ADVANT Beiten

RECHT DER KÜNSTLICHEN INTELLIGENZ

ADVANT Beiten

RECHT DER KÜNSTLICHEN INTELLIGENZ

Vorbemerkung

Anfang 2021 legten wir die erste Auflage dieser Broschüre vor. Wir waren sicher: Künstliche Intelligenz ist eines der ganz großen Zukunftsthemen für unsere Gesellschaft und Wirtschaft – und damit auch in rechtlicher Sicht hoch relevant.

Die Rasanz der Entwicklungen gerade in den letzten Monaten hat uns dann aber doch überrascht. Kaum ein Medium, das nicht in der einen oder anderen Form berichtete – und in Schulen werden die aktuellen Möglichkeiten ebenso ausgetestet wie in Unternehmen.

Mit dieser Broschüre wollen wir einen knappen Überblick über die aktuelle Rechtslage und den Stand der Diskussion geben. Eine kurze Darstellung wie die vorliegende kann dabei keinen Anspruch auf Vollständigkeit in Breite und Tiefe erheben.

Daneben wagen wir einen Ausblick auf künftig bevorstehende Entwicklungen und mögliche Anpassungen des Rechtsrahmens im Hinblick auf die fortschreitende Autonomie von KI- und Roboter-Systemen. Besonders spannend erscheinen uns hier Fragen um die Schutzfähigkeit von durch KI geschaffenen Werken einerseits und Haftungsfragen andererseits – bis hin zu der nicht nur provokanten Frage, ob Künstliche Intelligenzen Inhaber von Rechten sein sollten, vielleicht sogar eine Rechtspersönlichkeit erhalten. Auch hier können und wollen wir bei einem Werk mit beschränktem Umfang nur Denk- und Diskussionsanstöße geben.

Das Werk befindet sich überwiegend auf dem Stand von Juni 2023.

Zur besseren Lesbarkeit soll im Folgenden „Künstliche Intelligenz“ (kurz „KI“) als Oberbegriff verwendet werden, der sowohl (intelligente) Roboter als auch autonome und/oder selbstlernende Systeme, generative KI, Computerprogramme und Anwendungen umfasst.

Dr. Andreas Lober
Rechtsanwalt
ADVANT Beiten

Susanne Klein | LL.M.
Rechtsanwältin
ADVANT Beiten

Impressum
ADVANT Beiten
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33 | D-80339 München
AG München HR B 155350/USt.-Idnr: DE-811218811

Inhalt

1. Rechtsrahmen

Gegenwärtig gibt es (noch) keinen konkreten und eigens für Künstliche Intelligenz geschaffenen rechtlichen Rahmen. Die EU arbeitet aber mit Hochdruck an einer Spezialgesetzgebung in Form einer Rechtsverordnung („Gesetz über Künstliche Intelligenz", „AI Act"). Rechtsverordnungen sind in allen Mitgliedsstaaten der EU unmittelbar anwendbar, ohne dass ein nationales Umsetzungsgesetz nötig wäre. Sollte der AI Act zeitnah verabschiedet werden, würde dies wohl die weltweit erste umfassende Spezialgesetzgebung für die Nutzung von Künstlicher Intelligenz, inklusive der vor allem in den Jahren 2022 und 2023 enorm an Popularität gewinnenden generativen Künstlichen Intelligenz zur Erstellung von Texten, Bildern und anderer digitaler Inhalte, sein.

Künstliche Intelligenz verfügt derzeit auch nicht über eine eigene Rechtspersönlichkeit, anhand derer ihr Rechte und Pflichten zuerkannt würden. Vor allem gibt es aktuell noch keine eigenständige Haftung Künstlicher Intelligenz.

Daher gelten derzeit die allgemeinen Gesetze, wobei neben dem allgemeinen Haftungsrecht (insbesondere nach dem BGB) insbesondere das Immaterialgüterrecht und die Datenschutz-Grundverordnung von besonderer Relevanz sind.

Einen Ausblick darauf, wie die Rechtsstellung Künstlicher Intelligenz in Zukunft aussehen könnte, geben wir ab Ziffer 4.6.

2. Künstliche Intelligenz und Immaterialgüterrechte

Immaterialgüterrechte sind hochrelevant, wenn es um den Schutz oder die Schutzfähigkeit der KI-Technologie geht – aber auch für den Schutz von durch Künstliche Intelligenz geschaffenen Arbeitsergebnissen.

2.1 Schutz der KI-Technologie

Die KI-Technologie unterscheidet sich nicht grundlegend von anderen Technologien. Grundsätzlich kann eine KI oder eine KI-Anwendung durch alle Arten von geistigen und gewerblichen Schutzrechten geschützt werden, sofern deren spezifische Schutzvoraussetzungen erfüllt sind.

2.1.1 Schutz durch Patente und Gebrauchsmuster

Patente werden für technische Erfindungen erteilt, die neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind (vgl. etwa § 1 Abs. 1 PatG, Art. 52 Abs. 1 des Europäischen Patentübereinkommens).

Patente stellen das Immaterialgüterrecht dar, das den am weitestgehenden Schutz vermittelt, da sie nicht nur die konkrete Ausprägung einer Leistung schützen, sondern auch die zugrunde liegende Idee. Demgegenüber lassen sich beispielsweise über §§ 69a ff. UrhG nicht die Ideen und Grundsätze, die einem Computerprogramm zugrunde liegen, schützen. Geschützt ist ausschließlich der Quell- und Objektcode. Andererseits sind Computerprogramme als solche nicht als Patent schutzfähig, wohl aber computerimplementierte Erfindungen und Verfahrenspatente (siehe im Einzelnen noch unten).

In territorialer Hinsicht kann Patentschutz derzeit nur für einzelne Länder erworben werden. Hierfür stehen verschiedene Wege zur Verfügung: zunächst kann eine Patentanmeldung bei einem nationalen Patentamt, wie beispielsweise dem Deutschen Patent- und Markenamt (DPMA), eingereicht werden. Sofern Patentschutz in einer Vielzahl an Ländern gewünscht ist, bietet sich die Einreichung einer Europäischen Patentanmeldung beim Europäischen Patentamt in München (EPA) an. Bei einem Europäischen Patent durchläuft die Patentanmeldung eine einheitliche Prüfung durch das Europäische Patentamt. Nach Erteilung des Europäischen Patents zerfällt das Europäische Patent in ein Bündel von nationalen Patenten, die in den Staaten, in denen das Europäische Patent validiert wurde, wie ein nationales Schutzrecht behandelt werden. Auch der Patent Cooperation Treaty (PCT) bietet die Möglichkeit, durch Einreichen einer einzelnen Anmeldung (bei der World Intellectual Property Organization (WIPO) in Genf) eine Vielzahl an Schutzrechten in den teilnehmenden Staaten zu erlangen.

Seit dem 1. Juni 2023 steht nunmehr nach langer Vorbereitungsphase das Europäische Patent mit einheitlicher Wirkung, auch Einheitspatent genannt, zur Verfügung. Grundlage des Einheitspatents ist ein Europäisches Patent, das durch einen Antrag des Inhabers bis spätestens einen Monat nach Erteilung des Europäischen Patents zu einem Europäischen Patent mit einheitlicher Wirkung wird. Sein räumlicher Schutzbereich erstreckt sich auf diejenigen Staaten der Europäischen Union, die das Abkommen über das Einheitspatentgericht ratifiziert haben. Das sind derzeit 17 Staaten.

Wie bereits einleitend ausgeführt, werden Patente für technische Erfindungen erteilt, die neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind. Keine Erfindungen und damit dem Patentschutz nicht zugänglich sind jedoch mathematische Methoden, d.h. Algorithmen, oder Programme für Datenverarbeitungsanlagen, d.h. Software, (vgl. § 1 Abs. 3 a) und c) PatG, Art. 52 Abs. 2 a) und c) EPÜ). Der gemeinsame Grund für ihren Ausschluss liegt in ihrem fehlenden technischen Charakter.

Damit sind weder die bloßen Algorithmen patentierbar, die einer KI zugrunde liegen, noch die reine Software als Abfolge von Anweisungen, die von einem Computer ausführbar sind.

Dieser Ausschluss gilt jedoch nur, soweit ein Patent für die vorgenannten Entwicklungen „als solche“ beansprucht wird (vgl. § 1 Abs. 4 PatG, Art. 52 Abs. 3 EPÜ). Dem Patentschutz zugänglich sind damit sogenannte computerimplementierte Erfindungen, also solche Erfindungen, die Computer, Computernetze oder andere

programmierbare Vorrichtungen umfassen, wobei mindestens ein Merkmal durch ein Programm realisiert wird, sofern der Einsatz der technischen Vorrichtung sich nicht nur auf die „normale“ physikalische Wechselwirkung zwischen Software und Hardware beschränkt (vgl. im Einzelnen RL der Prüfung G II. 3.6., Richtlinien Kap. F. IV. 3.9). Computerimplementierte Erfindungen werden als technisch angesehen und sind nicht Programme für Datenverarbeitungsanlagen als solche, da sie notwendigerweise auf einem technischen Gerät, dem Computer, ausgeführt werden. Beispiele für computerimplementierte Erfindungen, bei denen eine KI zum Einsatz kommen kann, sind etwa die Steuerung eines autonomen Fahrzeugs oder die Verarbeitung von Messwerten, die zur Erkennung von Verkehrszeichen oder Tumoren auf Kamerabildern führen.[1]

Das Europäische Patentamt behandelt Erfindungen, die KI nutzen bzw. denen eine KI zugrunde liegt, ausdrücklich als computerimplementierte Erfindungen und bewertet deren Patentfähigkeit anhand der Kriterien, die für computerimplementierte Erfindungen gelten. Dieser Ansatz dürfte auch im DPMA verfolgt werden.

Damit ist Patentschutz für Erfindungen, bei denen eine KI genutzt wird oder zum Einsatz kommt, denkbar, sofern die übrigen Voraussetzungen der Patentierbarkeit gegeben sind, sie also neu, erfinderisch und gewerblich anwendbar sind.

Eine Erfindung ist neu, wenn sie nicht zum Stand der Technik gehört. Zum Stand der Technik gehören alle Kenntnisse, die vor dem Anmeldetag der Erfindung der Öffentlichkeit, also einem unbegrenzten Personenkreis, zugänglich waren, sei es durch schriftliche oder mündliche Beschreibung, Benutzung oder sonstige Offenbarungen (§ 3 Abs. 1 PatG, Art. 54 Abs. 1, 2 EPÜ).

Auch Informationen, die der Erfinder selbst öffentlich gemacht hat – und sei es nur im Rahmen eines Vortrags – zählen zum Stand der Technik. Der Erfinder sollte daher – ebenso wie sein Arbeitgeber – auf strengste Geheimhaltung achten und jede Weitergabe von relevanten technischen Informationen an Dritte mit starken Geheimhaltungsvereinbarungen absichern.

Eine Erfindung beruht auf einer erfinderischen Tätigkeit, wenn sie sich für den Fachmann nicht in naheliegender Weise aus dem Stand der Technik ergibt. Die Erfindung muss eine Weiterentwicklung des Stands der Technik sein, die über bloße routinemäßige Tätigkeiten des Fachmanns hinausgeht. Im Kontext von computerimplementierten Erfindungen ist bei der erfinderischen Tätigkeit zusätzlich zu beachten, dass nur diejenigen Merkmale, die zum technischen Charakter der Erfindung beitragen, die erfinderische Tätigkeit begründen können. Nicht-technische Merkmale können dagegen die erfinderische Tätigkeit nicht begründen.

Beispiele für technische Bereiche, in denen KI-basierte Erfindungen zum Einsatz kommen könnten, sind Medizingeräte, Automobiltechnik, Luft- und Raumfahrt, industrielle Steuerung, additive Fertigung, Kommunikations-/Medientechnik einschließlich

---

[1] Vgl. https://www.dpma.de/dpma/veroeffentlichungen/hintergrund/ki/kuenstlicheintelligenzundschutzrechte/index.html.

Spracherkennung und Videokompression, sowie die Bereiche Computer, Prozessoren oder Computernetzwerke selbst.

Wie das Patent setzt das Gebrauchsmuster – oft als „kleiner Bruder" des Patents bezeichnet – eine neue technische Erfindung voraus, die auf einem erfinderischen Schritt beruht und gewerblich anwendbar ist. Hinsichtlich der Schutzfähigkeitsvoraussetzungen, insbesondere bezüglich der erforderlichen Erfindungshöhe, gelten beim Gebrauchsmuster die gleichen Voraussetzungen wie beim Patent. Die Einschränkungen in Bezug auf den Schutz von Software und damit auch von KI-Systemen gelten also auch hier.

Im Gebrauchsmusterrecht ist im Gegensatz zum Patentrecht ein weiterer spezifischer Schutzversagungsgrund vorgesehen. Danach werden für Verfahren keine Gebrauchsmuster erteilt. Gerade Verfahrensansprüche sind jedoch im Bereich computerimplementierter Erfindungen vorherrschend. Im Zusammenhang mit computerimplementierten Erfindungen sind daher alle Verfahren, die eine KI zum Gegenstand haben, nicht durch ein Gebrauchsmuster schutzfähig.

Anders als beim Patent werden beim Gebrauchsmuster die sachlichen Schutzvoraussetzungen, d.h. Neuheit, erfinderischer Schritt und gewerbliche Anwendbarkeit, jedoch nicht vor der Eintragung geprüft. Auf europäischer Ebene gibt es den Gebrauchsmusterschutz nicht und es ist auch kein Gebrauchsmuster mit einheitlicher Wirkung wie im Patentrecht geplant.

Ein Patent gibt dem Patentinhaber (oder seinem ausschließlichen Lizenznehmer) das Recht, Dritte von der Nutzung des Gegenstands des Patents, d.h. der patentierten Technologie, auszuschließen und die Technologie alleine zu nutzen.

Ist Gegenstand des Patents eine Vorrichtung, etwa eine Maschine oder eine Anlage, die durch eine KI gesteuert wird, kann der Patentinhaber die Benutzung des Erzeugnisses als Ganzes verbieten, ebenso das Anbieten, in Verkehr bringen oder Einführen der Vorrichtung (§ 9 Nr. 1 PatG). Ferner ist die Lieferung von Mitteln, die sich auf ein wesentliches Element der Erfindung beziehen, verboten, wenn der Lieferant weiß oder es aufgrund der Umstände offensichtlich ist, dass diese Mittel dazu geeignet und bestimmt sind, für die Benutzung der Erfindung in Deutschland verwendet zu werden (sog. mittelbare Patentverletzung, § 10 PatG).

Handelt es sich bei der patentierten KI-Anwendung um ein Verfahrenspatent, kann der Patentinhaber jedem Dritten verbieten, das Verfahren im räumlichen Schutzbereich des Patents anzuwenden oder, wenn der Dritte weiß oder es auf Grund der Umstände offensichtlich ist, dass die Anwendung des Verfahrens ohne Zustimmung des Patentinhabers verboten ist, zur Anwendung im Geltungsbereich dieses Gesetzes anzubieten (§ 9 Nr. 2 PatG). Ebenso kann das Anbieten und Liefern einer Vorrichtung, mit der ein patentgeschütztes Verfahren ausgeübt werden kann, eine mittelbare Patentverletzung gemäß § 10 Abs. 1 PatG darstellen. Da im Bereich der computerimplementierten Erfindungen Verfahrenspatente vorherrschend sind, kommt § 9 Nr. 2 PatG eine hohe praktische Relevanz zu. Als Beispiel kann hier das bereits genannte Verfahren zur Erkennung von Tumoren dienen.

Schließlich kann der Inhaber eines Verfahrenspatents Dritten noch verbieten, die durch das Verfahren unmittelbar hergestellten Erzeugnisse anzubieten, in Verkehr zu bringen oder zu gebrauchen (§ 9 Nr. 3 PatG). Durch diese Variante soll verhindert werden, dass Produkte, die durch das patentierte Verfahren hergestellt werden, in den Verkehr gelangen, etwa weil das Verfahren im patentfreien Ausland ausgeführt wird und die Produkte sodann ins Inland verbracht werden. Umfasst sind in jedem Fall körperliche Produkte, die durch ein KI-gestütztes Herstellungsverfahren hergestellt werden.

Dem durch den Eingriff in sein Patent verletzten Patentinhaber stehen zunächst Ansprüche auf Unterlassung künftiger Rechtsverletzungen zu (§ 139 Abs. 1 PatG).

Weiter kann der Patentinhaber – bei vorsätzlicher oder fahrlässiger Handlung – den Ersatz aller durch die Benutzung des geschützten Patentgegenstands eingetretenen und noch eintretenden Schäden verlangen (§ 139 Abs. 2 PatG). Für die Schadensberechnung stehen dem Patentinhaber drei Berechnungsmethoden zur Verfügung: Ersatz seines entgangenen Gewinns, Zahlung einer fiktiven Lizenzgebühr, die vernünftige Lizenzvertragsparteien einem Lizenzvertrag zugrunde gelegt hätten (sogenannte Lizenzanalogie), und Herausgabe des Verletzergewinns. Dieser wird berechnet, indem vom Umsatz mit der geschützten Vorrichtung oder dem geschützten Verfahren die Kosten abgezogen werden, die unmittelbar durch die Herstellung oder den Vertrieb des rechtsverletzenden Produkts entstanden sind. Fixkosten sind nicht gewinnmindernd abzugsfähig.

Ferner hat der Patentinhaber einen Anspruch auf Auskunft und Rechnungslegung, um Informationen über die Herkunft und die Vertriebswege der Verletzungsprodukte sowie über die Namen und Anschriften der Hersteller, Lieferanten oder anderer Vorbesitzer und über die gewerblichen Abnehmer sowie über die Menge der hergestellten oder ausgelieferten Erzeugnisse zu erhalten (§ 140b PatG, § 242 BGB).

