Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

Haftung der KI

Leitfaden: rechtliche Aspekte der Nutzung Künstlicher Intelligenz

www.itwirtschaft.de

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Inhalt

1 Einführung 3

2 Definition der KI 3

3 KI als Herausforderung 5

3.1 Rechtliche Relevanz des Begriffs 5

3.2 Einsatz der KI 6

4 Rechtlicher Rahmen 10

5 Haftungsfragen 12

5.1 Produkthaftung 12

5.2 Produzentenhaftung 15

5.3 Anwenderhaftung 16

5.4 Datenschutzrechtliche Haftung 17

6 Europäische Initiativen 18

7 E-Person? 20

8 Ausblick 20

9 Kontakt 21

1 Einführung

Seit Jahren wird der Einsatz von **Künstlicher Intelligenz (KI)** in verschiedensten Bereichen unseres Lebens kontrovers diskutiert. Nicht selten stehen dabei die Risiken ihres Einsatzes im Fokus, wohingegen die Untersuchung geltender rechtlicher Rahmenbedingungen keine ausreichende Berücksichtigung findet. Dadurch bleiben jedoch die Chancen und die Potentiale der KI regelmäßig unentdeckt.

Eine besondere Herausforderung besteht dabei darin, dass eine neue technologische Entwicklung einem bestehenden Rechtsrahmen unterworfen werden muss. Grundsätzlich geht der deutsche Gesetzgeber (und in aller Regel auch der europäische) von einer **Technologieneutralität** aus: Rechtliche Vorschriften gelten also unabhängig davon, mithilfe welcher Technologien das eine oder das andere Ereignis zustande gekommen ist.

Wichtig ist dabei – insbesondere im Hinblick auf die gewünschte führende Rolle der deutschen Wirtschaft in der Welt – die Schaffung einer Balance zwischen der Unterstützung von Innovationen, mithin auch von Künstlicher Intelligenz, und dem Schutz der Verbraucher, der Umwelt und des Rechtsverkehrs. Wie kann das Recht einerseits die **Potentiale der KI stärken** und andererseits die damit einhergehenden **Risiken reduzieren**? Diese Frage versuchen wir hier zu beantworten.

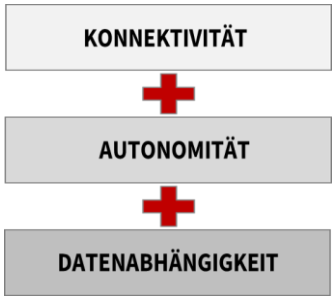
2 Definition der KI

Eine einheitliche Definition der Künstlichen Intelligenz existiert bislang, soweit ersichtlich, nicht. Allen in der Literatur, Praxis und Gesetzgebung angebotenen Definitionsversuchen ist jedoch der Aspekt einer (versuchten) **Simulation eines menschlichen Verhaltens durch Computer-Anwendungen** gemeinsam. Die KI versucht mithin, einzelne genuin menschliche kognitive Aufgaben wie etwa Spracherkennung oder Kunstschaffung auf Computer zu übertragen und mithilfe von Formeln und Algorithmen zu bewältigen.

Die von der Europäischen Kommission im Juni 2018 eingesetzte „Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz“ definiert die KI-Systeme als „vom Menschen entwickelte Softwaresysteme (und gegebenenfalls auch Hardwaresysteme), die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene handeln, indem sie ihre **Umgebung durch Datenerfassung wahrnehmen**, die gesammelten strukturierten oder unstrukturierten Daten **interpretieren**, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten, und über das **bestmögliche Handeln zur Erreichung des vorgegebenen Ziels entscheiden**“ (diese Definition wurde im April 2019 unter https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60664 veröffentlicht).

Europäische Kommission

Im Bericht der Europäischen Kommission an das Europäische Parlament, den Rat und den Europäischen Wirtschafts- und Sozialausschuss vom 19.2.2020 über die *Auswirkung künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung* werden folgende Merkmale der Künstlichen Intelligenz definiert (https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064):



„Künstliche Intelligenz, Internet der Dinge und Robotik weisen viele gemeinsame Merkmale auf. Sie können Konnektivität, Autonomie und Datenabhängigkeit miteinander verknüpfen, um **Aufgaben ohne oder nur mit geringer menschlicher Steuerung oder Aufsicht auszuführen**. KI-gestützte Systeme können zudem ihre Leistung verbessern, indem sie **aus Erfahrungen lernen**.

Ihre Komplexität spiegelt sich sowohl in der Vielfalt, der an der Lieferkette beteiligten Wirtschaftsakteure als auch in der Vielzahl von Komponenten, Teilen, Software, Systemen oder Dienstleistungen wider, die zusammen die neuen technologischen Ökosysteme bilden.

Hinzu kommt die Offenheit für Aktualisierungen und Verbesserungen nach der Markteinführung dieser Technologien. Die enormen beteiligten Datenmengen, der Rückgriff auf Algorithmen und die Opazität der KI-Entscheidungsfindung erschweren die Vorhersage des Verhaltens eines KI-gestützten Produkts und das Verständnis der potenziellen Schadensursachen. Schließlich können Konnektivität und Offenheit KI-Produkte und IoT-Produkte anfällig für Cyberbedrohungen machen."

