Was ist Maschinelles Lernen?

In den letzten 20 Jahren hat sich Maschinelles Lernen daher als zentrale Technologie zur Entwicklung von KI durchgesetzt. Das Problem der mangelnden Regelkenntnis lässt sich damit umgehen. Dabei lernen Computer die Muster und Regeln zur Lösung einer Aufgabe, indem sie eine große Menge an Beispieldaten durcharbeiten und auf diese Weise die statistischen Zusammenhänge und Regeln selbst finden. *Machine-Learning-Algorithmen* bezeichnen dabei die Programme, mit denen die Daten durchgearbeitet werden, um diese Zusammenhänge zur Lösung der gestellten Aufgabe aus den Beispieldaten abzuleiten. Wenn wir heute von KI sprechen, meinen wir zu einem überwiegenden Teil Anwendungen, die mit Maschinellem Lernen entwickelt wurden. Diese beiden Begriffe werden heute – technisch nicht ganz korrekt – oft austauschbar verwendet.

Ein Beispiel zur technischen Veranschaulichung: Ein traditioneller Ansatz bei der Programmierung funktioniert nach festen Regeln. Wenn man zum Beispiel möchte, dass eine Heizung die Temperatur in einem Raum reguliert, könnte man feste Anweisungen vorgeben: „Wenn es zu kalt ist, schalte die Heizung ein. Wenn es zu warm ist, schalte sie aus." Diese Methode ist direkt und einfach, allerdings kann das System nicht über diese vorprogrammierten Anweisungen hinaus lernen oder sich an neue Situationen anpassen.

Im Gegensatz dazu ermöglicht Maschinelles Lernen einem System, aus Daten zu lernen und sich anzupassen, ohne dass jede einzelne Handlung vorher fest programmiert werden muss. Statt starrer Regeln lernt es zum Beispiel aus vergangenen Temperaturdaten und anderen Umweltfaktoren, zu welchem Zeitpunkt Sie in der Vergangenheit unter welchen Bedingungen die Heizung eingeschaltet haben. Daraus erstellt es für sich eine Theorie, wann und wie die Heizung basierend auf den tatsächlichen Bedingungen und Verhaltensmustern aktiviert oder deaktiviert werden sollte. Dies führt auf Basis der statistischen Analyse von Trainingsdaten zu einer intelligenteren und effizienteren Steuerung, die sich dynamisch an unterschiedliche Situationen anpasst, sofern die KI diese Situationen aus den Trainingsdaten kennt.

Maschinelles Lernen ist nie zu 100 % verlässlich

Wir haben zuvor schon gelernt, dass KI auf der Grundlage von Maschinellem Lernen ihre Ergebnisse immer nur auf Basis von Schätzungen und Wahrscheinlichkeiten ausgeben kann. Wenn eine Bilderkennungs-KI zum Beispiel sagt, dass es sich zu 85 % um einen Hund handelt, den das Bild zeigt, bedeutet das im Umkehrschluss immer auch, dass es sich zu 15 % nicht um einen Hund handelt.

Das ist eine Konsequenz daraus, wie sie technisch arbeitet. Vergleichbar ist das mit repräsentativen Meinungsumfragen, die immer auch eine sogenannte Schwankungsbreite haben, das heißt einen Bereich, innerhalb dessen die Umfrage keine gesicherte Antwort geben kann. Das liegt nicht an einer mangelhaften Durchführung der Umfrage, sondern hat statistische Gründe. Sobald wir in der Datenerhebung ein Zufallselement haben, ist die Antwort nicht gesichert. Und das ist nicht nur bei Umfragen, sondern auch beim Erstellen von KI durch Maschinelles Lernen der Fall.

Die Vorstellung, dass KI immer recht hat und durch den Menschen nicht infrage gestellt werden darf, ist also definitiv falsch, weil jede KI in gewissem Ausmaß auch notwendigerweise ungenau ist. Das soll kein Hindernis sein, die Technologie zu verwenden, aber man muss vor der Anwendung überlegen, ob in einem bestimmten Anwendungsfall diese Ungenauigkeiten akzeptiert werden können. Im Fall eines EM-Chatbots zu den Fussballregeln würden fehlerhafte Antworten wahrscheinlich keine allzu ernsthaften Konsequenzen haben, im Fall eines Chatbots, der Laien in Rechtsfragen berät, allerdings sehr wohl. Menschliche Kontrolle ist in solchen Situationen auch noch eine Option, um diese Frage zu lösen.