Schließlich kann vom Verletzer der Rückruf der geschützten Erzeugnisse oder deren endgültige Entfernung aus den Vertriebswegen und die Vernichtung der im Eigentum oder im Besitz des Verletzers befindlichen geschützten Erzeugnisse verlangt werden (§140a PatG).

2.1.2 Halbleiter

Nach dem Halbleiterschutzgesetz (HalblSchG)[2] sind „Halbleitererzeugnisse“ dreidimensionale Strukturen, die aus einem Körper bestehen, dessen Oberfläche eine Schicht aus halbleitendem Material und eine oder mehrere weitere Schichten aus leitendem, isolierendem oder halbleitendem Material aufweist, die nach einem vorgegebenen dreidimensionalen Muster angeordnet sind.[3]

---

[2] Umsetzung der Europäischen Richtlinie 87/54/EWG.

[3] Klett/Sonntag/Wilske, Intellectual Property Law in Germany, Seite 51.

Schutzfähig ist die Topographie von mikroelektronischen Halbleitererzeugnissen und unabhängig nutzbaren Teilen sowie Darstellungen zur Herstellung der Topographie, § 1 Abs. 1 HalblSchG. Die zugrunde liegenden Konzepte, Verfahren, Systeme und Techniken sowie die gespeicherten Informationen sind ausdrücklich vom Schutz ausgenommen, § 1 Abs. 4 HalblSchG. Der Schutz von Halbleitererzeugnissen ist auf EU-Ebene harmonisiert.[4]

2.1.3 Urheberrecht

Das deutsche Gesetz über Urheberrecht und verwandte Schutzrechte (UrhG)[5] gewährt dem Urheber die alleinigen Rechte an seinem Werk. Der Schutz entsteht automatisch durch die Schaffung desselben, anders als ein Patent muss es also nicht in ein Register eingetragen werden. Das Gesetz erstreckt sich nicht nur auf eigenschöpferische Werke wie Kunstwerke oder musikalische Darbietungen, sondern auch auf Computerprogramme und Datenbanken (siehe nachfolgende Ziffer 2.1.3.2 für weitere Einzelheiten zu Datenbanken). Es ist daher für den Schutz von KI in allen Ausprägungen relevant.

2.1.3.1 Schutz von Computerprogrammen

KI-Systeme werden üblicherweise auf der Grundlage von Software realisiert, so dass zunächst an einen Schutz als Computerprogramm zu denken ist.

Das Gesetz enthält keine Legaldefinition des Begriffs Computerprogramm. Weithin wird ein Computerprogramm als ein Satz von Anweisungen an ein informationsverarbeitendes Gerät und an den mit diesem Gerät arbeitenden Menschen zur Erzielung eines Ergebnisses definiert.[6] Voraussetzung eines Schutzes ist ein Minimum an Schöpfungshöhe. Aus letztgenanntem Prinzip wird allgemein geschlossen, dass all diejenigen Elemente, die nicht individuell durch einen menschlichen Urheber geprägt wurden, nicht schutzfähig sind. Dazu gehören Algorithmen ebenso wie allgemeine Prinzipien mathematischer Logik.[7] Ebenso wenig schutzfähig sind diejenigen Komponenten, die automatisiert von einer Maschine erzeugt wurden.

Damit ist zwar grundsätzlich der Schutz der konkreten Anordnung bei hinreichender Schöpfungshöhe als Computerprogramm möglich. Allerdings bleibt die technische Funktionalität gemeinfrei, da Ideen und Konzepte als solche urheberrechtlich nicht schutzfähig sind.[8]

---

4 Richtlinie 87/54/EWG des Rates vom 16. Dezember 1986 über den Rechtsschutz der Topographien von Halbleitererzeugnissen.

5 Einschließlich des Gesetzes über Urheberrecht und verwandte Schutzrechte (UrhG) und des Gesetzes über das Urheberrecht an Werken der bildenden Künste und der Photographie (Kunsturhebergesetz – KunstUrhG).

6 KG Berlin CR 2010, 424, 425.

7 Schricker/Loewenheim/Spindler, Urheberrecht, § 69 a Rn. 12.

8 Apel/Kaulartz, RDi 2020, 24 ff. Rn. 18.

2.1.3.2 Schutz von Datenbanken

Zum Teil wird der Schutz von KI als Datenbankwerk oder über das Leistungsschutzrecht an der Datenbank diskutiert. Während ein Datenbankwerk legaldefiniert ist als ein Sammelwerk, dessen Elemente systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind, ist nach der Legaldefinition des § 87 a Abs. 1 UrhG eine Datenbank eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder in anderer Weise zugänglich sind. Allerdings handelt es sich bei einer generativen KI schon nicht um die hierfür erforderliche Sammlung unabhängiger Elemente mit selbständigem Informationswert. Begründet wird dies damit, dass der Information zwar ein Aussagegehalt zukomme, sie aber keinen Nutzen über den Kontext des konkreten Netzes hinaus habe und auch nicht unabhängig von den anderen Elementen des Netzwerks sei.[9] Dementsprechend bieten diese Regelungen aktuell keinen hinreichenden Schutz.

2.1.4 Designs und Geschmacksmuster

Der Designschutz nach dem deutschen Gesetz über den rechtlichen Schutz von Design (Designgesetz – DesignG) ist dem Schutz des Urheberrechts recht ähnlich. Ein wesentlicher Unterschied zum Schutz des Urheberrechts besteht darin, dass für den Schutz eines Designs grundsätzlich eine Eintragung erforderlich ist, § 27 DesignG. Ein schutzfähiges Design liegt bei zweidimensionalen Mustern oder dreidimensionalen Modellen vor, welche neu sind und Eigenart besitzen. Das schutzfähige Muster oder Modell kann sich nur auf ein Erzeugnis beziehen, worunter jeder industrielle oder handwerkliche Gegenstand verstanden wird, einschließlich der Verpackung und Ausstattung.

Computerprogramme als solche sind keine Erzeugnisse und daher vom Designschutz ausgeschlossen. Dem Designschutz zugänglich ist jedoch beispielsweise die konkrete Darstellung des Musters, nicht aber die mathematischen Anweisungen, welche die konkrete Darstellung erzeugen, d.h. nicht die Programmlogik.

Auch die EU bietet einen Geschmacksmusterschutz durch ein einheitliches EU-Geschmacksmusterrecht nach der Verordnung (EG) Nr. 6/2002 des Rates vom 12. Dezember 2001 (Gemeinschaftsgeschmacksmusterverordnung – GGV). Nach Art. 5 GGV ist ein Geschmacksmuster neu, wenn vor dem Anmeldetag kein identisches Design offenbart worden ist. Eigenart hat es dann, wenn sich der Gesamteindruck, den es bei einem informierten Benutzer hervorruft, von dem Gesamteindruck unterscheidet, den ein anderes Design bei diesem Benutzer hervorruft, welches vor dem Anmeldetag offenbart worden ist.

Im Rahmen von Künstlicher Intelligenz wird Designschutz daher dann eine Rolle spielen, wenn beispielsweise die äußere Gestaltung eines Roboters mit integrierter Künstlicher Intelligenz einem Schutz unterstellt werden soll.

---

[9] Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, § 9 Rn. 54.

2.1.5 Marken

Gemäß § 3 MarkenG und Art. 4 UMV können als Marke alle Zeichen, insbesondere Wörter, Abbildungen, Buchstaben, Zahlen, Klänge, dreidimensionale Gestaltungen sowie Farben und Farbzusammenstellungen geschützt werden, die geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden.

Künstliche Intelligenz, die kommerziell vertrieben wird, kann markenrechtlich geschützt werden:

Marken müssen stets für bestimmte Waren und Dienstleistungen eingetragen werden, die wiederum verschiedenen Klassen zugeordnet sind. In Deutschland ist der Schutz über eine deutsche, d.h. nationale Marke und eine Unionsmarke möglich, die nach ihrer Eintragung in allen Ländern der Europäischen Union Schutz beansprucht. Auf einer solchen Marke basierend kann dann in den meisten Ländern dieser Welt auch international Schutz über die Internationale Markenregistrierung beansprucht werden. Da es sich bei Künstlicher Intelligenz meist um mathematische Lösungen handelt, die in Software realisiert sind, kommt ein Schutz im Rahmen der Klassifizierung der Künstlichen Intelligenz als Software in Betracht. Demnach könnte ein Schutz für eine Künstliche Intelligenz in der Klasse 9 der sog. Nizza-Klassifikation beantragt werden.

Je nach Funktionalität und Verwendungsform der Künstlichen Intelligenz kann auch eine andere Klassifizierung in Betracht kommen. Wenn die Künstliche Intelligenz z.B. in ein bestimmtes Gerät eingebaut ist, ist die Marke in der Klasse zu schützen, in die das Gerät fällt. Ein intelligenter Kühlschrank mit einer integrierten KI würde wie ein herkömmlicher Kühlschrank in der Klasse 11 geschützt.

Neben der Anmeldung von Wort- und Bildmarken können auch Zeichen wie Hörmarken, dreidimensionale Gestaltungen, Farben und Farbkombinationen als Marke angemeldet werden. Allerdings ist Voraussetzung, dass das Zeichen unterscheidungskräftig und nicht rein beschreibend ist. Es muss stets als Herkunftshinweis wirken. Dies ist bei 3D-Marken und Farbmarken nicht immer der Fall. Handelt es sich um eine übliche Farbe oder Farbkombination oder eine übliche Gestaltungsform, werden entsprechende Markenanmeldungen nur dann eingetragen, wenn für die Anmeldung eine erhebliche Bekanntheit im Verkehr nachgewiesen werden kann.

Der Schutz einer 3D-Marke könnte beispielsweise für einen Roboter mit integrierter Künstlicher Intelligenz in Betracht kommen, wenn dieser eine charakteristische Formensprache aufweist und als Hinweis auf die Herkunft von den angesprochenen Verkehrskreisen wahrgenommen wird.

2.1.6 Know-how und Geschäftsgeheimnisse

Künstliche Intelligenz ist häufig innovativ – wie bei jeder innovativen Technologie stellt sich die Frage, inwieweit einzelne Elemente als Geschäftsgeheimnis gegen unbefugte Nutzung und Offenlegung geschützt sein können.

Eine KI in Form eines KI-basierten Systems, der Quellcode einer KI-Anwendung oder der ihr zugrunde liegende Algorithmus kann als Geschäftsgeheimnis geschützt sein. Der Quellcode einer KI-Anwendung respektive der der Anwendung zugrunde liegende Algorithmus stellt regelmäßig die Basis des Geschäftsmodells eines Unternehmens dar und vermittelt diesem einen entscheidenden Wettbewerbsvorteil. Dieser Wettbewerbsvorteil basiert gleichsam darauf, dass die Informationen nicht öffentlich bekannt und damit auch nicht ohne weiteres replizierbar sind.

Der Schutz von Geschäftsgeheimnissen wird durch das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), das seit dem 18. April 2019 in Kraft ist, geregelt. Nach § 2 Nr. 1 GeschGehG ist ein Geschäftsgeheimnis eine Information

a) 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

b) der Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Für die Qualifizierung als Geschäftsgeheimnis ist es zunächst erforderlich, dass die relevante Information, beispielsweise der Quellcode oder der Algorithmus, insoweit geheim gehalten werden, als die Öffentlichkeit keinen Zugang hat (Buchstabe a). Unerheblich ist dabei, wenn einzelne Elemente bekannt werden, da es nach dem Gesetz nur schädlich ist, wenn die Information insgesamt oder in ihrer genauen Anordnung und Zusammensetzung ihrer Bestandteile zugänglich ist.

Eine Information ist nicht allgemein bekannt, wenn nur der berechtigte Inhaber und zur Geheimhaltung verpflichtete Dritte sie kennen. Wird sie jedoch einem darüber hinaus gehenden größeren Kreis offenbart, kann der Geheimnischarakter in Frage gestellt sein. Letztlich handelt es sich hier um eine Wertungsfrage, so dass es auf den Einzelfall ankommt, ob eine Information allgemein bekannt ist. Entscheidend ist, ob der Geheimnisinhaber den Kreis der „Wissenden" unter Kontrolle behält.[10]

Die Information muss schließlich für den Inhaber einen wirtschaftlichen Wert haben, weil sie geheim ist. Dies ist der Fall, wenn ihre unbefugte Nutzung oder Offenbarung den Inhaber aller Voraussicht nach dadurch schädigt, dass das wissenschaftliche oder technische Potenzial, die geschäftlichen oder finanziellen Interessen, die strategische Position oder die Wettbewerbsfähigkeit des Inhabers untergraben werden.[11]

Dies liegt bei dem Quellcode oder dem Algorithmus einer KI-Anwendung auf der Hand. Die Veröffentlichung dieser Informationen würde den Wettbewerbsvorteil und damit ggf. die Anzahl der Nutzer und damit die Profitabilität und den Marktanteil des Inhabers beschränken.

---

[10] BVerwG PharmR 2020, 699, (701); Ohly/Sosnitza/Ohly, 8. Auflage 2023, GeschGehG, § 2 Rn. 6.

[11] Ohly/Sosnitza/Ohly GeschGehG § 2 Rn. 10.

Geschäftsgeheimnisschutz wird Informationen wie dem Quellcode einer KI-Anwendung nach dem GeschGehG nur zuerkannt, wenn der Inhaber den Umständen nach angemessene Geheimhaltungsmaßnahmen ergriffen hat (Buchstabe b).

Die Anforderungen sollen hier nicht überspannt werden. Ausreichend sind angemessene und vernünftige, nicht jedoch absolut wirksame oder unumgehbare Schutzmaßnahmen.[12] Eine schablonenhafte Anwendung bestimmter Maßnahmen ist nicht empfehlenswert. Für die Frage, welche Maßnahmen den Umständen nach angemessen sind, ist eine Einzelfallbetrachtung erforderlich, welche Maßnahmen für ein bestimmtes Geschäftsgeheimnis erforderlich sind.

Hierbei können insbesondere der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten, die Natur der Informationen, die Bedeutung für das Unternehmen, die Größe des Unternehmens, die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Informationen und vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern berücksichtigt werden.[13]

Empfehlenswert ist eine Kombination aus physischen oder technischen Zugangsbeschränkungen und Vorkehrungen (z.B. Passwortschutz, Zugang nur für bestimmte Mitarbeiter) mit vertraglichen Sicherungsmechanismen (z.B. Geheimhaltungsklauseln in Arbeitsverträgen und Projektverträgen). Grundsätzlich gilt, dass je wichtiger und wertvoller das Geschäftsgeheimnis für ein Unternehmen ist, desto aufwändigere Schutzmaßnahmen erforderlich sind, um den Schutz als Geschäftsgeheimnis zu erhalten.

Für das schließlich erforderliche berechtigte Interesse an der Geheimhaltung (Buchstabe c) ist jedes vernünftige wirtschaftliche Interesse ausreichend. Nur ausnahmsweise, etwa bei Vorliegen von Straftaten, kann das berechtigte Interesse fehlen. Im Zusammenhang mit dem Quellcode oder dem Algorithmus einer KI ist nur in krassen Ausnahmefällen ein fehlendes berechtigtes Interesse vorstellbar. Zu denken wäre hier, wenn überhaupt, an Algorithmen oder KI-Anwendungen, die auf Diskriminierungen angelegt sind, oder wenn ein KI-System eine verbotene Praktik gemäß Artikel 5 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung Harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union[14] einsetzt.

Besteht Geschäftsgeheimnisschutz für den Quellcode oder den Algorithmus eines KI-Systems, darf ein solches Geschäftsgeheimnis nicht gegen den Willen des Inhabers erlangt, offengelegt oder genutzt werden, § 4 GeschGehG. Verboten ist das Kopieren von Dokumenten, Gegenständen und Materialien, die das Geschäftsgeheimnis enthalten. Auch wer Geschäftsgeheimnisse von Dritten erhalten hat, darf diese nicht nutzen oder offenlegen, wenn es ersichtlich war, dass diese Dritte das Geschäftsgeheimnis unbefugt erlangt haben.

---

[12] OLG Hamm WRP 2021, 223 (237) – Stopfaggregat; Ohly/Sosnitza/Ohly, 8. Auflage 2023, GeschGehG § 2 Rn. 13. m.w.N.

[13] Begr. RegE BT-Drs. 19/4724.

[14] https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01a75ed71a1.0019.01/DOC_1&format=DOC.

Im Falle einer Verletzung des Geschäftsgeheimnisses kann der Inhaber gegen den Vertrieb von rechtsverletzenden Produkten vorgehen. Ihm steht insoweit ein Unterlassungs- und Beseitigungsanspruch zu, § 6 GeschGehG. Für vergangene Verletzungshandlungen kann der Inhaber Schadensersatz fordern, § 10 Abs. 1 GeschGehG. Zur Berechnung des Schadensersatzanspruchs kann der Verletzte zwischen mehreren Berechnungsmethoden die für ihn günstigste Berechnungsmethode auswählen: Ersatz seines entgangenen Gewinns, Berechnung auf der Basis eines fiktiven angemessenen Lizenzsatzes oder Abschöpfung des Gewinns des Rechtsverletzers, § 10 Abs. 2 GeschGehG.

Grundsätzlich ist es möglich, gegen alle Verletzungsprodukte vorzugehen, deren Konzeption, Merkmale, Funktionsweise, Herstellungsprozess oder Marketing in erheblichem Umfang auf dem rechtswidrig erlangten, genutzten oder offengelegten Geschäftsgeheimnis beruhen.

Weiter hat der Verletzte einen Anspruch auf Vernichtung oder Herausgabe von Unterlagen, die das Geschäftsgeheimnis verkörpern, und auf Rückruf, Entfernung und Rücknahme vom Markt sowie Vernichtung von rechtsverletzenden Produkten. Zur Aufdeckung des Umfangs der Verletzungshandlungen gibt das GeschGehG dem Inhaber eines Geschäftsgeheimnisses einen weitgefassten Auskunftsanspruch, § 8 GeschGehG.

