anlauf nicht das erwünschte Ergebnis, kann die Eingabe nochmals unter Nutzung von Synonymen getätigt werden. Es kann auch helfen, den Satzbau umzustellen.

Eine weitere Möglichkeit, ist die KI selbst zum sog. Prompt-Engineering einzusetzen. Stelle ihr die Frage, welche Rückfragen sie gerne beantwortet hätte, um den Prompt und die Zielrichtung besser zu verstehen und umsetzen zu können. Deine Erfolge und Misserfolge kannst du natürlich auch dokumentieren und so einen Überblick behalten, welcher dieser Tipps dir persönlich am meisten gebracht hat. Mit der Zeit werden deine Eingaben dann immer besser!

3. Ausblick

Zu Beginn haben wir uns aus dem Fenster gelehnt und behauptet, KI sei auf jeden Fall auch Teil der (informationstechnischen) Zukunft. Das sehen auch die Anbieter von KI so. Während wir die bestehenden Systeme nutzen und lernen, mit ihnen umzugehen, forschen die Anbieter bereits daran, wie man die Anwendungen optimieren und weiterentwickeln kann. Aber auch die andere Position wird vertreten: Eine Vielzahl von Forschenden hat sich bereits früh zusammenschlossen und verlangt, dass die Entwicklung großer KI-Modelle verlangsamt werden soll. Das ist aufgrund all der in diesem Whitepaper aufgeworfenen Fragen und Risiken gut verständlich – und diese stellen nur eine grobe Übersicht dar.

Trotz der berechtigten Kritik möchte das verantwortliche Ministerium das Potenzial der Künstlichen Intelligenz nutzen und weiterentwickeln. Aus diesem Grund hat das Bundesministerium für Bildung und Forschung (BMBF) im August 2023 einen Aktionsplan vorgestellt, der die folgenden Punkte umfasst:

- ▶ Die exzellente Basis Deutschlands bei Forschung und Kompetenzen im Bereich KI wird in sicht- und messbare wirtschaftliche Erfolge und einen konkreten spürbaren Nutzen umgesetzt.
- ▶ KI wird europäisch gedacht, mit dem Ziel vertrauenswürdiger KI „Made in Europe“ und einer optimalen Verzahnung mit den bisherigen nationalen Stärken.
- ▶ Der Dialog- und Strategieprozess zu KI mit anderen Ressorts, den Bundesländern, weiteren Stakeholdern und auf europäischer Ebene wird gezielt und ergebnisorientiert vorangetrieben.

Bundesministerin für Bildung und Forschung, Frau Bettina Stark-Watzinger, sieht Deutschland als exzellenten Standort für die Forschung und Entwicklung von Künstlicher Intelligenz. Im Ergebnis wird das BMBF in der laufenden Legislaturperiode über 1,6 Milliarden Euro in Künstliche Intelligenz investieren.

Das Thema ist also nicht vom Tisch. Unternehmer*innen und Selbstständige sind jetzt angehalten, Regelungen zum Umgang mit Systemen, die Künstliche Intelligenz nutzen, zu definieren und ihre Mitarbeitenden zu schulen und zu sensibilisieren. Zudem sollte in Bezug auf die technischen Aspekte geprüft werden, ob die Anwendungen optimal und datenschutzsicher eingestellt sind und ob die im Unternehmen getroffenen technischen sowie organisatorischen Maßnahmen unter Berücksichtigung der mit dem Einsatz von Künstlicher Intelligenz verbundenen Risiken ausreichend sind. Ferner sollten datenschutzrechtliche Dokumente wie Datenschutzerklärung, Verzeichnisse für Verarbeitungstätigkeiten und Musterverträge (z.B. zur Auftragsverarbeitung) auf Aktualität unter Berücksichtigung der sich durch den Einsatz von Künstlicher Intelligenz stellenden Fragen geprüft werden. Nicht zuletzt sollte auch das Lizenzmanagement in Bezug auf urheberrechtlich geschützte Werke an die neuen Bedürfnisse angepasst und optimiert werden.

...es gibt also genug zu tun! Wollen wir gemeinsam anfangen?

MORGENSTERN Academy Seminare & Co.

ChatGPT, Lensa & Co. | Wie du Künstliche Intelligenz in deinem Unternehmen rechtssicher einsetzen kannst

Bei der Nutzung von Künstlicher Intelligenz werden einige Rechtsgebiete berührt: Das Urheberrecht, das Datenschutzrecht, der Geschäftsgeheimnisschutz und viele mehr. Nur wer einen groben Überblick über die rechtlichen Widrigkeiten hat, kann KI verantwortungsbewusst und rechtssicher nutzen.

Das dazu notwendige Wissen holst du dir am besten direkt im Seminar ab!



Academy Shop



MORGENSTERN Rechtsanwaltsgesellschaft mbH

Große Himmelsgasse 1

DE - 67346 Speyer

Telefon

+49 (0) 6232 - 100119 0

E-Mail

contact@morgenstern-legal.com