Dass jedes KI-Ergebnis grundsätzlich auch fehlerhaft sein kann, bedeutet natürlich nicht, dass Künstliche Intelligenz Aufgaben nicht besser und genauer lösen kann als Menschen, die ebenfalls im Verdacht stehen, hin und wieder Fehler zu machen. Und viele Modelle arbeiten heute bereits besser als Menschen – wie zum Beispiel hinsichtlich Erkennung von Objekten auf Fotos, bei der die KI bereits seit Jahren eine höhere Genauigkeit erzielt als der durchschnittliche Mensch.

Maschinelles Lernen ist weder objektiv noch frei von „Vorurteilen“

Die Annahme, dass KI „objektiv“ sei, entsteht bei vielen oft dann, wenn sie hören, dass KI beim Training gewaltige Datenmengen statistisch auswertet.

… keine Wartung mehr braucht, sobald sie einmal im Einsatz ist?

Das ist manchmal wahr, manchmal aber auch nicht. Eine KI kann immer nur das beurteilen, was sie beim Training gelernt hat. Wenn sich die Welt verändert, muss die KI angepasst werden, denn die Beispieldaten aus dem ursprünglichen Training können die aktuelle Welt ja nicht mehr korrekt abbilden. Wenn beispielsweise ein KI-System dazu dient, schadhafte Produkte in einer Fabrik zu erkennen, muss es angepasst werden, sobald die Produktpalette geändert wird und die Produkte dadurch anders aussehen. Dasselbe ist notwendig, wenn Sie zum Beispiel im Jahr 2019 für eine Supermarktkette ein KI-Modell zur Prognose des Absatzes von Toilettenpapier entwickelt haben, das auf Basis der Verkaufszahlen von Toilettenpapier aus den Jahren 2016 bis 2019 basiert, um damit die Lagerhaltung zu optimieren und besser zu wissen, an welchen Tagen mehr gelagert werden muss. Das Modell funktioniert wahrscheinlich ganz gut – bis zum Februar 2020, in dem sich das Nachfrageverhalten nach Toilettenpapier gänzlich verändert. Dann wird das KI-Modell, das mit der „alten Realität“ trainiert wurde, für Sie keinen Mehrwert mehr haben und wahrscheinlich sogar kontraproduktiv sein.

Es hängt also sehr vom Einzelfall ab, wie lange man KI-Modelle verwenden kann.

Was ist Generative KI? Von ChatGPT bis zur Pharmaforschung

Seit November 2022 können wir kaum eine Zeitung aufschlagen oder eine Party besuchen, ohne auf Neuigkeiten über die beeindruckenden Fähigkeiten von Generativen KI-Tools wie ChatGPT zu stoßen. Diese können realistische Bilder erstellen oder komplexe Fragen beantworten. Wir wissen jetzt, was Künstliche Intelligenz (KI) ist – doch was genau ist „Generative KI“?

Was ist Generative KI?

„Generativ“ bedeutet „erzeugend“: Der Begriff bezeichnet die Eigenschaft, neue Dinge hervorzubringen. Generative KI bezieht sich auf eine Form der

TIPP: MULTIMODALE SPRACHMODELLE

Google Gemini

https://gemini.google.com/

OpenAI GPT-4o

https://openai.com/index/hello-gpt-4o/

Wie funktioniert Generative KI?

Keine Sorge, wir werden hier nicht in technische Details einsteigen, sondern lediglich einen intuitiven (und technisch extrem vereinfachten) Einblick geben, wie ChatGPT & Co es schaffen, so beeindruckende Ergebnisse zu erzielen.

Generative KI-Modelle werden mit Beispieldaten trainiert, um zu lernen, wie sie neue Daten erzeugen können, die den ursprünglichen Daten ähnlich sind.

Was bedeutet das im konkreten Fall von ChatGPT und dem Wissen, das wir uns vorher über Maschinelles Lernen erarbeitet haben?

Zur Erinnerung: Maschinelles Lernen bezeichnet eine Methode, Computern das Imitieren von menschlichen Fähigkeiten beizubringen, indem man ihnen eine Aufgabe stellt, dann Beispiele für die Lösung zeigt und sie auffordert, die Beispieldaten selbstständig durch statistische Analyse zu durchsuchen, um die Muster zur Lösung der gestellten Aufgabe selbst zu finden.