Bei diesen Beschreibungen fällt besonders ins Auge, dass die KI als eine Technologie verstanden wird, die „**ohne oder nur mit geringer menschlicher Steuerung**" funktioniert. Unser Rechtssystem ist indes darauf gerichtet, menschliches Verhalten zu steuern und ggf. auch zu sanktionieren.

Wie lässt sich also die KI in die bestehenden rechtlichen Rahmenbedingungen einordnen?

3 KI als Herausforderung

3.1 Rechtliche Relevanz des Begriffs

Grundsätzlich werden unter KI, wie oben bereits erwähnt, solche Anwendungen oder technische Systeme aus dem Bereich der Informatik verstanden, die intelligentes menschliches Verhalten nachbilden und auf selbstlernenden Algorithmen basieren. KI besitzt dabei die Fähigkeit, **selbstständig** – also unabhängig von einer äußeren Steuerung oder einem äußeren Einfluss – durch Interaktion sowie Erfahrungen zu lernen. Diese **Lernfähigkeit** ist dabei ein integraler Bestandteil der KI, ihr Kernstück. Sie ermöglicht es auch, dass die KI entweder selbst Entscheidungen trifft oder zumindest die Grundlage für zukünftige Entscheidungen wesentlich verbessert.

Um juristisch die KI und insbesondere die Konsequenzen ihres Einsatzes zu bewerten, reicht indes diese Definition nicht aus. Was also macht die KI im Einzelnen aus?

Die KI stellt ein mehrschichtiges neuronales Netz dar. Sie wird durch Lernalgorithmen in einem Trainingsprozess dazu befähigt, bestimmte Muster und Korrelationen in einem Datenbestand zu erkennen. Daraufhin soll die KI mithilfe bestimmter **Entscheidungsalgorithmen** die in einem

solchen Trainingsprozess gewonnenen Lernergebnisse auf neue Datenbestände übertragen. Dabei ist es sehr schwierig, die Entscheidungsmechanismen und die Lernschritte des Systems nachzuvollziehen. Aufgrund der Vielzahl unterschiedlicher Parameter, Variablen und Interdependenzen innerhalb eines neuronalen Netzes können **Lernvorgänge und Ausgabemuster nicht eindeutig vorhergesagt** werden.

Es wird nicht selten von sog. „**starker**“ und „**schwacher**“ **KI** gesprochen. Schwache KI ist dabei auf die Lösung eines konkreten Problems gerichtet, der Algorithmus umfasst einige (endlich viele) Handlungsoptionen und -Schritte, die mit vorgegebener Datenmenge vorgenommen werden müssen, um zu einem bestimmten Ergebnis zu kommen, das System ist in sich geschlossen und geht über die Lösung des konkreten Problems nicht hinaus. Starke KI ist im Gegensatz dazu ein Versuch, *menschliche Intelligenz zu erreichen* oder sogar zu übertreffen. Zwar wird diese auch durch einen Algorithmus oder Programmierungsbefehl gestartet, entwickelt sich aber selbstständig je nach den gewonnenen Ergebnissen weiter und kann dementsprechend auch den eigenen Algorithmus anpassen, sich selbst neue Fragen stellen und nach Antworten suchen. Während die schwache KI bereits in Anwendung ist, bleibt die starke KI bislang der Forschung und der Fantasie überlassen.

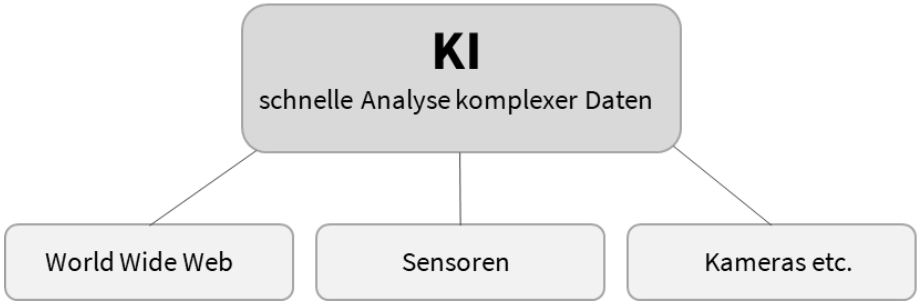
Es lässt sich also festhalten, dass die KI **mathematische Algorithmen** darstellt, die zumindest im vorhandenen Entwicklungsstadium **nicht zur Selbstständigkeit befähigt** werden.

Alle bereits zur Anwendung kommenden KI-Lösungen bewegen sich **innerhalb** der ihnen durch die Programmierung **aufgesetzter Grenzen**, erfüllen nur die Aufgaben, die ihnen gestellt worden sind, basieren auf den vorgegebenen Verfahren und Nutzen für die Analyse die Inputdaten, die ihnen geliefert werden. Diese zentralen Elemente also – Zweck, Verfahren, Ziele – werden vom Menschen programmiert und (zumindest derzeit) von der KI-Lösung nicht verändert. Dementsprechend ist die KI für die juristische Betrachtungsweise einem beliebigen (wenn auch sehr schwierigen) technischen System gleichzustellen.