Neben dem GeschGehG bestehen in Deutschland auch einige Sonderregelungen in anderen Gesetzen, insbesondere im Strafgesetzbuch.[15] Die rechtswidrige Verwertung von Betriebs- oder Geschäftsgeheimnissen Dritter ist etwa nach § 204 StGB strafbar, wenn der Dritte nach § 203 StGB zur Geheimhaltung der Informationen verpflichtet wurde.

2.1.7 Rechtliche Aspekte des Trainings von KIs

2.1.7.1 Urheberrechtliche Zulässigkeit der Verwendung von Daten zum Training von KIs

Die Frage der Zulässigkeit der Verwendung von urheberrechtlich geschütztem Material zum Training von KI-Anwendungen wird derzeit viel diskutiert, nicht zuletzt aufgrund einiger großer Gerichtsprozesse. So wehrt sich nicht nur Getty Images hiergegen,[16] auch die Künstlerinnen Sarah Andersen, Kelly McKernan und Karla Ortiz klagen vor US-amerikanischen Gerichten gegen die Nutzung ihrer Bilder zu Trainingszwecken mit dem Vorwurf, die Werke seien ohne entsprechende Einwilligung in die Datenbanken der KI-generierte Systeme eingespeist worden.[17]

---

[15] Zum Beispiel § 202a ff. StGB, Datenspionage und Phishing.

[16] Siehe https://www.heise.de/news/Kunst-oder-Klau-Getty-Images-verklagt-KI-Bildermacher-Stability-ai-7461617.html, zuletzt aufgerufen am 23.05.2023.

[17] Siehe https://www.golem.de/news/stable-diffusion-und-midjourney-urheberrechtsklage-gegen-ki-bildgeneratoren-2301-171242.html.

Für das Training von KI-Anwendungen werden die Daten in der Regel nur automatisiert verarbeitet, um daraus zu „lernen". Technisch erfordert dies aber zumindest eine vorübergehende Vervielfältigung. Hier kommt das Urheberrecht zur Anwendung, welches nicht nur an dauerhafte, sondern auch an temporäre Vervielfältigungen anknüpft. Grundsätzlich bedarf es zur Verwendung urheberrechtlich geschützter Texte oder Bilder daher einer Erlaubnis des Urhebers oder einer gesetzlichen Erlaubnis, dem Grunde nach also auch für die Verwendung von urheberrechtlich geschützten Werken zu Trainingszwecken für eine KI.

Eine Ausnahme von der Zustimmungsbedürftigkeit gewährt § 44a UrhG. Danach ist eine vorübergehende Vervielfältigung zulässig, sofern sie lediglich flüchtig oder begleitend ist und keine eigenständige wirtschaftliche Bedeutung hat. Diese Ausnahmeregelung greift vorliegend jedoch bereits deshalb nicht, da dem Trainingsmaterial als Grundlage des Trainings sehr wohl erhebliche wirtschaftliche Bedeutung zukommt.[18]

Relevant ist allerdings die Schranke des sog. Data Mining gemäß § 44b Abs. 1 UrhG. Unter Data Mining wird dabei die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken zur Gewinnung von Informationen, insbesondere über Muster, Trends und Korrelationen, verstanden. Nach der auf einer europäischen Richtlinie aus dem Jahr 2019 beruhenden Vorschrift des § 44b UrhG sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text- und Data Mining auch ohne Einwilligung des jeweiligen Urhebers zulässig.

Das Training einer KI-Anwendung unter Verwendung von urheberrechtlich geschützten Werken ist dementsprechend unter den oben genannten Voraussetzungen grundsätzlich lizenzfrei zulässig. Der Gesetzgeber schreibt vor, dass die Vervielfältigungen zu löschen sind, wenn sie für das Text- und Data Mining nicht mehr erforderlich sind, vgl. § 44b Abs. 2 UrhG. Dies dürfte regelmäßig nach Abschluss des Trainings der Fall sein.

Rechteinhaber haben jedoch die Möglichkeit zum Opt-Out. Sie können einen Vorbehalt gegen ein solches Data Mining erklären, der allerdings zwingend in maschinenlesbarer Form erfolgen muss (siehe § 44b Abs. 3 UrhG). Hier herrscht noch weitestgehend Unklarheit, wie dieser Vorbehalt im Einzelnen ausgestaltet sein muss. Reicht es beispielsweise aus, wenn vom Rechteinhaber eine Registrierungspflicht oder eine Paywall zum Schutz vor dem sogenannten Webscraping eingebaut wurde? Insoweit bleibt auch abzuwarten, ob § 44b UrhG in seiner jetzigen Form überhaupt erhalten bleiben wird: die Vorschrift wurde in das Gesetz eingeführt, bevor das Problem der generativen Künstlichen Intelligenz überhaupt breit diskutiert wurde. Sie dürfte daher in naher Zukunft auf dem Prüfstand stehen.

Ergänzend sei erwähnt, dass derzeit auch diskutiert wird, ob für *maschine learning* ein besonderes Leistungsschutzrecht eingeführt werden sollte, welches von Verwertungsgesellschaften verwaltet werden würde. Hierdurch bestünde die Möglichkeit – ähnlich der Kopierabgabe –, die betroffenen Urheber finanziell zu beteiligen. Die Frage,

---

[18] Spindler GRUR 2016, 1112, 1114.

ob es tatsächlich eines solchen Leistungsschutzrechts bedarf, lässt sich nicht einfach beantworten.[19] Insoweit besteht zudem das faktische Problem, dass die großen Player im Bereich Künstlicher Intelligenz bereits alles öffentlich Verfügbare zum Training verwendet, respektive „gescraped" haben. Es wird also eingewandt, dass durch etwaige Abgaben lediglich Hürden für neue Player entstünden, was den Marktvorsprung derjenigen zementierte, die Vorreiter in diesem Bereich waren. Indes werden auch die Vorreiter ihren Datenschatz regelmäßig aktualisieren müssen; in dem Fall wären sie durch etwaige Abgaben ebenfalls betroffen.

2.1.7.2 Datenschutzrechtliche Zulässigkeit der Verwendung von Daten zum Training von KIs

Auch datenschutzrechtliche Vorgaben gilt es beim Training von KI-Anwendungen im Blick zu behalten. Insoweit verweisen wir auf unsere Ausführungen in Kapitel 4.1.7 „Exkurs: Datenschutz bei ChatGPT". Die dort erläuterte Datenschutzrechtslage ist für andere text- oder bildgenerierende KIs ebenfalls relevant.

2.2 Schutz der mithilfe von Künstlicher Intelligenz geschaffenen Arbeitsergebnisse

Künstliche Intelligenz kann Arbeitsergebnisse schaffen, die durch geistige Eigentumsrechte geschützt wären oder geschützt werden könnten, wenn sie von Menschen produziert würden, wie z.B. Texte, Graphiken, Bilder, Videos oder Musik.[20]

Zahlreiche Projekte dieser Art wurden über die Medien einem breiteren Publikum bekannt, insbesondere das von einer KI-geschaffene und bei einer Auktion für rund eine halbe Million Euro verkaufte Portrait des Edmond de Belamy. Auf breiter Ebene wird mit KI experimentiert und es werden auch von Gebrauchstexten über Gedichte bis hin zu einfachen Computerspielen viele verschiedene Ergebnisse kreiert. Neben diesen Experimenten wird KI aber auch heute schon in größerem Umfang herangezogen, um Menschen bei ihrem Werkschaffen zu unterstützen. Zu denken ist hier an einfache Anwendungen wie Bildoptimierung, aber auch an die Unterstützung bei der Schaffung von Computerspielewelten. Nicht zuletzt die Ende 2022 vorgestellten Tools wie der Textgenerator ChatGPT oder die Bildgeneratoren Midjourney, Stable Diffusion oder DallE2 machen diese KI-Anwendungen nunmehr einem breiten Publikum nutzbar. Auch KI-Anwendungen, die Softwareentwickler bei der eigentlichen Programmierung von Source Code unterstützen (beispielsweise der GitHub Copilot), haben erhebliche Bedeutung erlangt und unter Umständen erhebliche Auswirkungen auf die Schutzrechte an den Arbeitsergebnissen.

Nach geltendem Recht ist es Künstlicher Intelligenz jedoch nicht möglich, geistiges oder gewerbliches Eigentum zu besitzen.

---

[19] Vgl. zur Diskussion Krone RDi 2023, 117, 122 m.w.N.

[20] Bezüglich mittels KI generierter Programmcodes siehe Siglmüller/ Gassner, RDi 2023, 124 ff.

Weniger leicht zu beantworten ist, inwieweit Menschen oder juristische Personen Inhaber der Rechte an geistigem oder gewerblichem Eigentum sein können, das von einer Künstlichen Intelligenz oder mit ihrer Hilfe geschaffen wurde – oder ob KI-geschaffene Arbeitsergebnisse, der sogenannte Output, überhaupt schutzfähig sind. Die Frage stellt sich vor allem dann, wenn die KI nicht nur Unterstützung wie ein Werkzeug leistet, sondern das Werk quasi selbstständig schafft. Insoweit ist nach den einzelnen Schutzrechten zu unterscheiden.

2.2.1 Vorschläge Expertengruppe der EU-Kommission 2019

Ausgangspunkt der Frage, wer als Urheber eines mittels KI-kreierten Werkes ist, ist § 2 Abs. 2 UrhG. Urheberrechtlich schutzfähig ist ein Werk jeglicher Art nur dann, wenn es eine persönliche geistige Schöpfung des Urhebers darstellt. Dabei ist „persönlich" nur, was auf menschliches Schaffen zurückgeht. Dies erfordert nach einheitlicher Ansicht eine menschlich-gestalterische Tätigkeit, weshalb weder Tiere noch Maschinen ein „Werk" im urheberrechtlichen Sinne erschaffen können. Mangels menschlichen Schaffens konnte beispielsweise auch das berühmte Selfie des Affen Naruto keinen Urheberrechtsschutz genießen. Ebenso fehlt es KI-generierten Werken an einer menschlichen Schöpfung.

Künstliche Intelligenzen selbst können demgemäß nach deutschem Urheberrecht grundsätzlich keine persönliche Schöpfung erbringen, damit auch kein urheberrechtsschutzfähiges Werk erschaffen. Die Entwickler oder Anbieter der KI sind mithin ebenso wenig Urheber des erzeugten Outputs und die von KI-erzeugten Ergebnisse sind nicht urheberrechtlich geschützt. Daher kann beispielsweise OpenAI an den mittels ChatGPT generierten Inhalten eigentlich auch keine Nutzungs- und Verwertungsrechte einräumen. Dies hält die Anbieter der KI allerdings in der Praxis oft nicht davon ab, in ihren Allgemeinen Geschäftsbedingungen den Nutzern sämtliche Rechte einzuräumen. Entsprechende Klauseln dürften so zu verstehen sein, dass die Entwicklungsunternehmen klarstellen, keine Rechte an den generierten Inhalten zu beanspruchen.

Naturgemäß kann sich ein Mensch allerdings technischer Hilfsmittel bedienen und die hierdurch erschaffenen Werke können schutzfähig sein. Man denke beispielsweise an den Einsatz eines Computers oder einer Kamera. Für sämtliche Werke gilt, dass sie ein gewisses Mindestmaß an Schöpfungshöhe erreichen und sich vom Handwerklichen oder Alltäglichen abheben müssen, um in den Genuss des urheberrechtlichen Schutzes – mit einer Dauer von 70 Jahren nach dem Tod des Urhebers – zu kommen.

Betrachtet man also die KI als ein solches Werkzeug, so käme als Urheber derjenige Nutzer in Betracht, der die Anfrage bei der KI wie ChatGPT stellt, nutzt er die entsprechende Computersoftware doch lediglich als Werkzeug/Hilfsmittel. Man denke nur an die Arbeit des OpenAI Mitarbeiters, der Vermeers berühmtes gemeinfreies Gemälde „*Das Mädchen mit dem Perlenohrring*" mittels KI über den Rand hinaus fortsetzen ließ. Um den urheberrechtlichen Schutzanforderungen zu genügen, müsste aber der menschliche Anteil am Output der KI wohl so hoch sein, dass dem Einsatz der KI eine lediglich untergeordnete Bedeutung zukommt. In vielen Fällen wird dem nicht so sein, insbesondere wenn der Nutzer den Output nur wenig steuern kann. In diesen Fällen wird kaum davon auszugehen sein, dass das Ergebnis dasjenige

einer künstlerischen Leitung und eines gestalterischen Prozesses des Eingebenden ist. Anders liegt es, wenn beispielsweise der von einer KI ausgegebene Text oder das Bild durch den Nutzer noch erheblich bearbeitet oder ergänzt wird. Dann könnte unter Umständen ein Schutz in Betracht kommen. Daneben sind viele Grenzfälle denkbar, die wohl in den kommenden Jahren die Rechtsprechung noch intensiver beschäftigen werden. Man stelle sich beispielsweise vor, dass ein Mensch die Prompts für eine KI wie Midjourney oder Dall-E lange und mühevoll in vielen Iterationen verfeinert, bis der Output seinen Vorstellungen entspricht.

Teilweise wird darüber nachgedacht, jenseits des Werkschutzes in Form eines Urheberrechts bestimmte Regelungen zu verwandten Schutzrechten anzuwenden. Diskutiert werden die Regelungen für Licht- und Laufbilder des § 72 UrhG oder auch die des Schutzes von Datenbanken des § 87a UrhG.

So gewährt § 72 UrhG einen Leistungsschutz für Lichtbildner. Hierunter fallen beispielsweise analoge Fotografien. Ausgenommen sind mittels elektronischer Befehle erzeugte Bilder einschließlich Computerbilder oder andere im Wege der digitalen Bildbearbeitung veränderte Bilder. Zudem wird auch für den Lichtbildschutz ein Mindestmaß an persönlicher geistiger Leistung gefordert. Diese wird zwar schon dann bejaht, wenn ein Bedienen der Kamera im Sinn einer handwerklichen Fertigung erfolgt. Lediglich bloß zufällig entstandenen Bildern fehlt dieses Tatbestandsmerkmal. Somit scheidet nach verbreiteter Ansicht ein Leistungsschutz nach § 72 UrhG für durch KI-generierte Bilder in vielen Fällen aus.

Daneben existiert in § 95 UrhG ein Leistungsschutz für sogenannte Laufbilder, unter anderem Filme. Auch Computerspiele können Laufbilder darstellen. Daher dürften auch von KI-generierte Laufbilder von der Vorschrift erfasst sein. Rechtsinhaber wäre derjenige, der den Prozess der Generierung der KI-generierten Laufbilder in Gang gesetzt hat. Soweit diese zufällig entstehen, scheidet § 95 UrhG ebenfalls aus.

Ähnlich verhält es sich gemäß § 85 UrhG mit dem Leistungsschutz des Tonträgerherstellers. Das Recht entsteht mit der erstmaligen Fixierung der konkreten Tonaufnahme. Tonträgerhersteller ist derjenige, dem aufgrund seiner wirtschaftlichen und organisatorischen Verantwortung der Erfolg der Herstellerleistung zuzuordnen ist. § 85 UrhG kommt bei KI-generieten Tonfolgen mithin immer dann zur Anwendung, wenn die Tonfolge erstmalig fixiert wird.

Schließlich ist das Recht des Datenbankherstellers nach § 87a UrhG zu erwähnen. Nach § 87a UrhG ist Datenbankhersteller derjenige, der die Investition in die Beschaffung, Überprüfung oder Darstellung der Datenbankelemente vorgenommen hat. Zweifelhaft ist in diesem Zusammenhang vor allem, ob bei den von einer KI-generierten Arbeitsergebnissen von einer erforderlichen systematischen und methodischen Anordnung im Sinne der Vorschrift gesprochen werden kann, erschöpft sich doch die von der KI-vorgenommene Anordnung in der Regel primär darin, einzelne Elemente zum Gesamtwerk zu fügen, nicht aber jegliche in der Sammlung enthaltene Elemente zu verorten.

2.2.1.1 Exkurs: Schutz der Prompts

Denkbar ist schließlich, dass Urheber der Texteingaben, die die Erstellung eines Bildes, Textes oder Codes steuern sollen, sogenannter „Prompts“, urheberrechtlichen Schutz für sich in Anspruch nehmen könnten. An die urheberrechtliche Schöpfungshöhe von Texten werden keine allzu hohen Anforderungen gestellt. Vielmehr reicht bereits die sogenannte „kleine Münze“ für die Schutzfähigkeit aus. Während man bei einfachen Prompts wohl davon ausgehen können wird, dass diese die für einen urheberrechtlichen Schutz erforderliche Schöpfungshöhe kaum erreichen dürften, könnten komplexere Prompts durchaus urheberrechtlichen Schutz genießen. Die Bejahung urheberrechtlichen Schutzes des Prompts führt allerdings noch nicht dazu, dass auch der mithilfe des Prompts kreierte Output ebenfalls dem Schutz unterstellt wird.