Wie haben KI-Entwickler ChatGPT nun gebaut?

Sie haben dem Computer die Aufgabe gestellt, dass er lernen soll zu imitieren, wie wir Menschen Sprache bilden, indem wir Wörter aneinanderreihen. Das sollte er lernen, indem er durch statistische Analyse eine Unmenge von Texten daraufhin untersucht, welche Wörter wir typischerweise aneinanderreihen, wenn wir kommunizieren.

Darf ich Ergebnisse von KIs verwenden? Und wenn ja – wie genau?

Sie haben sicher gehört, dass viele Autoren und Künstler Unternehmen, die Generative KI-Modelle bauen, wegen Urheberrechtsverletzungen klagen, weil diese Unternehmen für das Training der KI-Modelle die Texte und Bilder der Künstler verwendet haben sollen. Im Fall der musikgenerierenden Tools Suno und Udio haben die Entwickler schon offen zugegeben, dass ihre KI mit fremden Werken trainiert wurde, ohne besondere Erlaubnis der Musikschaffenden.

Die Frage, ob die Verwendung solcher urheberrechtlich geschützten Inhalte zum Bau der Modelle ohne Zustimmung der Künstler legal ist, wird wohl erst in den nächsten Jahren durch Höchstgerichte auf unterschiedlichen Kontinenten entschieden werden. Diese Frage betrifft primär die Entwickler der Modelle, wie OpenAI oder Microsoft. Ob und welche Auswirkungen dieser Aspekt auch für Sie als Anwender haben kann, diskutieren wir in diesem Kapitel.

Die Intensität der öffentlichen und rechtlichen Auseinandersetzung zeigt deutlich, wie heikel dieses Thema ist. Auf den ersten Blick ist es Ihnen vielleicht egal, welche Daten ChatGPT verwendet hat, um das Modell zu trainieren. Gleichzeitig ist es ChatGPT egal, was Sie als Anwender mit dem Ergebnis der KI tun. Seien Sie achtsam: Wie wir lernen werden, liegt ein großer Teil der Verantwortung im Umgang mit KI bei Ihnen, dem Nutzer. Daher wollen wir nun die wichtigsten rechtlichen Aspekte aufarbeiten.

Schauen wir uns zuerst an, was das Urheberrecht eigentlich alles regelt.

Urheberrecht verstehen: Grundlagen für Anwender

Worum geht es im Urheberrecht?

Das Urheberrecht möchte in erster Linie jene Personen schützen, die kreative Leistungen erbringen. Diese Personen sollen darüber entscheiden können, wer die Rechte an ihren Werken haben darf und wie diese genutzt werden sollen.

Diese Rechte umfassen – ganz grob gesprochen – zwei Arten: Erstens die *Verwertungsrechte*, das heißt, als Urheber selbst zu bestimmen, wofür das

Also nochmals die Faustregel kurz gefasst: Wenn es von Anfang an die Absicht war, das fremde Werk zu verändern und zu bearbeiten, um den Output dann außerhalb der eigenen Privatsphäre zu verwenden, sind wir wieder beim Standardszenario: Sie benötigen die Zustimmung des Originalurhebers.

Wenn aber Ihre Bearbeitung des geschützten Werkes nicht die Privatsphäre, nicht Ihr unmittelbares privates Umfeld verlässt, dann kann das ohne Zustimmung zulässig sein.

Wo ist der Haken an der Sache? Wie schon erwähnt, befinden wir uns hier in einer rechtlichen Grauzone. Und außerdem dürfen wir einen Aspekt nicht übersehen: Wenn Sie ChatGPT verwenden, geben Sie den Input nicht nur an OpenAI weiter, sondern es könnte damit auch trainiert werden und daher dieser Input in wiedererkennbarer Form als Output über einen anderen User veröffentlicht werden.

Zugegeben, das klingt alles sehr theoretisch. Aber in diesem Fall betrifft Ihr Handeln nicht mehr nur Ihre Privatsphäre, sondern tritt darüber hinaus. Daher ist die Ausnahme des Privatgebrauchs im Zusammenhang mit KI noch mit großer Vorsicht zu genießen.

Gibt es noch andere Ausnahmen im Urheberrecht, die ich kennen sollte?

Es gibt einige Vorgänge, die ein Urheber einfach akzeptieren muss. Diese Ausnahmen sind gesetzlich geregelt. Im Wesentlichen geht es dabei um die Aspekte, dass einerseits der Urheber in gewissen Bereichen keinen besonderen Schutz braucht, und andererseits darum, dass es ein überwiegendes Interesse der Allgemeinheit gibt.