3.2 Einsatz der KI

Künstliche Intelligenz kommt vor allem dort zum Einsatz, wo eine schnelle Analyse größerer Datenmengen notwendig ist, insbesondere wenn eine solche Analyse als Grundlage für Entscheidungen dienen soll. Besonders die Analyse von vielen unstrukturierten Daten wie

bspw. im Internet veröffentlichten Bildern oder Erkennung von vielen verschiedenen Texten (und eventuell auch Sprachen) stellt ein KI-System auf eine höhere Stufe als das menschliche Gehirn, da eine große Menge von Daten schnell verarbeitet (analysiert) werden kann. Dabei können diese Daten auch aus verschiedenen Quellen stammen, wie etwa Internet, Sensoren, Kameras etc.



Dabei sind zwei Aspekte von besonderer Bedeutung: zum einen das fehlerfreie Programmieren der Algorithmen, zum anderen ausreichende und zuverlässige Trainingsdaten.

Fehlerfreies Programmieren der Algorithmen

Fehlerfreies Programmieren der Algorithmen lässt sich mit juristischen Mitteln einigermaßen gut absichern. Zum einen ist bereits bei der Ausschreibung der Stelle, bei der Anstellung oder bei der Vergabe der entsprechenden Programmieraufgabe darauf zu achten, dass Expertenwissen und ausreichende Fähigkeiten der Bewerberinnen und Bewerber nachgewiesen werden. Ist ein entsprechender Abschluss nicht vorhanden, dafür aber ausreichende Erfahrungen und gute Kenntnisse, lässt sich das durch einen kleinen Test überprüfen. Dabei haben sowohl arbeitsrechtliche (die gewünschte KI-Anwendung wird von einer (mehreren) im Unternehmen neu angestellten Person) als auch werkvertragliche (die gewünschte KI-Anwendung wird von einer (mehreren) Person programmiert, mit der (oder mit dem ganzen Unternehmen) ein schuldrechtlicher Vertrag bezüglich dieser Leistung abgeschlossen wird) Konstellationen ihre Sicherungsmechanismen: das Arbeitsrecht kennt bspw. Probezeit, der Werkvertrag kann bestimmte „Stufen“ und Zwischenergebnisse vorsehen. In beiden Fällen lässt sich also relativ schnell feststellen, ob die für die Programmierung (mit)vorgesehene Person dieser Aufgabe gewachsen ist.

Zum anderen lässt sich die Aufgabe selbst gut vertraglich formulieren. Je besser die Aufgabe definiert und beschrieben ist, desto einfacher ist auch die zufriedenstellende Erfüllung dieser. Ist der Programmiererin oder dem Programmierer ihre oder seine Aufgabe nicht gänzlich klar, können bereits daraus Fehler entstehen. Auch der Einbau besonderer Kontrollen, Zwischenprüfungen und Reporting ist zu empfehlen, lassen sich doch so die möglichen Fehler schnell entdecken und somit auch beseitigen. Denkbar sind darüber hinaus „klassische“ Compliance-Maßnahmen wie etwa Vier-Augen-Prinzip, Zugriffschranken, Verschlüsselung, Redundanz etc.

Zuverlässigkeit von Trainingsdaten

Zuverlässigkeit von Trainingsdaten lässt sich ebenfalls vertraglich (mit)absichern. Folgende Kriterien der Datenqualität können dabei helfen:

Einige Use-Cases in vielen Bereichen wie etwa Autonome Mobilität, Zahnmedizin, Logistik, E-Health oder Fintech lassen sich hier nachlesen.

Produktdesign

- Ein Modehersteller lässt sich von einer KI, die mit Modefotos aus vergangenen Jahrzehnten trainiert wurde, eine neue Kollektion entwerfen.
- Ein Start-up entwickelt eine KI, mit der anhand von Kameras der Zustand des Wassers in der Fischzucht beurteilt und besser gesteuert werden kann.
- Ein Medienhaus lässt sich von einer KI journalistische Artikel schreiben (Roboterjournalismus).
- Ein Rückversicherer lässt durch eine KI globale Nachrichtenquellen auf Schadensfälle auswerten und kann auf diese Weise Versicherungstarife gestalten („early loss detection").
- Ein KFZ-Hersteller entwickelt ein autonom fahrendes Fahrzeug.
- Ein IT-Konzern entwickelt Spracherkennungssysteme wie Siri, Alexa oder Cortana.
- Ein Maschinenbauer entwickelt Bauteile durch Simulationen (digitaler Zwilling).

Fertigungsprozesse / Logistik

- Eine KI optimiert die Supply Chain und / oder die Transportwege.
- Eine KI optimiert die Produktionsprozesse und reduziert Stau, möglicherweise auch unter Personaleinsparung.
- Eine KI lernt für die Produktion Objekte zu erkennen (Griff in die Kiste durch Roboter).

Qualitätskontrolle

- Eine KI erkennt Fehlerzustände in Produktionsprozessen und entwickelt selbstständig Strategien zur Feinjustierung der Maschinenparameter.
- Mit einer KI wird die Leistungsfähigkeit einer visuellen Inspektion von Produktionsprozessen gesteigert.
- Eine KI plant eine vorausschauende Wartung von Maschinen („predictive maintanance").

Marketing, Vertrieb, Customer-Relationship-Management

- Eine KI segmentiert Kundengruppen passgenau, analysiert Kundenverhalten und prognostiziert die Nachfrage.
- Eine KI optimiert die Werbekampagne.
- Eine KI berät Kunden und Kundinnen bei der Auswahl von Produktvarianten und erkennt Upsell-Potenziale.
- Eine KI steuert eine dynamische Preisgestaltung.
- Eine KI erzeugt mehr oder weniger selbsttätig Texte für Werbebroschüren und andere Marketingunterlagen.