2.2.2 Markenrecht

Der von einer Künstlichen Intelligenz geschaffene Output kann in Zeichen wie Bildzeichen oder auch dreidimensionalen Zeichen münden, die sodann als Marke verwendet werden können. Insoweit gilt auch hier, dass der markenrechtliche Schutz im Regelfall erst durch eine Eintragung in die entsprechenden Register beim Deutschen Patent- und Markenamt (DPMA) bzw. beim Amt der Europäischen Union für Geistiges Eigentum (EUIPO) begründet wird und insoweit eine Zuordnung zu bestimmten Waren- oder Dienstleistungen erfolgen muss. Erst dann entfaltet die Marke ihren Schutz. Werden also KI-generierte Zeichen als Marke angemeldet, ist nicht ersichtlich, warum diese nicht einem Markenschutz unterstellt werden können sollen. Als Inhaber im Register benannt würde dann allerdings nicht die KI, sondern derjenige, der die Marke anmeldet. Denn als Anmelder einer Marke kommen lediglich natürliche oder juristische Personen sowie letztgenannten gleichgestellte Personeneinheiten in Betracht.[21]

2.2.3 Patent- und Gebrauchsmusterrecht

Nicht ganz eindeutig zu beurteilen ist die Situation bei Erfindungen nach dem Patent- oder Gebrauchsmustergesetz: Bei Patenten wird jede Erfindung nach dem Zuordnungsgrundsatz dem Erfinder zugeordnet.[22] Die Rechtfertigung für eine solche Zuweisung ist die schöpferische Leistung einer kreativen Persönlichkeit.[23]

Dem Patentrecht liegt die Vorstellung zugrunde, dass Erfindungen nur von natürlichen Personen gemacht werden können. Zwar dürften zumindest in der Vergangenheit Erfindungen ausschließlich von natürlichen Personen gemacht worden sein. Zukünftig werden jedoch immer häufiger KIs und KI-Systeme an Erfindungen beteiligt sein oder diese sogar eigenständig entwickeln.

---

[21] BeckOK MarkenR/Rohlfing-Dijoux, 33. Ed. 1.4.2023, UMV 2017 Art. 30 Rn. 9.1-10.1.

[22] Mellulis in: Benkard, Patentgesetz, 11. Auflage, § 6 Rn. 1.

[23] Mellulis in: Benkard, Patentgesetz, 11. Auflage, § 6 Rn. 1.

Der Erfinder ist gegenüber den beteiligten Patentämtern zwingend vom Anmelder zu benennen (außer der Erfinder verzichtet auf die Nennung). Ohne Benennung eines Erfinders wird die Anmeldung zurückgewiesen. Zudem steht ein aus einer Erfindung hervorgehendes Patent dem Erfinder oder seinem Rechtsnachfolger zu (vgl. § 6 Satz 1 PatG, Art. 60 Abs. 1 Satz 1 EPÜ).

Soweit ersichtlich, besteht unter den wichtigsten Patentämtern Einigkeit, dass eine KI nicht als Erfinder benannt und in das Patentregister eingetragen werden kann. So haben dies die Patentämter und Gerichte in den USA[24], Großbritannien[25], Deutschland[26] und Australien[27] abgelehnt, während das südafrikanische Patentamt die Erfindereigenschaft einer KI anerkannt hat.[28]

Auch die Juristische Beschwerdekammer des EPA hat in ihrer Entscheidung vom 21. Dezember 2021 (Rechtssache J 8/20) entschieden, dass eine KI kein Erfinder im Sinne des EPÜ sein kann. Das Bundespatentgericht (BPatG) hat die gleiche Frage differenzierter beantwortet: Zwar kann auch nach der Rechtsprechung des BPatG nur eine natürliche Person ein Erfinder sein. Allerdings eröffnet das BPatG die Möglichkeit, einen Zusatz anzubringen, wonach die natürliche Person „die KI dazu veranlasst habe, die Erfindung zu generieren."

Gleiches gilt für Gebrauchsmuster, die ebenfalls eine Erfindung voraussetzen, allerdings mit der Ausnahme, dass bei Gebrauchsmustern die Benennung des Erfinders nicht erforderlich ist. Der Gebrauchsmusterschutz kann daher dem Menschen nur aus den gleichen Gründen gewährt werden.

2.2.4 Halbleiterschutz

Die Topographie mikroelektronischer Halbleitererzeugnisse ist nur dann schutzfähig, wenn sie einen individuellen Charakter hat, der das Ergebnis geistiger Arbeit ist, § 1 Abs. 2 HalbSchG. Künstliche Intelligenz kann dies nicht erreichen.

2.2.5 Design- und Geschmacksmuster

Gemäß § 7 Abs. 1 DesignG und Art. 14 Abs. 1 GGV steht das Recht auf das Gemeinschaftsgeschmacksmuster dem Entwerfer oder seinem Rechtsnachfolger zu. Haben mehrere Personen das Erzeugnis gemeinsam entworfen, steht ihnen das Recht auf das

---

[24] In der Berufungsinstanz durch den U.S. Court of Appeals for the Federal Circuit bestätigt (Rechtssache Thaler v. Vidal, No. 21-2347 (Fed. Cir. 2022)).

[25] Bestätigt durch den Supreme Court in der Rechtssache Thaler (Appellant) v Comptroller-General of Patents, Designs and Trademarks (Respondent), Case ID: 2021/0201.

[26] Bundespatentgericht, Beschluss vom 11. November 2021, Aktenzeichen 11 W (pat) 5/21.

[27] https://www.managingip.com/article/2avep9ycmru17mjbp260w/australias-top-court-kills-dabus-and-landmark-ai-inventor-ruling.

[28] https://ipwatchdog.com/2021/07/29/dabus-gets-first-patent-south-africa-formalities-examination/id=136116/.

Gemeinschaftsgeschmacksmuster gemeinsam zu, § 7 Abs. 1 Satz 2 bzw. Art. 14 Abs. 2 GGV.

Unklar ist die Rechtslage bei autonom durch Künstliche Intelligenz erschaffenen Designs. Bekannt wurde beispielsweise das „The Chair Project (Four Classics)“ des Künstlerduos Philipp Schmitt und Steffen Weiß, bei welchem eine KI mittels einer Vielzahl von Designs von Stühlen trainiert wurde mit dem Ziel, sodann eigenständig Stühle zu entwerfen.

Zwar lässt sich weder dem DesignG noch der GGV entnehmen, dass eine Gestaltung durch einen menschlichen Akt der Kreativität erschaffen sein muss, um als Design eingetragen zu werden. Ganz allgemein wird jedoch davon ausgegangen, dass allen designrechtlichen Regelungswerken gemein ist, dass der Schutz eines Designs oder Gemeinschaftsgeschmacksmusters voraussetzt, dass eine natürliche Person ein solches Design bzw. Gemeinschaftsgeschmackmuster geschaffen hat, das die Verwirklichung einer schöpferischen Idee darstellt. Damit kann eine KI nicht Entwerfer eines Designs sein. Auch als Anmelder eines Designs kommt eine KI nicht in Betracht. In der Praxis sind Entwerfer und Anmelder eines Designs zumeist personenverschieden. Fehlt es also an einem Entwerfer, gilt nach der Fiktion des § 8 DesignG bzw. des Art. 17 GGV derjenige als Berechtigter, der das von der KI-geschaffene Design anmeldet, in der Regel also die natürliche Person.

2.2.6 Ergänzender wettbewerbsrechtlicher Leistungsschutz

Jenseits des Sonderrechtsschutzes durch das Urheber-, Design- und Patentrecht kommt ein Rückgriff auf den lauterkeitsrechtlichen Leistungsschutz in Betracht. Zu denken ist an die Tatbestände des § 4 Nr. 3 UWG. Danach handelt unlauter, wer Waren oder Dienstleistungen anbietet, die eine Nachahmung der Waren oder Dienstleistungen eines Mitbewerbers sind, wenn er a) eine vermeidbare Täuschung der Abnehmer über die betriebliche Herkunft herbeiführt, oder b) die Wertschätzung der nachgeahmten Ware oder Dienstleistung unangemessen ausnutzt oder beeinträchtigt, oder c) die für die Nachahmung erforderlichen Kenntnisse oder Unterlagen unredlich erlangt hat.

Selbst wenn sich eine Nachahmung bzw. eine wettbewerbliche Eigenart feststellen lassen, müssen zusätzlich die Tatbestandsmerkmale der Herkunftstäuschung (Buchst. a), des Ausnutzens oder der Beeinträchtigung der Wertschätzung (Buchst. b) oder einer unredlichen Informationserlangung (Buchst. c) vorliegen.

Auch ein Rückgriff auf die allgemeine Generalklausel des § 3 UWG unter dem Gesichtspunkt des unmittelbaren Leistungsschutzes dürfte zumeist wenig erfolgsversprechend sein. Die Rechtsprechung ist inzwischen mit der Annahme dieses Tatbestands – anders als früher – sehr zurückhaltend. Lediglich dann, wenn die Gefahr eines Marktversagens droht, d.h. dann, wenn der Anspruchsteller infolge freier Nachahmung nicht mehr in der Lage wäre, die für seine Tätigkeit erforderlichen Investitionen zu tätigen, kommt ein Anspruch in Betracht. Damit ist ein Rückgriff auf wenige Ausnahmefälle beschränkt.

Vor diesem Hintergrund dürfte das lauterkeitsrechtliche Normengefüge in den meisten Fällen keine Grundlage für einen Schutz der durch KI-erzeugten Arbeitsergebnisse darstellen.

2.2.7 Fazit zur Schutzfähigkeit

Arbeitsergebnisse, die sich aus den Handlungen einer Künstlichen Intelligenz ergeben, sind also im Grundsatz zunächst überhaupt nicht geschützt. Je nach Bearbeitungsgrad und Zutun des Nutzers können sie aber unter Umständen als ein urheberrechtlich geschütztes Werk der Person angesehen werden, die die Künstliche Intelligenz bedient hat.

Dieses Ergebnis mag auf den ersten Blick unbefriedigend sein, ist allerdings auch über die Grenzen des deutschen Rechts hinaus so anerkannt. Auch nach amerikanischem Recht wird das beispielsweise so gesehen.

So hatte im Februar 2023 das US Copyright Office in seinem ersten Fall zum Urheberrechtsschutz von KI-generierten Inhalten zu entscheiden. In dem als Fall „Kashtanova" bekannt gewordenem Verfahren hatte eine bekannte Künstlerin und KI-Forscherin Kristina Kashtanova den Comic „Zarya Of The Dawn" zum Schutz angemeldet. Die Bilder waren mithilfe der generativen KI Midjourney erstellt worden. Das US Copyright Office entschied, dass die einzelnen KI-generierten Bilder keinen Urheberrechtsschutz genießen. Lediglich die Anordnung der Bild- und Textelemente sowie der Text wurden als schutzwürdig erachtet.[29]

Es lässt sich natürlich auch die Frage stellen, ob ein umfassender Schutz der Arbeitsergebnisse von Künstlicher Intelligenz überhaupt wünschenswert wäre. KI kann in kürzester Zeit eine praktisch unbegrenzte Menge an Arbeitsergebnissen in die Welt setzen und könnte daher ebenso eine nahezu unbegrenzte Menge an Ausschließlichkeitsrechten produzieren. Dem könnte allenfalls durch eine strenge Auslegung der Schöpfungshöhe begegnet werden – wenn überhaupt. Plastisch wird das Problem anhand des Projektes „Allpriorart" (allpriorart.com), das sich zum Ziel gesetzt hat, Patentschutz als solchen zu vernichten, indem es eine unüberschaubare Anzahl von Texten in die Welt setzt, die dann als Stand der Technik gelten sollen und Patentschutz unmöglich machen. Wenn mit einem umgekehrten Ansatz beispielsweise versucht würde, urheberrechtlich schutzfähige Werke zu schaffen, könnte dies ebenfalls zu unangemessenen Ergebnissen führen.

Es lohnt sich, im Blick zu behalten, dass generative KI gewissermaßen erst seit November 2022 für jedermann verfügbar ist. Wie die Vielzahl der bereits nach kurzer Zeit anhängigen Klagen darlegt, befinden wir uns aktuell in einer Umbruchsituation. Viele der bisherigen Geschäftsmodelle werden durch die Möglichkeit der Nutzung KI-generierter Inhalte in Frage gestellt: wenn auf Knopfdruck ein Foto eines Models

---

[29] https://www.heise.de/hintergrund/Kuenstliche-Intelligenz-Kampf-um-das-Urheberrecht-7518607.html.

erstellt werden kann, so wird sich in Zukunft nicht nur die Firma Levi's fragen, warum sie aufwendige Modefotografie durchführen soll.[30] Vermehrt dürfte auch mit Fällen wie desjenigen des Magazins „Lisa Kochen und Backen" zu rechnen sein, in welchem die angepriesenen 99 Rezepte ausschließlich KI-generiert und mit entsprechenden Bildern versehen waren, ohne dass diese Tatsache dem Leser kenntlich gemacht worden wäre.[31] Viel einschneidender wird die Situation für Anbieter von Stock Fotographie wie beispielsweise Getty Images, die es möglicherweise in ein paar Jahren nicht mehr in der heutigen Form geben wird. Daher ist gut nachzuvollziehen, dass sie sich mit allen Mitteln, insbesondere juristischen, gegen die kostenfreie Nutzung ihrer Daten zum Training von KI zur Wehr setzen. Es dürfte nicht zu weit gegriffen sein, aktuell von einem „AI War" zu sprechen. Auch sollte den warnenden Stimmen wie der des „Godfather of AI", Geoffrey Hinton, zukünftig mehr Beachtung geschenkt werden. Es bleibt derzeit abzuwarten, wer in diesem Kulturkampf die Gewinner und Verlierer sein werden und insbesondere wie sich die Gesetzgeber und Gerichte hier positionieren werden.

2.3 Rechtsverletzungen durch Verwendung von KI-generierten Inhalten

2.3.1 Verletzung von Urheberrechten

Nutzer von Materialien wie Texten und Bildern, die mithilfe von KI-generiert wurden, werden sich die Frage stellen, ob sie hierdurch ggf. eine Urheberrechtsverletzung begehen könnten. Praktisch relevant ist dies beispielsweise dann, wenn eine KI wie ChatGPT einem urheberrechtlich geschützten Liedtext sehr stark ähnelt oder ein Gedicht nahezu identisch zum Original „ausgespuckt" wird. Der EuGH hat in der Vergangenheit bereits entschieden, dass ein aus elf Wörtern bestehender Auszug eines geschützten Werkes urheberrechtlich geschützt sein kann.[32] Noch plastischer wird es, wenn man sich vorstellt, dass eine bildgenerierende KI ein neues Bild auswirft, das beispielsweise auf der Grundlage eines berühmten Gemäldes eines noch lebenden Künstlers erschaffen wurde oder diesem stark angelehnt ist.

Urheber erfinden seit jeher das Rad nicht jedes Mal neu, sondern knüpfen oft an bereits bestehende schutzfähige Werke an. Dementsprechend regelt § 23 UrhG, dass Bearbeitungen eines Werkes nur mit Zustimmung des Urhebers veröffentlicht und verwertet werden dürfen. Wahrt das neu geschaffene Werk demgegenüber einen hinreichenden Abstand zum benutzten Werk, so liegt keine Bearbeitung, sondern eine freie Benutzung vor.

---

[30] https://www.derstandard.de/story/2000144903604/levis-nutzt-kuenftig-ki-generierte-models-um-die-diversitaet-zu.

[31] https://www.faz.net/aktuell/feuilleton/ausgabe-einer-zeitschrift-mit-ki-erstellt-burda-taeuscht-leser-18905878.html.

[32] EuGH GRUR 2009, 1041 Rn. 48 – Infopaq.

Die Frage der Abgrenzung zwischen (zulässiger) freier Benutzung und (zustimmungsbedürftiger) Bearbeitung stellte sich auch in der Vergangenheit in der analogen Welt vielfach und wurde mit Blick auf Parodien und Repliken von Kunstwerken vom Bundesgerichtshof näher ausgestaltet. Es kommt entscheidend auf den Abstand an, den das neue Werk zum ursprünglichen einhält, geht es doch um eine wertende Unterscheidung zwischen erlaubter Inspiration und verbotener Kopie. Für eine zulässige freie Benutzung müssen angesichts der Eigenart des neu geschaffenen Werks die entlehnten eigenpersönlichen Züge des geschützten älteren Werks verblassen.[33] Ein hinreichender Abstand liegt nach dem Europäischen Gerichtshof regelmäßig dann nicht vor, wenn das benutzte Werk wiedererkennbar ist.[34]

Diesen Maßstab wird man auch bei durch KI-generierte neuen Werken anwenden können. Dabei wird es im Einzelfall darauf ankommen, ob ein mittels KI-generiertes Werk (Text, Bild oder Graphik) einen hinreichenden Abstand zum ursprünglichen Werk aufweist und damit ohne Zustimmung des Urhebers des ursprünglichen Werkes zulässig ist. Das ist stets eine Frage des Einzelfalls. Im Blick zu behalten ist der angemessene Interessenausgleich zwischen dem Interesse des Rechtsinhabers an der Verwertung seines Werkes sowie dem Interesse an einer Fortentwicklung der Nutzer.[35]

Kommt man zum Ergebnis, dass der Output eine Rechtsverletzung darstellt, gilt im Verhältnis zwischen dem Nutzer und dem verletzten Urheber folgendes: Der Unterlassungsanspruch nach § 97 Abs. 1 UrhG ist verschuldensunabhängig und der Nutzer wäre Täter der Urheberrechtsverletzung.

Für einen Schadensersatzanspruch gemäß § 97 Abs. 2 UrhG wäre darüber hinaus ein vorsätzliches oder fahrlässiges Handeln erforderlich. Dem Nutzer einer KI sind Fehler nicht zuzurechnen, die für ihn – aufgrund seiner Stellung als Nutzer und nicht als Entwickler der KI – nicht erkennbar waren. Allerdings können Nutzer von KI sich wohl in der Regel nicht darauf berufen, dass sie Funktionen der KI nicht kannten bzw. abschätzen konnten und sie dennoch eingesetzt haben. Viele Fragen des Haftungsregimes sind aktuell umstritten. Es ist daher nicht ausgeschlossen, dass insbesondere ein ungeprüftes Übernehmen von durch KIs wie ChatGPT generierten Inhalten eine eigene Sorgfaltspflichtverletzung seitens des Nutzers darstellt und dass ein Urheber den Nutzer für Rechtsverletzungen durch den Einsatz einer KI verantwortlich macht.