Die Grenze bildet auch hier meistens der private Gebrauch. Solange die Nutzung ein Privatvergnügen bleibt und keine Öffentlichkeit mitspielt, benötigt man keine Zustimmung des Urhebers.

Das gilt auch für die Bearbeitung eines urheberrechtlich geschützten Werkes. Wir können davon ausgehen, dass es bei einer großen Anzahl der Anwendungen von Generativer KI darum geht, eine vorhandene Vorlage in irgendeiner Art und Weise zu bearbeiten. Die Bearbeitung ist prinzipiell zulässig, solange ich diesen Output dann für mich behalte und eben nicht beruflich

Grundlagen des Datenschutzrechts

In diesem Abschnitt stellen wir die zentralen Konzepte des Datenschutzes vor, wie sie in der DSGVO definiert sind und auch europaweit gelten.

Was regelt der Datenschutz?

Datenschutz ist ein Grundrecht. Das Ziel des Datenschutzes ist es, Privatsphäre und Geheimhaltungsinteressen aller Menschen zu schützen. Zu diesem Zweck werden für die Verarbeitung von Daten, die Menschen betreffen, bestimmte Regeln aufgestellt.

Der Datenschutz betrifft also nicht alle Arten von Daten, sondern regelt nur den Umgang mit sogenannten *personenbezogenen* Daten. Das sind alle Informationen, die konkrete Menschen beschreiben und dadurch direkt oder indirekt identifizierbar machen.

„Personenbezogen" ist dabei ein sehr weiter Begriff: Dazu gehören Stammdaten wie der Name und das Geburtsdatum, aber auch Daten, die einer Person zuzuschreiben sind, wie ihr Aussehen, ihre Stimme und Hautfarbe, ihre Religion sowie ihre Social-Media-Posts, Fotos, Bankdaten, Gesundheitsbefunde und Kreditkartennummern. Aber auch Informationen, die eine Person eindeutig identifizieren können, wie etwa die IP-Adresse in der elektronischen Kommunikation, sind personenbezogene Daten, genauso wie Arbeitszeitaufzeichnungen. Personenbezogene Daten lauern auch dort, wo man sie im ersten Moment nicht unbedingt vermutet.

Es geht also um allerlei Daten über Menschen. Daten über Unternehmen oder über fiktive Personen sind nicht Gegenstand des Datenschutzes, diese können aber aufgrund anderer Gesetze geschützt sein.

Im Zentrum des Datenschutzes steht die sogenannte *Verarbeitung* der personenbezogenen Daten. „Verarbeitung" umfasst *de facto* jede Art der Verwendung von Daten, das heißt, Daten in irgendeiner Form elektronisch zu speichern, sie in sonstiger Weise zu nutzen oder zu verändern. Schon die bloße Übermittlung personenbezogener Daten an andere Empfänger ist eine Verarbeitung im rechtlichen Sinne.

Was bedeutet Haftung eigentlich?

Haftung ist ein rechtlicher Begriff, der beschreibt, wann und wie eine Person einzustehen hat, wenn etwas in ihrem Verantwortungsbereich schiefgeht. Insbesondere dann, wenn ein Schaden entsteht, stellt sich die Frage: Wer muss den Schaden wiedergutmachen?

Bei der Frage, wer haften kann, gibt es grundsätzlich zwei Möglichkeiten: Es können entweder natürliche oder juristische Personen verantwortlich sein. Es haften also entweder Menschen oder Unternehmen.

Wenn Schäden durch die Anwendung von KI entstehen, gilt demnach: Einerseits können die Entwickler und Anbieter der KI gegenüber ihren Kunden haften – genauso wie jeder andere Hersteller für die Sicherheit seines Produktes verantwortlich ist. Im Fall von ChatGPT ist das das Unternehmen OpenAI als Entwickler. Die Entwickler könnten haften, wenn sie fehlerhafte Software erstellen, die beispielsweise zu wirtschaftlichen Verlusten führt.

Und andererseits können die Nutzer der KI haften, wenn sie die Ergebnisse verwenden und daraus jemand anderem ein Schaden entsteht, etwa durch die Verbreitung fehlerhafter Informationen oder durch Urheberrechtsverletzungen.