Kundenservice

- Kunden und Kundinnen werden im ersten Kontakt von einem Chatbot / digitalen Assistenten / Serviceroboter betreut.
- Eine KI beantwortet einfache Kundenanfragen automatisch und schafft damit den Kundenberater:innen mehr Zeit für komplexere Anliegen.
- Ein:e Hersteller:in von Computer-Games analysiert zeitnah die Online-Communities zu den eigenen Produkten und kann auf Stimmungen reagieren.

Controlling

- Eine KI bucht Zahlungsein- und -ausgänge.
- Eine KI erstellt automatisierte Forecasts.

Sicherheit / Compliance

- Eine KI erkennt frühzeitig Cyberangriffe.
- Eine KI erkennt strafbare und / oder jugendgefährdende Inhalte in eigenen Internetdiensten.
- Eine KI deckt unternehmensinterne Compliance-Verstöße auf („fraud detection").

Human Resources

- Eine KI trifft eine Bewerbervorauswahl.
- Eine KI unterstützt das People Management durch Prognosen über Talententwicklungen und zu erwartende Kündigungen.

Anwendungsbeispiele KI nach *Till Kreutzer, Per Christiansen*, KI in Unternehmen. Ein Praxisleitfaden zu rechtlichen Fragen, Gütersloh 2021, S. 14.

4 Rechtlicher Rahmen

Bevor eine KI im Unternehmen eingesetzt wird, entscheidet die Geschäftsleitung über zwei Fragen:

Erstens, um welche Art der KI (Expertensysteme vs. Maschinelles Lernen) es sich dabei handelt.

Entscheidet sich die Geschäftsleitung für ein **Expertensystem**, ergeben sich – im Vergleich zu einer „**herkömmlichen**“ **Software** – praktisch keine Besonderheiten. Die den Expertensystemen innewohnende Determiniertheit führt dazu, dass die üblich im Bezug auf die KI angesprochenen „Schwächen“ wie Intransparenz oder fehlende Nachvollziehbarkeit eben nicht vorliegen. Da Expertensysteme also einem „fest“ programmierten Regelwerk folgen, können sie auch vertraglich, wie eine „übliche“ Software behandelt werden.

Komplizierter sieht es mit KI-Lösungen mit Maschinellem Lernen aus. Denn hier kommt der Frage der **Aufteilung von Verantwortung** zwischen Hersteller:in/Programmierer:in und Betreiber:in große Bedeutung zu: „Lernt“ die KI-Anwendung auch im laufenden Betrieb weiter, wäre die alleinige Verantwortung der/des Hersteller:in/Programmierer:in unbillig, denn es können bspw. fehlerhafte Daten im Betrieb zugefügt werden. Auch weitere Risiken wie etwa die vielerorts angesprochene Opazität (Black-Box-Effekt) der KI müssen adressiert werden. Eine **vertragliche Klärung** ist hier **unabdingbar**.

Zweitens, ob die KI-Anwendung „im Hause“, also intern, entwickelt, durch einen Auftragnehmer nach präzisen Angaben der Geschäftsleitung extern entwickelt oder (zumindest zunächst) extern erworben wird.

Die Entscheidung, eine KI einzusetzen, wird von vielen Faktoren beeinflusst. Zu nennen sind hier etwa die finanzielle Lage des Unternehmens, Fragen, die mithilfe der KI gelöst werden müssen, oder auch interne Kompetenzen. Einer der entscheidenden Faktoren ist darüber hinaus die rechtliche Regelung dieser doch noch relativ neuen Technologie, insbesondere

die Fragen der Haftung. Diese Fragen gilt es nachfolgend zumindest ansatzweise zu erläutern.

Wird die KI **intern im Unternehmen entwickelt**, bleiben auch alle Rechte an der KI selbst im bzw. beim Unternehmen.

Auch wenn natürlich nicht die GmbH oder die AG, sondern konkrete Personen im Unternehmen, Mitarbeiterinnen und Mitarbeiter, die KI entwickeln, bleiben die Rechte an der KI beim Unternehmen, wie das Urheberrechtsgesetz sowie das Gesetz über Arbeitnehmererfindungen anordnen.

Wird diese jedoch **erworben** bzw. für das Unternehmen hergestellt, müssen diese Rechte zunächst vertraglich gesichert werden (auch dann, wenn Freelancer o.Ä. die KI fürs Unternehmen entwickeln). Dabei ist die KI unterschiedlichem Schutz zugänglich:

⇨ **Patentschutz**

Neue Verfahren (nicht der Algorithmus und nicht der Code) können durch den Erwerb eines Patents geschützt werden.

⇨ **Urheberschutz**

Software selbst (etwa als Programmcode) kann urheberrechtlich geschützt werden. Der Vorteil des Urheberschutzes vor dem Patentschutz liegt darin, dass der Urheberschutz "automatisch" mit der Schaffung des Werkes entsteht und keine Eintragung (anders als Patent) bedarf. Der Urheberschutz bedeutet, dass andere Personen die Software nicht ohne Zustimmung des Urhebers nutzen dürfen.