Im Falle von ChatGPT und Dall E wäre auch ein Rückgriff des Nutzers auf OpenAI schwierig. Nach den Nutzungsbedingungen haftet das Unternehmen OpenAI nicht für etwaige Urheberrechtsverletzungen, die aus einer Verwendung des ChatGPT resultieren. Vielmehr verweist OpenAI den Nutzer auf seine eigene Verantwortung sicherzustellen, dass die Inhalte, die ChatGPT liefert, angemessen genutzt werden und dass der Nutzer ggf. die erforderlichen Rechte und Genehmigungen besitzt. Eine davon zu trennende Frage ist, ob der Entwickler oder Anbieter der KI selbst (auch) gegenüber dem Urheber des verletzten Werkes haftet.

---

[33] BGH NJW 2003, 3633, 3635 – Gies-Adler; BGH NJW 1971, 2169 – Disney-Parodie.

[34] EuGH GRUR 2019, 929, 931 - Metall auf Metall III.

[35] Vgl. hierzu Erwägungsgrund 31 der Richtlinie 2001/29/EG.

Da für den Nutzer einer KI nicht ersichtlich ist, mit welchen Inhalten eine KI trainiert wurde und dementsprechend unklar ist, ob eventuell Urheberrechte an den verwendeten Inhalten verletzt werden, ist große Sorgfalt geboten. Wenn Output ohne manuelle Prüfung übernommen wird, besteht die Gefahr, dass die Übernahme solcher Inhalte als fahrlässiges, wenn nicht sogar als grob fahrlässiges Verhalten gewertet werden wird. Dafür hätte der Nutzer als Täter der Urheberrechtsverletzung einzustehen. Die Folgen einer Urheberrechtsverletzung sind weitreichend: so bestehen nicht nur – verschuldensunabhängige – Unterlassungsansprüche des Urhebers, sondern darüber hinaus auch Schadensersatzansprüche und ggf. auch Rückrufansprüche. Zu denken wäre beispielsweise an die Konstellation, dass KI-generierte Marken oder Texte auf Produktverpackungen verwendet werden, was schnell zu beträchtlichen Kosten auf Seiten des Verletzers führen kann. Hier sollte das individuelle Risikoprofil geklärt werden.

Schließlich sei abschließend darauf hingewiesen, dass die Verwendung von KI-generiertem Output auch weitere rechtliche Fragen aufwerfen wird. So erlangte beispielsweise kürzlich der KI-generierte Song „Heart on My Sleeve" im Stil der Musiker Drake und The Weeknd besondere Aufmerksamkeit.[36] Dabei wurden die Stimmen der Künstler verwendet, die Musik war – bis auf wenige Takte – KI-generiert. Da es keinen urheberrechtlichen Schutz für einen bestimmten Stil gibt, kommt in derartigen Fällen wohl am ehesten ein Schutz über das allgemeine Persönlichkeitsrecht in Betracht (siehe 2.3.5).

2.3.2 Verletzung von Patenten

Eine Patentverletzung käme dann in Betracht, wenn der mittels KI-generierte Output und die hiernach hergestellten Produkte oder angewendeten Verfahren einen Eingriff in das Patent eines Patentinhabers darstellen. Theoretisch ist dies möglich. Dem verletzten Patentinhaber stünden dann Ansprüche auf Unterlassung künftiger Rechtsverletzungen zu, § 139 Abs. 1 PatG.

Weiter kann der Patentinhaber – bei vorsätzlicher oder fahrlässiger Handlung – den Ersatz aller durch die Benutzung des geschützten Patentgegenstands eingetretenen und noch eintretenden Schäden verlangen, § 139 Abs. 2 PatG. Schließlich kann vom Verletzer der Rückruf der geschützten Erzeugnisse oder deren endgültige Entfernung aus den Vertriebswegen und die Vernichtung der im Eigentum oder im Besitz des Verletzers befindlichen geschützten Erzeugnisse verlangt werden, § 140a PatG.

2.3.3 Verletzung von Markenrechten

Wie eingangs erläutert, kann der von einer Künstlichen Intelligenz geschaffene Output in Zeichen münden, die sodann als Marke verwendet werden können. Insoweit gilt es für den Nutzer eines KI-generierten Zeichens zu berücksichtigen, dass er die geltenden Grundsätze des Markenschutzes zu beachten hat. Sofern ein mittels

---

[36] https://www.bonedo.de/artikel/15-millionen-klicks-computergenerierter-rap-song-geht-viral/.

KI-erzeugtes Zeichen einem prioritätsälteren Zeichen verwechslungsfähig ähnlich ist und für ähnliche Waren oder Dienstleistungen verwendet wird, haftet der Nutzer des mittels KI-erzeugten Zeichens unter Umständen wegen Markenrechtsverletzung auf Unterlassung und bei schuldhaften Verhalten darüber hinaus auf Schadensersatz, vgl. § 14 Abs. 2 Nr. 2, Abs. 5 und 6 MarkenG bzw. Art. 9 Abs. 2 b) UMV. Bei der Nutzung eines KI-generierten Zeichens, welches einer bekannten Marke verwechslungsfähig ähnlich ist, gilt dies darüber hinaus sogar dann, wenn es sich um unähnliche Waren oder Dienstleistungen handelt, § 14 Abs. 2 Nr. 3 MarkenG bzw. Art. 9 Abs. 2 c) UMV.

Die Folgen einer Markenrechtsverletzung sind weitreichend. So bestehen nicht nur Unterlassungsansprüche. Auch haftet der Verletzer auf Schadensersatz sowie unter Umständen auf Rückruf und Vernichtung der markenrechtsverletzenden Produkte. Dies kann nicht nur weitreichende finanzielle Folgen nach sich ziehen, auch der Ruf des „Markenrechtsverletzers" kann hierdurch in Mitleidenschaft gezogen werden.

2.3.4 Verletzung von Designs

Im Hinblick auf Designs gilt im Wesentlichen das zu Urheberrechten und Marken Gesagte. Es ist denkbar, dass der KI-generierte Output in einem designfähigen Muster oder Modell mündet. Im Hinblick auf die Verwendung eines solchen Designs ist der Nutzer verantwortlich sicherzustellen, dass er keine Designrechte verletzt, andernfalls drohen Unterlassungs- und Schadensersatzansprüche.

2.3.5 Verletzung von Persönlichkeitsrechten

Bislang wenig Beachtung erfuhr zunächst die Frage nach einer Verletzung von allgemeinen Persönlichkeitsrechten durch KI-generierte Inhalte. Dies dürfte sich nun ändern, seit im April 2023 die Veröffentlichung des ersten KI-generierten Songs großes Aufsehen erweckte: Der Song „Heart on my Sleeve" ging innerhalb eines Wochenendes viral und wurde mehr als 15 Millionen Mal angesehen bzw. heruntergeladen. Dabei handelte es sich um einen Song, der ausschließlich mithilfe einer KI-generiert wurde, indem die Stimmen des bekannten kanadischen Künstlerduos Drake und The Weeknd verwendet und mit einem KI-generierten Song zu einem ganz neuen Song vermischt wurden. Aufgrund eines 1:1 übernommenen kurzen Intros konnte der Song durch die Universal Music Group als rechtsverletzend gemeldet werden und wurde von den Plattformen wie Spotify und Apple Music entfernt.[37]

Greift das Urheberrecht nicht ein, dürfte aber das allgemeine Persönlichkeitsrecht bzw. auch das Kunsturhebergesetz zum Tragen kommen. Ob es sich hierbei um eine Rechtsverletzung handelt, bestimmt sich u.a. nach der „Intensität" des Eingriffs und der berührten „Sphäre" (Sozialsphäre, Privatsphäre oder Intimsphäre) auf Seiten der betroffenen Person. Dem Verletzten stehen in der Folge verschiedene zivilrechtliche Ansprüche, etwa auf Unterlassung oder bei schuldhaftem Handeln auf Schadensersatz, zu. In besonders gravierenden Fällen droht eine strafrechtliche Verfolgung.

---

[37] https://en.wikipedia.org/wiki/Heart_on_My_Sleeve_(ghostwriter977_song).

3. Künstliche Intelligenz und Recht der Daten

Künstliche Intelligenz benötigt Daten. Sie nutzt Daten, um trainiert zu werden, sie generiert Daten, um Arbeitsergebnisse zu produzieren, und sie verarbeitet Daten, um weiter zu lernen und intelligenter zu werden. Bei diesen Daten kann es sich um personenbezogene oder nicht-personenbezogene Daten handeln. Sind es personenbezogene Daten, auf die eine KI zugreift und die von ihr verarbeitet werden, sind die Vorgaben des Datenschutzrechts zu beachten. Unbeschadet dessen stellt sich die Frage, wem die Daten gehören, die in einer KI vorhanden sind bzw. von ihr generiert werden.

3.1 Der Schutz von personenbezogenen Daten

3.1.1 Datenschutz-Grundverordnung und Bundesdatenschutzgesetz

Wenn eine Künstliche Intelligenz Daten erhebt und verarbeitet, welche die Identifizierung einer natürlichen Person zulassen, unterfallen diese Verarbeitungsprozesse der EU Datenschutz-Grundverordnung („DSGVO"), die in Deutschland von dem Bundesdatenschutzgesetz („BDSG") und den Landesdatenschutzgesetzen ergänzt wird. Insbesondere bei der Informationsaufnahme, etwa der Erfassung der Umgebung mit einem optischen Sensor, können derartige Daten anfallen. Die Erbringung von personalisierten Leistungen setzt die Identifizierung von natürlichen Personen gegebenenfalls sogar voraus. Der Hersteller, Betreiber oder (ggf.) Eigentümer der Künstlichen Intelligenz ist dann für die Einhaltung dieser Datenschutzgesetze verantwortlich.

Allerdings stehen wesentliche Prinzipien der DSGVO, etwa der Grundsatz der Datenminimierung oder der Speicherbegrenzung (Art. 5 Abs. 1 lit. c) und e) DSGVO), KI-Systemen entgegen, die auf die Verarbeitung möglichst umfangreicher Datensätze angewiesen sind. Für die zulässige Entwicklung und den rechtskonformen Betrieb derartiger KI-Systeme wird es entscheidend darauf ankommen, Prozessabläufe so zu gestalten, dass Daten wo immer möglich nur in anonymisierter Form erhoben und verarbeitet werden und die Zusammenführung solcher Datensätze verhindert wird, die Rückschlüsse auf natürliche Personen zulassen würden. Nur auf diese Weise unterfällt die Künstliche Intelligenz nicht dem Anwendungsbereich der DSGVO und des BDSG. Nach unserer Einschätzung wird es bei der überwiegenden Anzahl der KI-Systeme aber nicht möglich sein, alle Verarbeitungsprozesse vollumfassend zu anonymisieren.

3.1.2 Zulässigkeit der Datenverarbeitung

Die DSGVO untersagt das Erheben und Verarbeiten von personenbezogenen Daten, sofern diese Erhebung bzw. Verarbeitung nicht durch Art. 6 DSGVO gerechtfertigt ist (sog. „Verbot mit Erlaubnisvorbehalt"). Praktisch besonders wichtig ist die Verarbeitung auf Basis einer Einwilligung des Betroffenen, zur Erfüllung eines Vertrages mit dem Betroffenen oder zur Wahrung berechtigter Interessen.

Eine im Bereich der Künstlichen Intelligenz praktisch besonders wichtige gesetzliche Rechtsgrundlage sieht die DSGVO für Datenverarbeitungen vor, die zur Erfüllung eines Vertrags mit dem Betroffenen erforderlich sind, Art. 6 Abs. 1 S. 1 lit. b) DSGVO. Schließen etwa zwei Parteien einen Vertrag[38] über die Erbringung einer KI-spezifischen Dienstleistung oder sind (lediglich) Nebenleistungs- oder Schutzpflichten aus einem Vertrag mithilfe von KI-Systemen zu erbringen, darf die entsprechende Künstliche Intelligenz die hierfür erforderliche Verarbeitung von personenbezogenen Daten des Betroffenen auch durchführen, ohne dass zusätzlich eine Einwilligung eingeholt werden müsste. Wichtig ist dabei, dass der Vertrag mit dem Betroffenen selbst geschlossen wird, weil nur dann von einer eigenen Willensentscheidung des Betroffenen ausgegangen werden kann, die auch die Verarbeitung seiner Daten umfasst und legitimiert.

Wird kein Vertrag geschlossen, ist eine Datenverarbeitung jedenfalls zulässig, wenn die betroffene Person in diese einwilligt, Art. 6 Abs. 1 S. 1 lit. a) i.V.m. Art. 7 DSGVO. Hierfür ist die betroffene Person zunächst umfassend über die konkreten Umstände der Datenverarbeitung zu informieren. Teils komplexe Datenverarbeitungsprozesse müssen verständlich dargestellt werden. Bereits das kann im Bereich Künstlicher Intelligenz schwierig sein, weil gerade bei selbstlernenden Systemen unter Umständen nicht genau beschrieben werden kann, welche Daten in welchem Umfang aktuell oder zukünftig von der Künstlichen Intelligenz verarbeitet werden. Damit eine Einwilligung wirksam ist, muss sie zudem freiwillig erteilt werden. Hierfür muss die betroffene Person eine echte Wahl haben, die Datenverarbeitung abzulehnen, ohne dass ihr deswegen Nachteile entstehen. Dieser Freiwilligkeit kann ein „faktischer" Zwang entgegenstehen, wenn der (gesamte) Betrieb einer Künstlichen Intelligenz von der Einwilligung in einzelne, technisch nicht erforderliche Datenverarbeitungen abhängig gemacht wird, die beispielsweise nur erwünschte, aber nicht notwendige Zusatzfunktionen ermöglichen und auf Datenverarbeitungen basieren, die für den Betrieb der Künstlichen Intelligenz an sich nicht notwendig sind. Wird in einem solchen Fall der Betrieb der Künstlichen Intelligenz davon abhängig gemacht, dass eine Einwilligung auch für die darüber hinausgehenden Datenverarbeitungen erteilt wird, wird diese Einwilligung im Zweifel nicht freiwillig erteilt und wäre deshalb unwirksam (sog. Kopplungsverbot, Art. 7 Abs. 4 DSGVO). Daher kann es etwa für multifunktionale Roboter notwendig sein, bestimmte Kernfunktionen zu definieren, für deren Erbringung die erforderlichen Verarbeitungsprozesse (etwa im Rahmen einer Vertragserfüllung) stets zulässig sind, und darüber hinausgehende Funktionen optional auszugestalten und von der jeweiligen Einwilligung des Nutzers abhängig zu machen. Für Kinder dürften Einwilligungen ohnehin nicht das erste Mittel der Wahl sein. Kinder unter 16 Jahren können in Deutschland nicht selbst wirksam einwilligen, Art. 8 Abs. 1 DSGVO.

Wird ein KI- oder Robotersystem im öffentlichen Raum eingesetzt, wie beispielsweise ein intelligentes Überwachungssystem öffentlicher Plätze, das durch Sensoren aktiviert wird, ist es in tatsächlicher Hinsicht nicht möglich, Einwilligungen von allen Personen einzuholen, die von den Sensoren erfasst werden. Häufig hängt die Zulässigkeit der Datenverarbeitung in solchen oder ähnlichen Fällen von dem Ergebnis einer Interessenabwägung ab, in der die berechtigten Interessen des Verantwortlichen

---

[38] Auf den einzelnen Vertragstyp kommt es hierbei nicht an. Roboterspezifische Dienstleistungen könnten zukünftig insbesondere in den Bereichen des Kauf-, Dienst-, Werk- und Mietvertragsrechts üblich werden, etwa im Rahmen von Beförderungs-, Behandlungs- oder Nutzungsverträgen.

oder eines Dritten (an dem Betrieb des Roboters zu bestimmten Zwecken) den Interessen der betroffenen Personen (an dem Schutz ihrer Privatsphäre) gegenübergestellt werden, Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Entscheidend kann es darauf ankommen, in welchem Kontext die Datenverarbeitung stattfindet und welche Erwartungshaltung die betroffenen Personen damit verbinden.[39] Der vermehrte Einsatz von KI- und Robotersystemen mit spezifischen Aufgabenzuweisungen im öffentlichen Raum und die fortschreitende Sensibilisierung der Öffentlichkeit für deren Funktionsweise könnten langfristig dazu führen, dass diese Interessenabwägung zunehmend zugunsten der Betreiber von KI-Systemen ausfällt, insbesondere wenn sich die vernünftige Erwartungshaltung der Bevölkerung dahingehend ändert, dass mit dem Einsatz derartiger Systeme zu rechnen ist.

Eine weitere Rechtsgrundlage erlaubt Datenverarbeitungen, wenn diese für den Schutz von lebenswichtigen Interessen erforderlich sind, Art. 6 Abs. 1 S. 1 lit. d) DSGVO. Dies kann für Robotersysteme aus den Bereichen des Brand- und Katastrophenschutzes oder der Kampfmittelräumung relevant werden.

In einem Betrieb ist der Einsatz von KI oder KI-gestützten Robotersystemen zulässig, soweit das System für die Durchführung des Arbeitsverhältnisses erforderlich ist, § 26 Abs. 1 S. 1 BDSG. Auch insoweit greift somit der Gedanke der Vertragserfüllung, Art. 6 Abs. 1 S. 1 lit. b) DSGVO. In Deutschland ist der Einsatz von Künstlicher Intelligenz im Arbeitsleben bereits alltägliche Realität. Hierzu können „intelligente" Werkzeuge, etwa Datenbrillen oder vernetzte Handschuhe, und der Einsatz von Industrierobotern gehören,[40] wenn dadurch der Gesundheits- und Gefahrenschutz für die Beschäftigten deutlich verbessert wird. Weit verbreitet ist bereits die Unterstützung bei der Bewerberauswahl im Bewerbungsverfahren durch KI-Systeme. Vermehrt werden intelligente Systeme aber auch für das Tracking von Arbeitsleistungen oder Anwesenheitszeiten der Beschäftigten genutzt. In Lagerhäusern und Vertriebszentren etwa werden von den Beschäftigten Wearables getragen, um Logistikprozesse zu steuern und auf Schwankungen in der Produktivität zu reagieren. Darüber hinaus können auch minutengenau Qualitäts- und Quantitätsleistungsdaten der Beschäftigten erhoben und analysiert werden.[41] Derartige Überwachungs- und Kontrollhandlungen bzgl. Mitarbeitern können aus betrieblichen Gründen erforderlich sein, müssen aber stets gesondert auf ihre Rechtmäßigkeit geprüft werden und bedürfen einer Abwägung im Einzelfall.