Allgemeine Voraussetzung für jede Haftung ist natürlich immer, dass jemand anderer geschädigt wurde, also ein Schaden an einer Person vorliegt – sprich eine körperliche Verletzung – oder ein Vermögensschaden, also ein finanzieller Verlust eingetreten ist. Wenn dann auch noch bewiesen wird, dass der Schaden aufgrund eines Fehlverhaltens verursacht wurde, dann bleibt nur noch die Frage, in welchem Ausmaß der Schädiger die Folgen tragen muss.

Haftungen können verschiedene Formen haben. Wenn jemand durch Ihren Fehler einen finanziellen Schaden erleidet, müssen Sie ihn dafür in der Regel mit Geld entschädigen. Wenn Sie durch einen Fehler gegen ein Gesetz verstoßen, kann das in schweren Fällen sogar zur strafrechtlichen Verfolgung führen.

Und das sind auch schon die zwei wesentlichen Haftungsgrundlagen: Sie müssen für einen Schaden einstehen, wenn Sie gegen ein Gesetz verstoßen oder – was uns hier mehr interessiert, weil im Alltag relevanter – wenn Sie einen Vertrag verletzen.

Was passiert mit KI-Systemen, die ein unannehmbares Risiko mit sich bringen?

KI-Anwendungen mit unabsehbarem Risiko werden in der EU verboten sein. Das sind zum Beispiel *Social Scoring* oder die biometrische Kategorisierung und das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder aus Videoüberwachung, Emotionserkennung am Arbeitsplatz oder kognitive Verhaltensmanipulation. Unzulässig wird auch das *Predictive Policing* sein, also der Versuch, mögliche Straftaten mittels KI aus bestimmten personenbezogenen Daten vorherzusagen.

Dennoch wird es Ausnahmen hinsichtlich dieser Verbote geben, was unter Datenschützern auf viel Kritik stößt. Zum Beispiel sollen Strafverfolgungsbehörden sehr wohl auf biometrische Massenüberwachung zurückgreifen können, zur Verhinderung von Terroranschlägen oder sonstigen schweren Verbrechen.

Und was bedeutet das zum Beispiel für ChatGPT?

Die vorläufige Einschätzung ist, dass ChatGPT im Rahmen der Bewertung durch den AI-Act ein System mit begrenztem Risiko darstellt – aber genau wissen wir es noch nicht, denn bis der AI-Act in ein paar Jahren voll in Kraft tritt, kann sich sowohl technisch als auch rechtlich noch viel tun.

Darüber hinaus sind die KI-Modelle, die den KI-Anwendungen zugrunde liegen, gesondert zu betrachten. Hier wird es spezielle Regelungen für Modelle geben, die in der Lage sind, ein breites Spektrum unterschiedlicher Aufgaben zu erfüllen – dazu zählen unter anderem Video-, Text- und Bilderzeugung oder die Erzeugung von Computercode. Es müssen gewisse Transparenzpflichten erfüllt werden, bevor diese Modelle auf den Markt kommen. Die Unternehmen, die solche sogenannten Basismodelle entwickeln (wie eben OpenAI für ChatGPT), werden die heute schon oft gestellten Fragen im Vorhinein beantworten müssen: Im Rahmen der technischen Dokumentation muss dann Auskunft über die Trainingsdaten und Testverfahren gegeben werden. Außerdem muss in gewissen Bereichen nachweisbar sein, dass geltendes Urheberrecht nicht verletzt wurde.

Kapitel 6

Gesellschaftliche Fragen, die sich durch Generative KI stellen

Viele Menschen sind sich heute sicher: Generative Künstliche Intelligenz (GenKI) wird sich als revolutionäre Technologie erweisen, die in zahlreichen Bereichen umwälzende Anwendungen hervorbringen wird, von denen die Menschheit enorm profitieren kann. Doch wie bei jeder neuen Technologie und jeder Transformation ergeben sich auch hier Herausforderungen, die sowohl technische als auch rechtliche, soziale und ethische Fragen aufwerfen. Die Menschheit hat in ihrer Geschichte bewiesen, dass sie solche Herausforderungen durchaus erfolgreich meistern kann. Und es spricht nichts dagegen, dass wir das auch dieses Mal schaffen. Aber wir dürfen diese Fragen nicht fahrlässig aus den Augen verlieren. In diesem Kapitel wollen wir ein paar der Fragen ansprechen, die wir uns als Menschen stellen müssen.