⇨ **Geschäftsgeheimnisschutz**

Algorithmen können als Geschäftsgeheimnisse geschützt werden. Natürlich ist nicht gleich jeder Algorithmus ein Geschäftsgeheimnis. Jedoch sicherlich solche Algorithmen, die folgende drei Anforderungen des § 2 Geschäftsgeheimnisgesetzes erfüllen:

1 - der Algorithmus ist 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

2 - der Algorithmus ist Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

3 - bei diesem Algorithmus besteht ein berechtigtes Interesse an dessen Geheimhaltung.

Werden **Standardlösungen** erworben, entstehen lediglich vertragliche Nutzungsrechte und -pflichten. Bei Standardlösungen liegt keine Individualität vor, sodass auch die Exklusivität, also alleinige Nutzung durch den Erwerber, nicht gegeben ist. Hier ist besonders darauf zu achten, dass vertraglich solche Probleme adressiert werden wie etwa Fehler in der Anwendung, Umstellung auf andere Lösungen, ggf. Schnittstellen oder auch Insolvenz des Anbieters, denn bei Standardlösungen ist die eigene Macht des Unternehmens, in die KI einzugreifen, praktisch nicht vorhanden (erst recht bei sog. Software as a Service Lösungen). Dafür liegt es in der Macht des Unternehmens (des Anwenders), durch eigene aktive Vertragsgestaltung das eigene Recht zu schaffen.

5 Haftungsfragen

Die Frage nach den Konsequenzen des Einsatzes der KI entsteht gleichzeitig mit der Frage nach deren Anwendung. Hier werden wir jedoch nicht auf das beliebteste Beispiel für den Einsatz der KI abstellen – das autonome Fahren, sondern solche Anwendungen primär im Blick haben, die in der deutschen IT-Branche bereits jetzt eine große Rolle spielen.

5.1 Produkthaftung

Betrachtet man das geltende europäische Recht, stellt man schnell fest, dass das bestehende Haftungsregime – das System der Produkthaftung der Europäischen Union – mehr oder weniger in dieser Form seit 1986 vorhanden ist, denn die Produkthaftungsrichtlinie 85/374/EWG wurde im Jahr 1986 erlassen und daraufhin in den (fast allen) Mitgliedstaaten umgesetzt.

Bei der Produkthaftung im Sinne des europäischen Gesetzgebers geht es dann um eine **verschuldensunabhängige Haftung des Herstellers** eines Produktes bzw. des Herstellers bestimmter Komponenten des Produktes.

Führt ein Produkt also zu einem Schaden, ist der Hersteller (ggf. der Hersteller einer Komponente) zum Schadensersatz gegenüber dem Nutzer bzw. ggü. jedermann verpflichtet. In Deutschland ist die Produkthaftungsrichtlinie im Produkthaftungsgesetz umgesetzt. Die Voraussetzungen des Schadensersatzanspruchs sind dabei in § 1 Abs. 1 ProdHaftG ausgezählt: „Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen."

Was zunächst klar und deutlich klingt, bereitet in der Praxis viele Probleme, denn derjenige, der einen Schaden erleidet, muss den Fehler im Produkt, den (eigenen) Schaden sowie die Kausalität, also den **Ursache-Wirkung-Zusammenhang** zwischen dem Fehler und dem Schaden, nachweisen.

Besondere Schwierigkeiten bereitet dabei die besagte Kausalität. Auch wenn der Europäische Gerichtshof die Nachweiserbringung stets versucht zu erleichtern und den

Verdacht auf einen bestehenden Fehler dem Fehler selbst gleichstellt, ist der Nachweis der Ursachenwirkung nicht immer leicht. Hinzu kommt, dass bei technisch komplizierten Produkten, zu den in aller Regel auch die Produkte unter Mitwirkung Künstlicher Intelligenz gehören, bereits der Nachweis des Fehlers problematisch ist. In der allgemeinen Diskussion um die Haftung der Künstlichen Intelligenz wird dabei häufig auf die sog. „Blackbox" verwiesen: da die gesamte Entscheidungskette der KI nicht **nachvollziehbar** sei, könne der Fehler nicht nachgewiesen werden. Hinzu kommt eine große Menge an Daten, die durch die KI verarbeitet werden und teilweise zu unerwarteten Entwicklungen führen können, die vom Hersteller des Produkts kaum bis gar nicht vorhergesehen werden können.

Kann/darf man dann dem Hersteller die Haftung für diese (Fehl)Entwicklungen auferlegen?

Um eine eindeutige Antwort auf diese Frage liefern zu können, muss man zunächst untersuchen, was unter einem Fehler zu verstehen ist. Das oben bereits genannte Produkthaftungsgesetz definiert ein Produkt dann als fehlerhaft, wenn dieses „nicht die **Sicherheit** bietet, die unter Berücksichtigung aller Umstände, insbesondere

a) seiner Darbietung,

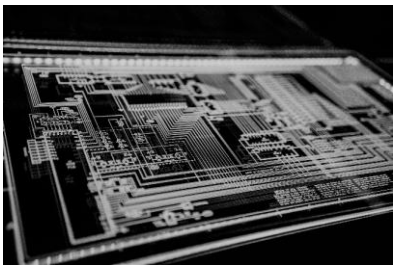
b) des Gebrauchs, mit dem billigerweise gerechnet werden kann,

c) des Zeitpunkts, in dem es in den Verkehr gebracht wurde,

berechtigterweise erwartet werden kann“, § 3 Abs. 1 ProdHaftG.