Sensible Daten, wie etwa Gesundheitsdaten, biometrische Daten, Informationen zu Gewerkschaftszugehörigkeit, politischen Meinungen oder der sexuellen Orientierung der betroffenen Person, werden von der DSGVO als sog. „Besondere Kategorien von personenbezogenen Daten" wesentlich strenger geschützt als „normale" Daten. Die Verarbeitung dieser Daten ist nur zulässig, wenn eine spezielle Rechtsgrundlage

---

[39] Vgl. Erwägungsgrund 47 DSGVO.

[40] Beispiele nach Gola/Pötters in: Gola/Heckmann, Bundesdatenschutzgesetz, 3. Auflage 2022, § 26 Rn. 164.

[41] Mit Urteil vom 09.02.2023 hat das VG Hannover (10 A 6199/20) entschieden, dass Amazon berechtigt ist, Beschäftigte in bestimmten Arbeitsbereichen mit Handscanner auszustatten, mittels derer bestimmte Arbeitsschritte erfasst werden und auch individuelle Quantitätsleistungs- und Qualitätsleistungsprofile erstellt werden können. Das Gericht wandte sich damit gegen die durch die Landesbeauftragte für Datenschutz in Niedersachen ausgesprochene Untersagung der Datenerfassung.

vorliegt, das heißt ein Ausnahmetatbestand des Art. 9 Abs. 2 oder 3 DSGVO erfüllt ist. Dies kann den Einsatz von Künstlicher Intelligenz in bestimmten Bereichen erschweren, etwa für medizinische, physiologische oder therapeutische Zwecke, in der Pflege oder dem Gebäudeschutz. Gleichwohl kann eine Verarbeitung auch hier zulässig sein, wenn die betroffene Person ausdrücklich einwilligt oder wenn der Einsatz für besonders hochrangige Schutzgüter, etwa für die Gesundheitsvorsorge oder die medizinische Diagnostik, erforderlich ist.

3.1.3 Pflichten des Verantwortlichen

Wer über den Zweck und die Mittel der Datenverarbeitung entscheidet, ist für die Einhaltung des Datenschutzes „verantwortlich", Art. 4 Nr. 7 DSGVO. Bei KI-Systemen kann die Verantwortlichkeit etwa bei dem Eigentümer, Betreiber, Hersteller und/oder Entwickler[42] liegen, je nachdem, wie die Verarbeitungsprozesse im Einzelnen ausgestaltet sind. Der Verantwortliche hat für die Einhaltung der Datenschutzgesetze einzustehen und muss die Rechtmäßigkeit der unter seiner Verantwortung durchgeführten Datenverarbeitungen stets nachweisen können, Art. 5 Abs. 2 DSGVO. Des Weiteren hat er hinreichende Informationen zu den Verarbeitungsprozessen bereitzustellen und Rechte von betroffenen Personen zu befriedigen, Art. 12 ff. DSGVO. Es besteht die Pflicht, ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen, das den Aufsichtsbehörden auf Anfrage zur Verfügung zu stellen ist, Art. 30 Abs. 1 DSGVO, und in vielen Fällen ist ein Datenschutzbeauftragter zu bestellen, Art. 37 DSGVO i.V.m. § 38 BDSG.

Vor der erstmaligen Inbetriebnahme einer Künstlichen Intelligenz wird zudem häufig eine Datenschutz-Folgenabschätzung durchzuführen sein, um die Auswirkungen der Datenverarbeitung auf die Privatsphäre der betroffenen Personen zu bewerten und etwaige Risiken der Datenverarbeitung im Voraus zu erkennen und zu reduzieren, Art. 35 Abs. 1 DSGVO. So nehmen etwa KI-gestützte Robotersysteme umfangreiche Informationen aus ihrer Umgebung auf, führen diese mit weiteren Daten zusammen und werten diese Datensätze im Rahmen einer Entscheidungsfindung aus. Derart komplexe Verarbeitungen bergen datenschutzrechtlich mitunter ein hohes Überwachungsrisiko, insbesondere wenn solche Robotersysteme im öffentlichen Raum eingesetzt werden oder mit besonders sensiblen Daten, etwa Gesundheitsdaten, in Berührung kommen.

Schließlich ist der Verantwortliche verpflichtet, etwaige Verletzungen des Datenschutzes unverzüglich an die zuständige Aufsichtsbehörde zu melden, es sei denn, die Verletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen, Art. 33 DSGVO. Ein solches Risiko wird regelmäßig vorliegen, wenn Dritte unberechtigten Zugriff auf die Künstliche Intelligenz und die in ihr liegenden umfangreichen Daten bestände erlangen. Liegt ein hohes Risiko vor, sind zudem die betroffenen Personen zu informieren, Art. 34 DSGVO.

---

[42] So auch Hartwig/Martin/Schumacher, Rechtliche Rahmenbedingungen für den Einsatz von autonomen Robotern in Assistenzfunktionen – Studie des Instituts für Klimaschutz, Energie und Mobilität e.V., Stand Januar 2020.

In Deutschland bestehen mehrere voneinander unabhängige Aufsichtsbehörden. Die Bundesländer unterhalten eigene, unabhängige Aufsichtsbehörden, die neben den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der insbesondere die Aufsicht über Bundesbehörden ausübt, treten. Die für einen Verstoß zuständige Behörde richtet sich primär nach dem Sitz des Verantwortlichen.

3.1.4 Auftragsverarbeitung

Verarbeiten externe Dienstleister oder andere Dritte personenbezogene Daten im Auftrag und auf Weisung des Verantwortlichen, liegt eine Auftragsverarbeitung nach Art. 28 DSGVO vor. Der als Auftragsverarbeiter tätige Dritte wird von Gesetzes wegen als Teil des Verantwortlichen angesehen, nicht mehr als Außenstehender, sodass die Übermittlung von oder der Zugriff auf personenbezogene Daten keiner weiteren gesetzlichen Erlaubnis oder Einwilligung mehr bedarf. Erforderlich ist aber der Abschluss eines gesonderten Vertrags über die Auftragsverarbeitung, der die Anforderungen des Art. 28 Abs. 3 DSGVO vollständig abbilden muss.

3.1.5 Datenübermittlung in Drittländer

Eine Datenübermittlung in Staaten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums (sog. Drittländer) ist zulässig, wenn die EU-Kommission in einem sog. „Angemessenheitsbeschluss" festgestellt hat, dass das Drittland über ein ausreichend hohes Schutzniveau verfügt, Art. 45 DSGVO. Für die USA bestand bis Mitte 2020 ein solcher Angemessenheitsbeschluss insoweit, als sich der in den USA befindliche Empfänger der Daten dem EU-US-Datenschutzschild („Privacy Shield") unterworfen hatte. Der Europäische Gerichtshof (EuGH) hat den Privacy Shield mit Urteil vom 16. Juli 2020 (Rechtssache C-311/18 – „Schrems II") jedoch für unwirksam erklärt. Der EuGH bewertete das Datenschutzniveau in den USA aufgrund verschiedener nachrichtendienstlicher Erhebungsbefugnisse sowie fehlender Rechtsschutzmöglichkeiten für die davon betroffenen Personen als nicht ausreichend. Das Urteil hatte auch für die Übermittlung von Daten in andere Staaten außerhalb des Europäischen Wirtschaftsraums, für die kein Angemessenheitsbeschluss besteht, weitreichende Konsequenzen, weil es die Anforderungen an Datenübermittlungen in Drittländer insgesamt verschärfte.

Im März 2022 haben sich die EU-Kommission und die USA mit dem „EU-U.S. Data Privacy Framework" grundsätzlich auf einen Nachfolger für den Privacy Shield geeinigt.[43] Um die Bedenken des EuGH aus der Schrems II-Entscheidung auszuräumen, wurden in dem Entwurf eines entsprechenden Agreements die Zugriffsmöglichkeiten der US-amerikanischen Geheimdienste einschränkt, neue Beschwerdemöglichkeiten für EU- Bürger geschaffen und strengere Verpflichtungen der US-Unternehmen für aus der EU übermittelte Daten etabliert. Nachdem der US-Präsident im Oktober 2022 eine

[43] Die EU-Kommission hat am 25.03.2022 in einem Factsheet die Grundprinzipien des Datenschutzabkommens festgelegt, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/ip_22_2087.

Executive Order (Durchführungsverordnung) unterzeichnet hat,[44] hat die EU-Kommission im Dezember 2022 den Entwurf des Angemessenheitsbeschlusses vorgelegt, welcher noch das Annahmeverfahren passieren muss.[45] Mit einem Inkrafttreten des EU-U.S. Data Privacy Framework wird bis Herbst 2023 gerechnet.

Liegt ein Angemessenheitsbeschluss nicht vor, wie aktuell im Falle der USA, ist eine Datenübermittlung durch die beteiligten Parteien mithilfe von sog. „geeigneten Garantien" abzusichern, Art. 46 DSGVO. Die geeigneten Garantien sollen die Einhaltung des angemessenen Datenschutzniveaus im Drittland sicherstellen. Hierbei wird zumeist auf die Standardvertragsklauseln der Europäischen Kommission oder, für konzerninterne Datenübermittlungen, auf verbindliche interne Datenschutzvorschriften der eigenen Unternehmensgruppe (sog. Binding Corporate Rules) zurückgegriffen.

Es bestehen nach der Rechtsprechung des EuGH in Sachen Schrems II aber erhebliche Zweifel daran, ob diese Garantien in vielen Drittstaaten tatsächlich ein angemessenes Datenschutzniveau herstellen können. Offen ist etwa die Frage, wie sich der Datenempfänger gegen hoheitliche Maßnahmen des Drittlandes effektiv erwehren soll. Vertragliche Verpflichtungen können die nachrichtendienstlichen Erhebungsbefugnisse eines Drittlandes jedenfalls nicht außer Kraft setzen.

Um den Anforderungen des EuGH aus dem Schrems II Urteil nachzukommen, hat die EU-Kommission im Juni 2021 neue Standardvertragsklauseln veröffentlicht. Neben dem Abschluss dieser Klauseln muss der Datenexporteur unter Einbeziehung des Datenimporteurs die Rechtslage und -praxis des Drittlands prüfen und ggf. zusätzliche Schutzmaßnahmen ergreifen bzw., wenn dies nicht gelingt, von der Übermittlung Abstand nehmen. Erforderlich ist danach eine umfassende Risikoeinschätzung für die Datenverarbeitung im betreffenden Drittland („Transfer Impact Assessment"). Ohne diese Risikoeinschätzung und etwaige zusätzliche Maßnahmen können die Standardvertragsklauseln nicht als geeignete Garantie für eine Datenübermittlung in Drittländer herangezogen werden.

All dies gilt es zu beachten, wenn KI-Systeme in einem Drittland, wie den USA, betrieben werden, oder wenn die Daten aus Kosten-, Effizienz- oder Redundanzgründen (auch) dort verarbeitet werden.

3.1.6 Automatisierte Einzelfallentscheidungen

Für die Entscheidungsfindung einer Künstlichen Intelligenz kann das Verbot automatisierter Entscheidungen besondere Relevanz entfalten, Art. 22 DSGVO. Demnach hat eine betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

---

[44] Enhancing Safeguards for United States Signals Intelligence Activities", abrufbar unter https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/.

[45] https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7631.

Der Mensch soll nicht zum bloßen Objekt einer computergesteuerten Entscheidung herabgewürdigt werden, die allein aufgrund einer automatisierten Bewertung von Persönlichkeitsmerkmalen und ohne menschliche Einflussnahme ergeht.[46]

Automatisierte Entscheidungen im Sinne des Art. 22 DSGVO können bei den verschiedensten Datenverarbeitungen auftreten. Denkbar ist etwa der Einsatz einer KI-Software, welche die Entscheidung eines Facharztes ersetzt (z.B. für die Anpassung einer Medikation oder in der Diagnostik),[47] Entscheidungsbefugnis in einem Gerichts- oder Verwaltungsverfahren innehat,[48] eine automatisierte Bewerberauswahl durchführt oder eine eigenständige Kaufentscheidung bei einem Online-Händler trifft.

Automatisierte Einzelfallentscheidungen sind nur in den gesetzlich vorgesehenen Ausnahmefällen des Art. 22 Abs. 2 DSGVO zulässig, d.h. wenn die automatisierte Entscheidung für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist oder auf Grundlage einer gesonderten Rechtsvorschrift bzw. einer Einwilligung der betroffenen Person erfolgt.

Für den Fall, dass eine automatisierte Entscheidungsfindung erfolgt, muss der Verantwortliche hierüber informieren. Dabei muss nicht nur die Tatsache der automatisierten Entscheidungsfindung an sich offengelegt werden, sondern es müssen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der zugrunde liegenden Datenverarbeitung für die betroffene Person bereitgestellt werden, Art. 13 Abs. 2 lit. f), 14 Abs. 2 lit. g) DSGVO. Das bedeutet, dass die Datenschutzerklärung Angaben nicht nur über den Einsatz der Künstlichen Intelligenz zum Zwecke der automatisierten Entscheidungsfindung enthalten muss, sondern es müssen auch nachvollziehbare Erläuterungen über die wesentlichen Entscheidungsparameter, die von der Künstlichen Intelligenz entwickelt und angewendet werden, offengelegt werden, damit die betroffenen Personen die Tragweite der Verarbeitung ihrer personenbezogenen Daten erfahren und bewerten können. Dies ist indes nicht gleichbedeutend mit einer vollständigen Offenlegung der Künstlichen Intelligenz selbst, also ihrer Programmierung, des Quellcodes, der ergänzenden Dokumentation etc., die weiterhin Geschäftsgeheimnis und geschütztes geistiges Eigentum ihres Schöpfers sein können.

3.1.7 Exkurs: Datenschutz bei ChatGPT

Die praktischen Schwierigkeiten bei der Umsetzung der vorstehend erläuterten datenschutzrechtlichen Anforderungen zeigen sich insbesondere am Beispiel von ChatGPT. Die Veröffentlichung von ChatGPT des US-Anbieters OpenAI im November 2022 gilt als Meilenstein im Bereich generativer KI, führte aber auch zu divergierendem

---

[46] So auch *Buchner*: in Kühling/Buchner, DSGVO/BDSG, 3. Auflage 2020, Art. 22 DSGVO, Rn. 1.

[47] In den USA hat die Food and Drug Administration (FDA) bereits ein Medizinprodukt auf Basis einer KI-Software in der Schlaganfalldiagnostik zugelassen, vgl. hierzu Dettling in Künstliche Intelligenz und digitale Unterstützung ärztlicher Entscheidungen in Diagnostik und Therapie, PharmR 2019, 633.

[48] Vgl. Enders in Einsatz Künstlicher Intelligenz bei juristischer Entscheidungsfindung, JA 2018, 721.

Medien-Echo. Angepriesen werden einerseits die erstaunlichen Fähigkeiten der Software. Andererseits wird vor den drohenden Gefahren der KI, etwa durch den Verlust von Arbeitsplätzen, gewarnt.

Jedes sechste Unternehmen (17 Prozent) in Deutschland plant den Einsatz von ChatGPT oder ähnlicher KI-Anwendungen, weitere 23 Prozent haben keine konkreten Planungen, können sich die Nutzung aber vorstellen.[49] Laut verschiedenen Berichten hat ChatGPT derzeit geschätzt 616 Millionen Website-Besucher im Monat.[50] Erst kürzlich haben Wissenschaftler und Prominente aus der TechBranche eine sechsmonatige Pause beim Trainieren von KI-Systemen gefordert, die leistungsfähiger sind als das aktuell veröffentlichte Modell GPT4. „Leistungsstarke KI-Systeme sollten erst dann entwickelt werden, wenn wir sicher sind, dass ihre Auswirkungen positiv und ihre Risiken überschaubar sein werden", heißt es in dem offenen Brief, an dem bekannte Persönlichkeiten wie Elon Musk und AppleMitgründer Steve Wozniak, mitgewirkt haben.[51]

ChatGPT ist ein Sprachmodell und wird durch Benutzereingaben und frei verfügbare Informationen im Internet trainiert, um im Rahmen eines Chatbots Antworten zu liefern. Eine Vielzahl von Einsatzmöglichkeiten ist dabei denkbar und auch schon möglich, z.B. das Erstellen von Texten oder Grafiken, das Zusammenfassen und Redigieren von Texten, die Erstellung von Gesprächsprotokollen aus Videokonferenzen, die Beantwortung juristischer Fragen oder das Schreiben von Gedichten. In einer zahlungspflichtigen Version können Unternehmen die Software über eine API-Programmierschnittstelle in die eigene IT-Umgebung integrieren und als Chatbot im Kundenbereich nutzen. Die Qualität und die Richtigkeit der von der KI ausgeworfenen Ergebnissen schwanken derzeit allerdings noch stark. Bei einer im Selbstversuch durchgeführten Recherche zu Rechtsprechung und aktuellen Urteilen spuckte die Software teils abenteuerliche Antworten aus und nannte z.B. nicht existente oder falsche Urteile.