Ein fehlerhaftes Produkt entspricht also nicht den **berechtigten Erwartungen** der Nutzer bezüglich seiner Sicherheit. Dabei lassen sich zwei Fehlerkreise unterscheiden: einerseits gibt es Fabrikationsfehler, also solche Fehler, die bei der Herstellung eines konkreten Produktes entstanden sind und somit nur dieses eine Produkt fehlerhaft machen, und andererseits Sorgfaltspflichtverletzungen, bspw. Konstruktionsfehler oder Instruktionsfehler, also solche Fehler, die die gesamte Produktionslinie betreffen.

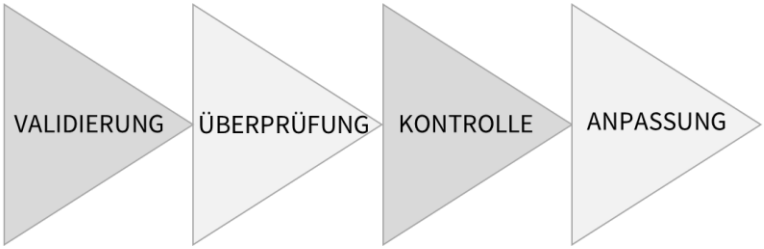
Dem Hersteller ist allerdings durch die angebotenen Definitionen wenig geholfen, denn er muss wissen, was genau unter den berechtigten Sicherheitserwartungen zu verstehen ist und welcher Maßstab auf seine Pflichten angewandt wird. Hilfe schaffen zwei Paragraphen des Produkthaftungsgesetzes: zum einen die Kriterien des § 3 Abs. 1 ProdHaftG, so dass es um eine **wertende Beurteilung** unter Einbeziehung der Darbietung, des zu erwartenden Gebrauchs sowie des Zeitpunktes der Inverkehrbringung des Produkts geht; zum anderen die Ausnahme des § 1 Abs. 2 Nr. 5 ProdHaftG, demnach die Haftung für einen Fehler, der nach dem **Stand der Wissenschaft und Technik** in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte, ausgeschlossen ist. Es lässt sich somit erkennen, dass den Maßstab für die Beurteilung der Fehlerhaftigkeit eines Produkts der Stand der Wissenschaft und Technik zum Zeitpunkt der Inverkehrbringung des Produkts bildet. Dieser Stand muss untersucht werden, um die berechtigten Erwartungen von Nutzern zu bestimmen und somit ein fehlerfreies Produkt herzustellen.



In Bezug auf die KI und die mit ihrer Hilfe entwickelten Produkte lässt sich somit zunächst festhalten, dass der Hersteller die damit einhergehenden Probleme, wie etwa unzureichende Analyse- bzw. Trainingsdaten, schlechte Qualität dieser Daten, fehlerhafte Programmierung u.v.m., erkennen muss, denn bereits ohne eine tiefergehende Analyse des

aktuellen Standes der Wissenschaft und Technik ist die Problematik rund um die KI wohlbekannt.

Darüber hinaus muss der Hersteller alle ihm zur Verfügung stehenden Möglichkeiten der **Validierung, Überprüfung, Kontrolle und Anpassung** seines Produkts ausschöpfen, bevor er dieses Produkt auf den Markt bringt. Dabei kommt es maßgeblich darauf an, ob das Produkt zum Zeitpunkt seiner Inverkehrbringung dem entsprach, was – vereinfacht ausgedrückt – möglich war. Gab es zu diesem Zeitpunkt bereits neuere bzw. bessere Erkenntnisse in Bezug auf das Produkt selbst oder seine Bestandteile oder die damit verbundene KI-Anwendung, die der Hersteller missachtet hat, ist davon auszugehen, dass das Produkt nicht den berechtigten Sicherheitserwartungen entsprach und somit fehlerbehaftet war (und ggf. weiterhin ist). Entscheidend ist dabei nicht die Fähigkeit des Herstellers, bestimmte oder unbestimmte Fehlentwicklungen der KI (oder des Produktes) vorherzusehen, sondern seine Möglichkeit, durch Programmieren, Trainieren oder anderweitig alle unerwünschten Entwicklungen auszuschließen. Nutzt er alle ihm zur Verfügung stehenden Möglichkeiten, befreit er sich in aller Regel vom Vorwurf eines fehlerhaften Produktes.



5.2 Produzentenhaftung

Als Auffangbecken gilt zusätzlich noch die sog. Produzentenhaftung (deliktische Produkthaftung) im Sinne von § 823 Abs. 1 BGB, die eine **Schadensersatzpflicht** für die Verletzung der **Sorgfaltspflicht** statuiert. Es geht dabei um die Pflicht des Herstellers, ein sicheres Produkt auf den Markt zu bringen, insofern sind die Fehlerbegriffe des ProdHaftG und der deliktischen Haftung des BGB identisch, Fehler ist ein Verstoß gegen die Sorgfaltspflicht. Diese Sorgfaltspflicht besteht dabei aus kleineren Pflichtenkreisen:

- **Organisationspflicht**, denn der Hersteller ist verpflichtet, sein Betrieb so zu organisieren, dass Fehler vermieden, rechtzeitig entdeckt und beseitigt werden können;

- **Instruktionspflicht**, denn der Hersteller ist verpflichtet, den Nutzer über das Produkt, die mit ihm ggf. Verbundenen Risiken und Gefahren und seine richtige Nutzung zu informieren;

- **Produktbeobachtungspflicht**, denn der Hersteller ist verpflichtet, den Hinweisen über die von seinem Produkt ausgehenden Gefahren und Risiken auch nach der Inverkehrbringung nachzugehen;

- **Gefahrabwendungspflicht**, denn der Hersteller ist verpflichtet, die nach der Inverkehrbringung bekannt gewordenen Gefahren zu beseitigen und ggf. das Produkt sogar zurückzurufen.

Im Rahmen der Produktbeobachtungspflicht wären bspw. die Fehler beim Programmieren oder bei den Trainingsdaten der KI-Anwendung zu erkennen und zu beseitigen. Im Endeffekt lässt sich also die eingangs aufgeworfene Frage nach der Haftung des Herstellers eines Produktes für die Fehler der KI bejahen. Es kommt dabei weniger auf die juristische Auslegungsarbeit, sondern vielmehr auf die tatsächlich vorhandene **Nachweisbarkeit von technischen und organisatorischen Vorkehrungen**, die der Hersteller getroffen haben muss, um die Fehler im Endprodukt auszuschließen.

5.3 Anwenderhaftung

Nicht selten stellt sich in der Praxis die Frage nach der Haftung derjenigen, wer die KI einsetzt und anwendet. Hier ist zwischen der schuldrechtlichen und deliktsrechtlichen Haftung zu unterscheiden.

Der Anwender einer KI-Lösung kann seine schuldrechtliche Haftung, also solche Haftung, die auf einem **Vertrag** fußt, durch eine ausgewogene Vertragsgestaltung minimieren. Werden etwa Ersatzteile durch eine KI-Anwendung überprüft und bestellt und kommt es dabei zu einem Fehler, der die Bestellung mehrerer identischer Ersatzteile nach sich zieht, kann dies vertraglich zwischen dem Lieferanten und dem Besteller etwa dahingehen

adressiert werden, dass bei einer ungewöhnlich hohen Anzahl der Bestellten Ersatzteile oderungewöhnlich häufiger Bestellung eins und desselben Ersatzteils der Besteller vom Lieferanten kontaktiert wird und die Bestellung durch eine im Unternehmen dafür zuständige Person verifiziert und bestätigt bzw. storniert wird.

Deliktsrechtliche Haftung kann indes nicht so leicht adressiert werden. Auch beim Anwender kann eine Haftung aus § 823 Abs. 1 BGB in Betracht kommen. Dann haftet dieser, wenn die von ihm eingesetzte KI eine Verletzung eines Rechtsguts wie Leben, Eigentum oder Gesundheit verursacht hat und daraus ein Schaden entstanden ist. Jedoch knüpft auch diese Haftung an **Verschulden** an. Dabei ist die Bewertung, inwiefern der Anwender seiner Sorgfaltspflicht Genüge getan hat, sehr anspruchsvoll. Im Endeffekt wird diese in der Frage münden, ob der Anwender die KI **richtig bedient** hat. Das bedeutet einerseits den „richtigen", dem Verwendungszweck und der Beschreibung des Herstellers entsprechenden, Einsatz der KI, und andererseits kein Hinnehmen von offenkundigen gravierenden Fehlern (wie etwa dauerhafte Nutzung der Schimpfwörter durch einen KI-basierten Chat-Bot). Grundsätzlich sollte man davon ausgehen, dass die Bedienung richtig war.

Der Nachweis fehlerhafter Bedienung obliegt dabei demjenigen, wer eine entsprechende Schadenersatzklage erhebt.

5.4 Datenschutzrechtliche Haftung

Die DSGVO erwartet von jedem Verantwortlichen, dass die Daten „von Anfang an" rechtskonform verarbeitet werden, mithin die Grundsätze der „**Privacy by Design**" und „**Privacy by Default**" im täglichen Leben umgesetzt werden. Das bedeutet unter anderem, dass bereits vor dem Einsatz der KI und auch vor deren Entwicklung datenschutzrechtliche Aspekte mitberücksichtigt werden müssen.

Beim Einsatz der KI sind die **Trainingsdaten** von besonderer Bedeutung. Auch hierbei ist die Einhaltung datenschutzrechtlicher Vorschriften unabdingbar. Diese Daten müssen also bereits vor ihrem Einsatz bestimmt, **Rechtsgrundlage** der Verarbeitung identifiziert, Betroffenenrechte sichergestellt werden etc. Bei der Anonymisierung ist beispielsweise stets darauf zu achten, dass nicht einfach der Name der betroffenen Person gelöscht wird

(das ist noch keine Anonymisierung!), sondern richtige (mathematische) Anonymisierungsvorgänge durchgeführt werden.

Mehr Informationen zum Datenschutz finden Sie in unserem Leitfaden mit Mustern und Checklisten.

6 Europäische Initiativen

Am 21. April 2021 stellte die EU-Kommission den Entwurf eines **Artificial Intelligence Act** vor:

In diesem wird die Künstliche Intelligenz nicht als Technologie reguliert, sondern als verschiedenste Anwendungen der Technologie in verschiedensten Bereichen. Hier geben wir einen kurzen Überblick über diese Initiative der EU-Kommission.