Entsprechend haben auch verschiedene Datenschutzbehörden ChatGPT einer näheren Betrachtung unterzogen. In den USA wurde die Federal Trade Commission im März 2023 durch eine gemeinnützige Organisation, das Center for AI and Digital Policy (CAIDP), aufgefordert, in einem Verfahren gegen OpenAI eine Untersuchung einzuleiten und weitere Modelle der Software vorerst zu verhindern. Der kanadische Datenschutzbeauftragte hat im April 2023 aufgrund einer Beschwerde über die Erhebung, Verwendung und Offenlegung personenbezogener Daten ohne Zustimmung der betroffenen Person eine Untersuchung gegen OpenAI eingeleitet. Auch die

---

[49] https://www.bitkom.org/Presse/Presseinformation/ChatGPT-Jedes-sechste-Unternehmen-plant-KI-Einsatz-Textgenerierung.

[50] https://www.tooltester.com/de/blog/chatgpt-statistiken/.

[51] https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

[52] Pressebericht abrufbar unter https://edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en.

[53] ZD-Aktuell 2023, 01168 mit weiteren Nachweisen.

Datenschutzbehörden in Frankreich und Spanien teilten im April 2023 mit, mehreren Beschwerden nachzugehen und Untersuchungen einzuleiten. Ebenfalls im April hat der Europäische Datenschutzausschuss (EDSA) beschlossen, wegen der Datenschutzbedenken gegenüber ChatGPT eine Taskforce einzurichten.[52] In Deutschland haben daraufhin mehrere Datenschutzbehörden (u.a. von Hessen, Baden-Württemberg und Rheinland-Pfalz) OpenAI einen umfangreichen Fragenkatalog zugeschickt, in welchem sich OpenAI u.a. zu Details der Datenverarbeitung und den Rechtsgrundlagen äußern soll.[53] Aufsehen erregte aber zuvor schon ein Verfahren der italienischen Datenschutzbehörde Ende März 2023 gegen OpenAI. Aufgrund datenschutzrechtlicher Bedenken wurde der Zugang zu ChatGPT landesweit vorübergehend gesperrt.[54] Erst nach der Erfüllung mehrerer Auflagen der Behörde durch OpenAI wurde der Zugang wieder freigeschaltet.

Problematisch bei der Datenverarbeitung durch die KI-Software ist zunächst das Finden der einschlägigen Rechtsgrundlage nach Art. 6 DSGVO, falls personenbezogene Daten verarbeitet werden. Betroffene können dabei entweder die Nutzer selbst sein, die personenbezogene Daten in die Software eingeben, oder Personen, deren Daten im Rahmen der Recherche oder des Trainings durch ChatGPT gesammelt werden. Die italienische Aufsichtsbehörde bemängelte in dem Verfahren gegen OpenAI, dass keine Rechtsgrundlage für die Erhebung und Verarbeitung personenbezogener Daten zu eigenen Zwecken ersichtlich sei. Schließlich nutzt OpenAI die eingegebenen Daten zum Trainieren des eigenen Algorithmus. Personenbezogene Daten können dabei nach Aussage von ChatGPT nicht selbst erkannt oder aussortiert werden. Dies teilt der Chatbot auf entsprechende Anfrage selbst mit. Auf eine Datenverarbeitung zur Vertragserfüllung (Art. 6 Abs. 1 S. 1 lit. b) DSGVO) dürfe sich das Unternehmen laut der Behörde dabei nicht stützen. Denkbar wären als Rechtsgrundlagen hinsichtlich der Nutzer der KI die Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit a) DSGVO oder die Erforderlichkeit der Datenverarbeitung zur Wahrung der berechtigten Interessen nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO. Für eine informierte Einwilligung wäre zunächst Transparenz bezüglich der Datenverarbeitung erforderlich, welche aktuell jedoch nicht vorliegt. Bei einer Interessenabwägung ist eine Einzelfallabwägung erforderlich. Dabei kommt neben der vernünftigen Erwartungshaltung der Betroffenen vor allem dem Jugendschutz ein besonderes Gewicht zu, wobei moniert wird, dass ChatGPT keine wirksame Altersabfrage vornimmt und auch keinen Jugendschutzfilter verwendet. Beim Training der KI mit personenbezogenen Daten aus dem Internet kommt bezüglich der Betroffenen nur eine Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO als Rechtsgrundlage in Betracht. Ob dabei die Interessen von OpenAI überwiegen, ist fraglich, da die Betroffenen mit Sicherheit nicht mit einer massenhaften Erfassung ihrer Daten durch KI-Systeme rechnen mussten,[55] und natürlich auch insoweit die Frage nach dem Schutz minderjähriger Betroffener unbeantwortet bleibt.

Des Weiteren bemängelte die italienische Datenschutzbehörde, dass die von ChatGPT gelieferten Ergebnisse teilweise unrichtig seien und damit gegen das Prinzip der Datenrichtigkeit gemäß Art. 5 Abs. 1 lit. d) DSGVO verstoßen. Die Behörde vertritt

---

[54] Pressemitteilung der Behörde abrufbar unter https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874751#english.

[55] Buchmann/Panfili: ChatGPT und die DSGVO: Freie Fahrt für freie Bürger?, VuR 2023, 161, 162.

insoweit ein weites und damit strenges Verständnis der Norm, bei welchem auch die Ergebnisse der Software der Datenrichtigkeit entsprechen müssen. Bei einem engen Verständnis würde sich der Grundsatz dagegen nur auf die ursprünglichen Trainingsdaten beziehen. Zweifel bestehen auch hinsichtlich Art. 5 Abs. 1 lit. a) DSGVO, wonach personenbezogene Daten „auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden" müssen. Nachdem die Datenverarbeitungen durch ChatGPT bereits für Datenschutzbehörden und IT-Sicherheitsexperten nicht nachvollziehbar sind, dürften sie erst recht für die betroffenen Personen nicht nachvollziehbar sein.

Selbstverständlich müssen die Betreiber von KI-Systemen die Betroffenen gemäß den Art. 13 und 14 DSGVO ordnungsgemäß informieren. Auch die italienische Aufsichtsbehörde forderte OpenAI auf, die Nutzer entsprechend den Vorgaben von Art. 13 DSGVO ausreichend zu informieren. Daneben müsste OpenAI grundsätzlich auch sämtliche von Datenverarbeitungen betroffene Personen gemäß Art. 14 DSGVO informieren, was schwer vorstellbar ist bzw. praktisch nicht umsetzbar sein dürfte. Einen Ausweg könnte hier Art. 14 Abs. 5 lit. b) DSGVO bieten, wonach keine Informationspflicht besteht, wenn die Erteilung von Informationen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.[56]

Unklar ist daneben auch die rechtliche Situation bezüglich der Verantwortlichkeit von OpenAI. Für die entgeltliche Version stellt OpenAI den Nutzern einen Auftragsverarbeitungsvertrag zur Verfügung, wobei Änderungen nicht akzeptiert werden. Da OpenAI die Daten jedoch auch zu Trainings- und wohl auch zu Werbezwecken verarbeitet, liegt eine Verarbeitung im eigenen Interesse von OpenAI vor. Dies widerspricht einer Auftragsverarbeitung und deutet auf eine zumindest teilweise getrennte oder gar gemeinsame Verantwortlichkeit hin. Ein Vertrag über eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO wird von OpenAI jedoch nicht angeboten.

Zu guter Letzt handelt es sich bei OpenAI um ein US-amerikanisches Unternehmen. Die Daten können daher bei Nutzung von ChatGPT laut Aussage des Chatbots selbst auch an Server in den USA oder anderen Drittländern übertragen werden. Solange für die USA kein Angemessenheitsbeschluss besteht, bestehen die unter Ziffer 3.1.5 dargestellten Risiken. OpenAI hat bislang auch weder ein Transfer Impact Assessment noch die notwendigen Informationen, die nutzenden Unternehmen die Durchführung eines eigenen Transfer Impact Assessments ermöglichen würden, bereitgestellt.

Es zeigt sich, dass die Verwendung von ChatGPT noch mit zahlreichen offenen Fragen und Risiken verbunden ist, die sich zumindest aktuell noch nicht sicher beantworten oder lösen lassen. Die weitere Entwicklung und die Stellungnahmen der Datenschutzbehörden bleiben abzuwarten. Insbesondere von den Entscheidungen der diversen Aufsichtsbehörden sind Impulse zu erwarten, die über den konkreten Fall von ChatGPT hinaus für den gesamten Einsatz von KI und ihr Verhältnis zum Datenschutz von Interesse sind. Bis dahin ist Unternehmen zu raten, den Einsatz von ChatGPT oder ähnlichen Systemen nicht leichtfertig zu veranlassen und eine sorgfältige Risikoabwägung durchzuführen, um Bußgelder oder Einstellungsverfügungen zu vermeiden.

---

[56] Buchmann/Panfili: ChatGPT und die DSGVO: Freie Fahrt für freie Bürger?, VuR 2023, 161, 162.

3.2 Eigentum an Daten

Es stellt sich zudem die Frage, wem die von der Künstlichen Intelligenz gespeicherten Daten „gehören" und wie man sie vor der Nutzung durch andere schützen kann.

Das deutsche Urheberrecht bietet keinen umfassenden Schutz, da unstrukturierte Daten nicht als persönliche geistige Schöpfung betrachtet werden. Auch das sogenannte Datenbankurheberrecht auf der Grundlage von § 4 Abs. 2 UrhG wird in den meisten Fällen keinen Schutz bieten, da auch dieses Recht eine Schöpfung voraussetzt, also eine persönliche geistige Schöpfung, die eine ausreichende Schöpfungshöhe aufweist, was bei Datenbanken, wie sie von Künstlicher Intelligenz genutzt werden, regelmäßig nicht der Fall sein dürfte.

Das sogenannte Datenbankherstellerrecht auf der Grundlage der §§ 87a ff. UrhG kann oftmals Schutz gewähren. Eine „schutzfähige Datenbank" ist definiert als eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch geordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind, wenn deren Beschaffung, Überprüfung oder Darstellung eine nach Art und Umfang wesentliche Investition erfordert, § 87a Abs. 1 UrhG. Dies kann anwendbar sein und damit Schutz für Daten gewähren, die in systematischer oder methodischer Weise erhoben und aufbereitet worden sind. Geschützt ist damit allerdings nur die Datensammlung in ihrer systematischen oder methodischen Form, nicht das einzelne Datum. Ob und wenn ja, in welchem Umfang an diesem ein Eigentumsrecht besteht oder überhaupt bestehen kann, ist eine andere Frage.

Neuen Schwung in die Diskussion um das Dateneigentum hat der im Februar 2022 veröffentlichte Vorschlag der EU-Kommission für den sog. Data Act gebracht.[57] Zwar wird auch dort die Frage nach dem Eigentum an Daten nicht beantwortet. Jedoch will der Gesetzgeber Datenzugang und Datennutzung völlig neu gestalten. Der Data Act unterscheidet zwischen Datennutzern und Dateninhabern. Dateninhabern sollen erhebliche Pflichten auferlegt werden, Zugriff auf Daten zu fairen Bedingungen zu ermöglichen. Noch ist der Data Act Zukunftsmusik. Der Inhalt des Entwurfs beinhaltet jedoch verschiedene Denkanstöße. So könnte die Entwicklung eher weg von alleinigem Dateneigentum und hin zu einem Teilen der Daten gehen, um Daten allgemein nutzbar zu machen.

3.3 Datensicherheit

Datensicherheit ist ein wesentlicher Bestandteil aller Datenschutzbemühungen und muss auch bei der Einführung und Nutzung von KI-Systemen gewährleistet sein. Grundlegende Anforderungen an technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten sind in Art. 32 DSGVO festgelegt. Zu diesen Maßnahmen gehören insbesondere, je nach Art der konkreten Datenverarbeitung und

[57] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0068.

Kritikalität der Daten, Vorkehrungen zur Pseudonymisierung, Verschlüsselung und raschen Wiederherstellung von Daten, zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der verwendeten Systeme sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Sicherheitsmaßnahmen. Die Gewährleistung von Datensicherheit ist somit ein dynamischer Prozess, der stets beobachtet und ggf. angepasst werden muss. Art und Umfang der zu ergreifenden Maßnahmen unterliegen allerdings einer Verhältnismäßigkeitsprüfung, die den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Schwere des Risikos für die Rechte des jeweiligen Betroffenen berücksichtigen muss. Es geht also nicht um die Realisierung des (nur) theoretisch denkbar größtmöglichen Schutzes, sondern vielmehr um die Gewährleistung eines dem jeweiligen Risiko angemessenen Schutzniveaus für die konkret verarbeiteten Daten, Art. 32 Abs. 1 DSGVO.

Weitere Anforderungen an technische Vorkehrungen und organisatorische Maßnahmen, ein schließlich der Meldepflichten bei Störungen, ergeben sich aus der auch in Deutschland umgesetzten EU-Richtlinie zur Netz und Informationssicherheit (NIS-Richtlinie) und dem deutschen IT-Sicherheitsgesetz, insbesondere für Betreiber kritischer Infrastrukturen wie Telekommunikations- oder Energieinfrastrukturbetreiber.[58] Mit der im Januar 2023 in Kraft getretenen NIS 2-Richtlinie hat die EU als Reaktion auf die steigenden Bedrohungen durch Cyberkriminalität die Anforderungen der Unternehmen an den Schutz ihrer Netzwerke und Systeme nochmals erhöht.[59]

Mit dem Erlass der Cybersecurity-Verordnung[60] hat sich die Europäische Union der Aufgabe verschrieben, ein europäisches Zertifizierungssystem für die Sicherheit von IT-Systemen zu etablieren. Die Zertifizierungsschemata sehen unterschiedliche Anforderungsniveaus vor („hoch", „mittel" und „niedrig"), abhängig von dem jeweiligen Verwendungsrisiko, und werden für spezifische IT-Prozesse bzw. Dienste entwickelt.[61] Ziel ist es, eine Harmonisierung von anerkannten Sicherheitsstandards herbeizuführen. Die Zertifizierung bescheinigt einem IT-Produkt, entsprechende Sicherheitsanforderungen zu erfüllen. Die Cybersecurity-Verordnung könnte damit die DSGVO-Prinzipien „Privacy by Default" und „Privacy by Design" (Art. 25 DSGVO) näher ausformen und eine gewisse Rechtssicherheit für die Betreiber von IT-Systemen schaffen. An der Entwicklung und Überwachung des Zertifizierungssystems wird die Agentur der Europäischen Union für Cybersicherheit („ENISA") beteiligt, deren Mandat auch im Übrigen durch die Cybersecurity-Verordnung gestärkt wurde. Für die Ausstellung von Zertifikaten sollen hingegen nationale Behörden bzw. akkreditierte öffentliche Stellen zuständig sein.

---

[58] Die Bundesregierung hat im Dezember 2020 den Entwurf des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT Sicherheitsgesetz 2.0") verabschiedet.

[59] Die EU-Mitgliedsstaaten haben ab Inkrafttreten 21 Monate Zeit, die darin enthaltenen Vorgaben in nationales Recht umzusetzen.

[60] https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1560103639487&uri=CELEX%3A32019R0881.

[61] Für weitere Informationen vgl. Kipker/Scholz in MMR-Aktuell 2019, 414986.

4. Haftungsregime

Künstliche Intelligenz kann Schäden verursachen. Sie funktioniert anders als Menschen. Dies weckt auch Ängste. Fragen wie die, nach welchen Kriterien eine KI arbeitet, wenn sie über Leben und Tod zu entscheiden hat, wecken Emotionen. Bekannt ist das Beispiel der KI eines selbstfahrenden Autos, die in einem Entscheidungsdilemma steckt, wenn sie bei einer gefährlichen Situation nur den Fahrer oder einen Fußgänger retten kann – und der andere Verkehrsteilnehmer getötet wird. Entsprechend gehört das Haftungsregime seit Jahren zu den meistdiskutierten rechtlichen Themen bei KI. Die jüngsten Fortschritte aus dem Bereich generative KI wie ChatGPT und Dall-E – die Inhalte wie Text, Grafiken, Audio oder Videos erzeugen kann – haben den Blick jedoch zunehmend auf die Verletzung immaterieller Rechte gelenkt – sowohl was die Daten angeht, durch die diese Systeme lernen, als auch was die so erzeugten Daten angeht. Fehlinformationen durch diese Systeme rückten ebenfalls stärker in den Fokus der Diskussion. Fragen des Immaterialgüterrechts haben wir bereits oben behandelt; die allgemeineren Fragen der Haftung sind in der aktuellen Diskussion um generative KI und Immaterialgüter sowie Datenschutz etwas in den Hintergrund gerückt, aber nach wie vor sehr relevant – gerade auch mit Blick auf die Zukunft und immer autonomer agierende KI- und Roboter-Systeme.

4.1 Vertragliche und gesetzliche Haftung

Das deutsche Haftungsregime unterscheidet hauptsächlich zwischen einer vertraglichen und einer gesetzlichen Haftung. Die wichtigsten Bestimmungen zur vertraglichen Haftung finden sich in den §§ 280 ff. BGB und die zur gesetzlichen Haftung in den §§ 823 ff. BGB.

Die vertragliche Haftung ergibt sich aus der Verletzung einer vertraglichen Pflicht; die (außervertragliche) gesetzliche Haftung ergibt sich aus der Verletzung gesetzlicher Rechte oder Pflichten. In beiden Haftungssystemen ist eine Verletzung geschützter Rechte oder bestehender Pflichten notwendig. Geläufig sind hier zunächst Eigentum, Gesundheit oder Leben. Darüber hinaus kann aber auch eine Vielzahl weiterer Rechte betroffen sein, beispielsweise Immaterialgüterrechte oder Persönlichkeitsrechte. Für eine Haftung muss die Verletzung für den Schaden kausal und zurechenbar sein. Eine Haftung für atypische Schäden besteht in der Regel nicht.