„**Artificial intelligence systems**“ (KI-Systeme) werden als „software that is developed with one or more of the techniques and approaches listed in Annex I and [that] can, for a given set of humandefined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environment they interact with“ definiert.

Die Regulierung richtet sich an drei technische Ansätze:

- ⇨ das maschinelle Lernen
- ⇨ logik- und wissensbasierter Ansatz
- ⇨ Statistik

Die Verordnung folgt dem gleichen Ansatz der Technikneutralität, der bereits in der DSGVO erkennbar ist, wirkt jedoch etwas „konkreter“ als diese, und geht grundsätzlich von einem weiten Verständnis der KI.

KI-Systeme werden – je nach der Höhe des davon ausgehenden Risikos – in ebenfalls drei Gruppen unterteilt:

- ✓ ein minimales oder geringes Risiko,

- ✓ ein hohes Risiko,
- ✓ ein inakzeptables Risiko.

Die Kommission folgt einem risikobasierten Ansatz und verbietet Einsatzbereiche und Zwecke, die ein inakzeptables Risiko darstellen.

Die Bereiche mit einem hohen Risiko sind etwa:

(1) die biometrische Identifikation und Kategorisierung natürlicher Personen,

(2) das Management und der Betrieb von Kritischen Infrastrukturen,

(3) Bildung und Berufsbildung,

(4) Beschäftigung, Personalmanagement und Zugang zu selbstständiger Tätigkeit,

(5) Zugang zu und Nutzung von essenziellen privaten und öffentlichen Diensten und Leistungen,

(6) Strafverfolgung,

(7) Migration, Asyl und Grenzkontrollen sowie

(8) Rechtspflege und demokratische Prozesse.

Eine zentrale Stelle nehmen die Grundrechte ein. Der Entwurf spricht diese an mehreren Stellen unmittelbar an und **verbietet** bspw. ein solches KI-System, „that exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological Der zukünftige Artificial Intelligence Act verbietet grundsätzlich solche KI-Systeme, die nach der Wertung der Kommission inakzeptable Risiken mit sich bringen, wie etwa unterschwellige Techniken zur **Verhaltensbeeinflussung** oder das Ausnutzen der Verletzlichkeit bestimmter Bevölkerungsgruppen, sofern dieses zu physischen oder psychischen Verletzungen führen kann. Ebenfalls verboten ist die Bewertung der Vertrauenswürdigkeit natürlicher Personen durch öffentliche Stellen (das sog. „Social Scoring“).

7 E-Person?

Nicht selten ist von der sogenannten E-Person zu hören. Dabei erscheint diese Schöpfung mehr als zweifelhaft, denn – zumindest nach dem jetzigen Stand der Wissenschaft und Technik – nur die sog. starke KI ggf. eigenständig agieren könnte, die bislang zur Anwendung kommenden KI-Lösungen gehören der sog. schwachen KI an. Die Schaffung einer (zusätzlichen) **Persönlichkeit** ist erst dann notwendig, wenn die Fragen der **Zurechnung** von einem bestimmten Verhalten oder Wissen aufkommen. Handeln kann nach dem geltenden Recht lediglich ein Mensch, eine natürliche Person. Seine Handlungen werden teilweise nur ihm, dem Menschen, teilweise zusätzlich noch einer juristischen Person, bspw. seinem Arbeitgeber, zugerechnet. Eine Handlung ist dabei der Ausdruck freien Willens, der bislang lediglich einem Menschen zugebilligt wird. Ob es in der Zukunft notwendig sein wird, E-Person zu kreieren, wird sich noch zeigen, nach dem geltenden Recht ist dies weder vorgesehen noch notwendig.

8 Ausblick

Der Einsatz Künstlicher Intelligenz birgt – wie jede neue Technologie – teilweise unbekannte Risiken, unter anderem auch im rechtlichen Bereich. Dennoch sind die Chancen der KI so groß, ihre Anwendungsbereiche so breit, dass die deutsche IT-Branche und mit ihr sicherlich auch die Anwender:innen es hoffentlich schaffen werden, durch bedachten Einsatz, ausgewogene Vertragsgestaltung und Berücksichtigung datenschutzrechtlicher Vorschriften die KI zu ihrem ständigen und rechtskonformen Begleiter zu machen.

9 Kontakt

Haben Sie Fragen oder Anregungen, melden Sie sich gerne bei uns. Wir freuen uns auf Sie!

Ansprechpartnerin:

Olga Kunkel, LL.M.
Telefon: +49 3375 508 641
E-Mail: olga.kunkel@itwirtschaft.de

Kompetenzzentrum IT-Wirtschaft
vertreten durch:

Bundesverband IT-Mittelstand e.V. (BITMi)
Hauptstadtbüro Berlin:
Haus der Bundespressekonferenz
Schiffbauerdamm 40, 10117 Berlin
T +49 30 22605 005

www.itwirtschaft.de

Was ist Mittelstand-Digital?

Das Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft ist Teil der Förderinitiative Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren vor Ort helfen dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter: www.mittelstand-digital.de

Impressum

Konzeption und Text: Olga Kunkel

Bildnachweis: Unsplash.com

Stand: Dezember 2021