4.2 Kein Vertrag: Verschuldenshaftung und Gefährdungshaftung

Das deutsche Haftungsregime unterscheidet im Rahmen der nachfolgend maßgeblich behandelten, außervertraglichen, d.h. gesetzlichen Haftung zwischen der Verschuldenshaftung und der Gefährdungshaftung.

4.2.1 Verschuldenshaftung

Die Verschuldenshaftung setzt, wie aus dem Begriff bereits deutlich wird, ein Verschulden voraus. Ein Verschulden beruht in der Regel entweder auf Vorsatz oder auf Fahrlässigkeit. Eine Person handelt fahrlässig, wenn sie die im Verkehr erforderliche Sorgfalt außer Acht lässt, § 276 BGB. Dieses Verschulden kann durch Handeln oder Unterlassen begründet werden, die Rechtsverletzung muss zudem rechtswidrig gewesen sein.

Bei der Verschuldenshaftung muss der Geschädigte grundsätzlich das Vorliegen der Anspruchsvoraussetzungen beweisen – und somit auch ein Verschulden des Gegners. Dies bedeutet in der Praxis eine nicht unerhebliche Hürde für viele Geschädigte. Ganz besonders groß kann diese Hürde bei KI sein – wir werden darauf unten gleich noch näher eingehen (Abschnitt 2.3).

Eine Art der Verschuldenshaftung, die im Hinblick auf Künstliche Intelligenz besonders von Bedeutung sein kann, ist die „Produzentenhaftung" nach § 823 Abs. 1 BGB. Auch die Produzentenhaftung setzt zunächst ein vorsätzliches oder fahrlässiges Verhalten des Herstellers (Produzenten) oder seiner Mitarbeiter voraus. Grundsätzlich muss eine Person, die eine Verletzung oder einen anderen Schaden an einem durch § 823 Abs. 1 BGB geschützten Rechtsgut, d.h. des Lebens, des Körpers, der Gesundheit, der Freiheit, des Eigentums oder eines sonstigen Rechts, durch ein Produkt erlitten hat, also zunächst nachweisen, dass diese Schäden auf ein vorsätzliches oder fahrlässiges und zugleich rechtswidriges Verhalten des Herstellers zurückzuführen sind.

Dabei ist die haftungsbegründende Handlung des Produzenten darin zu sehen, dass er eine fehlerhafte Software in den Verkehr gebracht hat.[62]

Auch dann, wenn ein Hersteller andere Personen mit der Produktion beauftragt, ist er haftbar. Dies gilt allerdings nicht, wenn er bei der Auswahl dieser Personen oder bei seiner Leitung der Herstellung die im Verkehr erforderliche Sorgfalt hat walten lassen. Die Ersatzpflicht tritt außerdem nicht ein, wenn der Schaden auch bei Anwendung dieser Sorgfalt entstanden sein würde, § 831 BGB.

In den meisten Fällen ist es für einen Geschädigten, der keinen Einblick in den Herstellungsprozess oder das Produkt hat, unmöglich zu beweisen, dass der Hersteller vorsätzlich oder fahrlässig und rechtswidrig gehandelt hat, oder die Behauptung eines Herstellers, er habe sorgfältig gehandelt, zu widerlegen. Daher gibt es im Rahmen der Produzentenhaftung in einigen Fällen eine Beweislastumkehr für dieses Verschulden. Hat der Geschädigte den Fehler eines Produkts bewiesen oder steht dieser Fehler objektiv fest, kann eine Beweislastumkehr sogar für die Pflichtverletzung des Herstellers in Frage kommen. Der Geschädigte muss aber in jedem Fall den Schaden und die Ursächlichkeit des Fehlers für den Schaden beweisen. Diese Beweislastumkehr kann für durch eine KI-Geschädigte eine erhebliche Erleichterung darstellen, da der Entwicklungsprozess der KI von Außenstehenden schwer zu durchschauen ist.

---

[62] Vgl. Taeger/Pohle, Computerrechts-Handbuch, Teil 18, Rn. 18 ff., 42 ff.

Die Fehlerhaftigkeit der KI festzustellen, kann aber ebenfalls Schwierigkeiten bereiten, dazu sogleich noch (Abschnitt 2.3).

Daneben können Schäden, die durch die Verletzung von Schutzgesetzen außerhalb des BGB entstehen, zu Ansprüchen des Geschädigten führen, § 823 Abs. 2 BGB. Dies können beispielsweise Gesetze wie das Medizinproduktegesetz (MPG) oder das Produktsicherheitsgesetz, aber auch einzelne Normen des Strafgesetzbuchs (StGB) sein. Allerdings gelten auch hier die Grundsätze der Verschuldenshaftung.

4.2.2 Gefährdungshaftung

Die unter 2.2.1 beschriebene Verschuldenshaftung wird durch die Gefährdungshaftung ergänzt. Sie beruht in der Regel auf besonderen gesetzlichen Bestimmungen, zum Beispiel in § 7 StVG für Kraftfahrzeuge, § 1 ProdHaftG für Produkte, § 1 HaftPflG für Züge, § 33 LuftVG für Luftfahrzeuge und § 1 UmweltHG für Kraftwerke und ähnliche Gefahrenquellen.

Für eine Gefährdungshaftung genügt es, dass jemand eine Gefahrenquelle schafft oder beherrscht. Er kann ohne Verschulden haften, d.h. es bedarf nicht einmal leichter Fahrlässigkeit. Beispielsweise kann ein Fahrzeughalter für Schäden, die durch sein Fahrzeug verursacht werden, auch dann haften, wenn er diese Schäden nicht selbst verschuldet hat, § 7 StVG. Das mit dem Eigentum an einem potenziell gefährlichen Fahrzeug verbundene Risiko ist ausreichend, um eine solche Haftung zu begründen.

Eine wichtige Sonderform der Gefährdungshaftung gerade auch in Bezug auf Künstliche Intelligenz ist die „Produkthaftung“ nach dem Produkthaftungsgesetz, das auf der europäischen Produkthaftungsrichtlinie basiert.[63] Dieses Gesetz erfasst indes nur Schäden an Leben, Körper, Gesundheit oder Sachen. Rein wirtschaftliche Schäden oder Schäden an anderen Rechtsgütern werden somit nicht erfasst. Die Produkthaftung beruht auf der Annahme, dass das Inverkehrbringen eines Produktes bereits ein Risiko verursacht, für das der Hersteller haften muss. Nach allgemeiner Meinung kann eine fehlerhafte Software auch Ansprüche nach dem Produkthaftungsgesetz auslösen.[64] Der Geschädigte muss hierbei zwar nachweisen, dass ein Schaden durch den Fehler eines Produktes verursacht worden ist. Ein Fehler eines Produktes lässt sich in der Regel leichter nachweisen als ein vorsätzliches, fahrlässiges oder rechtswidriges Verhalten des Herstellers. Ist dies der Fall, haftet der Hersteller.

Die Produkthaftung macht die anderen Haftungsregime jedoch keineswegs obsolet. Sie ist hinsichtlich der Arten von Schäden, die geltend gemacht werden können, beschränkt. Nicht abgedeckt sind insbesondere Vermögensschäden und Schäden am

---

[63] Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte. Am 28. September 2022 hat die Kommission einen neuen Vorschlag einer Produkthaftungsrichtlinie veröffentlicht (COM(2022)), nach der Software ausdrücklich als Produkt im Sinne der Richtlinie definiert wird.

[64] Vgl. Taeger/Pohle, Computerrechts-Handbuch, Teil 18, Rn. 119 f.

Produkt selbst, § 1 ProdHaftG. Sachschäden sind nur gedeckt, wenn der Schaden an einer Sache verursacht wurde, die üblicherweise zum privaten Gebrauch oder Verbrauch bestimmt ist und zum eigenen privaten Gebrauch oder Verbrauch verwendet wurde, § 1 Abs. 1 ProdHaftG. Darüber hinaus sind solche Schäden nur dann gedeckt, wenn sie 500,00 Euro je Schadensfall übersteigen, § 11 ProdHaftG. Die Produkthaftung ist auch hinsichtlich der Gesamthöhe für den Ersatz von Schäden, die durch ein Produkt verursacht wurden, beschränkt, § 10 ProdHaftG.[65]

4.2.3 Haftung nach spezialgesetzlichen Regelungen (Immaterialgüterrecht)

Wie eingangs erwähnt, existieren eine Vielzahl spezialgesetzlicher Regelungen, die Haftungsfragen klären. Zu erwähnen sind insbesondere die immaterialgüterrechtlichen Bestimmungen. Diesen Regelungen ist gemein, dass sie bei begangener Rechtsverletzung und befürchteter Wiederholungsgefahr zumeist einen Unterlassungsanspruch gewähren. Dieser ist sowohl im Marken-, Patent- sowie Urheberrecht als auch im Gesetz gegen den unlauteren Wettbewerb vorgesehen. Die Besonderheit des Unterlassungsanspruchs liegt darin, dass dieser verschuldensunabhängig ist. Ein Verschulden ist erst für die entsprechenden spezialgesetzlichen Schadensersatzansprüche erforderlich, vgl. beispielweise § 14 Abs. 5 MarkenG, § 9 Abs. 1 UWG oder § 97 Abs. 2 UrhG. Die Rechtsverletzung muss dabei für den entstandenen Schaden kausal und zurechenbar sein.

Darüber hinaus können persönlichkeitsrechtliche Bestimmungen eine Rolle spielen. Rechtsgrundlage des allgemeinen Persönlichkeitsrechts ist Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG. Das Bundesverfassungsgericht hat das allgemeine Persönlichkeitsrecht aus Art. 2 Absatz 1 in Verbindung mit Art. 1 Absatz 1 GG abgeleitet[66] und seither fortentwickelt. Der Schutzbereich ist vielgestaltig und erfasst die persönliche Lebenssphäre einer Person, das Recht auf (informationelle) Selbstbestimmung, das Recht am eigenen Bild und Wort u.v.m. Das allgemeine Persönlichkeitsrecht wird als „sonstiges Recht“ als ein geschütztes Rechtsgut im Sinne des § 823 Absatz 1 BGB verstanden. Dementsprechend steht dem Geschädigten bei einer Rechtsgutsverletzung ein Anspruch auf Schadensersatz zu. Im deutschen Schadensrecht gilt das Prinzip der Naturalrestitution, das heißt der Geschädigte ist so zu stellen, wie er stünde, wenn das schädigende Ereignis nie eingetreten wäre. Dies ist bei einer Verletzung des Persönlichkeitsrechts in der Regel gerade nicht möglich, so dass der Schadensersatz ausnahmsweise in Geld zu bemessen ist (vgl. dazu §§ 249 ff. BGB). Darüber hinaus hat der Geschädigte gegen den Schädiger auch hier einen verschuldensunabhängigen Beseitigungs- und Unterlassungsanspruch aus § 1004 Absatz 1 BGB.

Einzelheiten zum Immaterialgüterrecht haben wir bereits oben behandelt.

---

[65] Zurzeit insgesamt 85 Mio. Euro für alle Personenschäden pro Fehler, § 10 Abs. 1 ProdHaftG.

[66] BVerfGE 30, 174 ff.

4.3 Anwendung auf Künstliche Intelligenz

4.3.1 Problemstellung

Obwohl das deutsche Haftungsregime verschiedene Möglichkeiten der Haftung kennt, gibt es derzeit keine Haftung der Künstlichen Intelligenz selbst. Dies entspricht der Rechtstradition, die bislang nur eine Haftung von Menschen (ggf. mittelbar über juristische Personen) kennt. Technologien haften hingegen nicht „selbst". Wie und inwieweit das bestehende Haftungssystem auf Künstliche Intelligenz und autonome Systeme angewendet werden sollte, wird aktuell umfassend diskutiert.[67]

Besonderheiten ergeben sich vorliegend insbesondere dann, wenn Systeme autonom agieren. In diesen Fällen kann es sehr schwierig sein, die Kausalitätskette von einem Schaden, der durch das betreffende System autonom verursacht wurde, zu einer verantwortlichen natürlichen (d.h. „echten") oder juristischen Person zurückzuverfolgen. Gleiches gilt für die häufig von außen kaum durchschaubaren internen Prozesse einer Künstlichen Intelligenz (sogenannte Opazität).

Dabei sind nicht nur Zwei-Personen-Konstellationen (Hersteller/Geschädigter) Gegenstand von Haftungsfragen. Vielmehr ist auch zu klären, inwieweit der Verwender einer Künstlichen Intelligenz, die bei Dritten Schäden verursacht, haftbar zu machen ist. Allerdings wird diesem nur dann ein haftungsrechtlicher Vorwurf zu machen sein, wenn er beim Einsatz des Systems nicht sorgfältig gehandelt hat.[68]

Ferner ist zu bedenken, dass Künstliche Intelligenz ohne eigenes „Verschulden" Schäden verursachen kann – Vorsatz oder Fahrlässigkeit sind zunächst menschliche Schuldkategorien; eine Technologie kann daher im Rechtssinne nicht vorsätzlich oder fahrlässig handeln.[69] Vielmehr können sich Schäden durch Künstliche Intelligenz als Ergebnis fehlerhafter Software, fehlerhafter oder ungeeigneter Lerndaten, zufälliger Elemente oder der Einflussnahme Dritter darstellen.

Unbeabsichtigte Ergebnisse einer herkömmlichen, nicht „intelligenten" Software können Rechte verletzen, doch die damit zusammenhängenden Fragen unterscheiden sich nicht wesentlich von Schäden, die durch oder mithilfe anderer Sachen verursacht

---

[67] Vgl. nur Borges, NJW 2018, 977; Bräutigam/Klindt, NJW 2015, 1137; Denga, CR 2018, 69; Eichelberger, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 5 Rn. 1 ff.; Hacker, NJW 2020, 2142; Linardatos, ZIP 2019, 504; Riehm/Meier, in: Fischer/Hoppen/Wimmers, DGRI Jahrbuch 2018, „Künstliche Intelligenz im Zivilrecht"; Spindler, CR 2015, 766; Bericht der Arbeitsgruppe „Digitaler Neustart" der Justizminister der Länder zur Haftung von autonomen Systemen vom 15. April 2020.

[68] Vgl. Bräutigam/Klindt, NJW 2015, 1137, 1139.

[69] Denkbar erscheinen aber Fälle, in denen die Künstliche Intelligenz einen ihr naheliegenden Vorteil programmierungsgemäß herbeiführen will, wie in dem (etwas drastischen, aber plastischen) Beispiel von Denga, CR 2018, 69, 71: „Ein Finanzanlage-Roboter könnte über seine Vernetzung mit anderen Systemen eine Zug-Entgleisung bewirken, um vom Leerverkauf der Aktien des Bahnunternehmens zu profitieren."

werden. Bei Künstlicher Intelligenz und autonomen Systemen stellen sich neuartige Fragen. Autonome Fahrzeuge, die einen Unfall verursachen, werden häufig diskutiert.[70]

Auch über das plastische Beispiel autonomer Fahrzeuge hinaus werden Haftungsfälle durch den Einsatz Künstlicher Intelligenz immer häufiger auftreten und erfordern einen rechtlichen Rahmen, der Geschädigten eine angemessene Haftung zubilligt. Ähnlich plastisch erscheinen beispielsweise Fehlüberweisungen durch Künstliche Intelligenz oder Fehlberatungen durch Robo Advisors, ebenso wie Datenschutzverstöße durch ADM-Systeme[71], Leaks von vertraulichen Informationen durch Textgenerierungsprogramme[72] oder Verletzungen von geistigem Eigentum durch Künstliche Intelligenz in viralem Marketing oder durch generative KI.

4.3.2 Anwendung bestehender Regelungen

Bis zur Ausarbeitung spezifischer Regelungen für Künstliche Intelligenz sind die bestehenden Haftungsregelungen anzuwenden, soweit diese Anwendung sachlich angemessen ist.

Zunächst erscheint es angemessen, Systeme, die über einen gewissen Grad an Autonomie und ein gewisses Potenzial verfügen, Schäden an den Schutzgütern des Produkthaftungsrechts (u.a. Leben und Gesundheit) zu verursachen, der Gefährdungshaftung des Herstellers[73] zu unterwerfen. Auch hier dürfte weiterhin die Annahme gelten, dass der Hersteller des Endprodukts den größten Einfluss auf die Gefahren dieses Produkts hat – auch wenn Hersteller von „zusammengesetzten" Produkten aus Hard- und Software wie beispielsweise autonomen Fahrzeugen dies naturgemäß anders beurteilen mögen.[74] Besonderen Herausforderungen unterliegt die Produkthaftung mit Blick auf Künstliche Intelligenz allerdings insoweit, als dass „reine" Software bislang kein „Produkt" im Sinne der Produkthaftung ist; nur bewegliche Sachen und Strom sind erfasst. Hier mehren sich Stimmen, die zur Vermeidung von Schutzlücken auch Software der Produkthaftung unterwerfen wollen.[75] Dieses Problem wird nun in dem Vorschlag für eine neue Produkthaftungsrichtlinie vom

---

[70] So waren Testfahrzeuge von Google von Januar 2015 bis Oktober 2015 in acht Unfälle verwickelt, http:// www.sueddeutsche.de/auto/autonomes-fahren-crash-kurs-mit-google-1.2684782; 2018 wurde eine Passantin bei einem Unfall mit einem autonomen Uber-Fahrzeug aufgrund eines Softwarefehlers – und eines menschlichen Fehlers – getötet, https://www.auto-motor-und-sport.de/verkehr/toedlicher-unfall-autonom-auto-uber-softwarefehler/. Die Quantität der Vorfälle mag indes auch an der immer umfangreicheren Testung und Nutzung autonomer Fahrzeuge liegen.

[71] Algorithmic Decision Making.

[72] Falls vertrauliche Geschäftsgeheimnisse zum Anlernen von generativer Software verwendet werden, vgl. https://www.techradar.com/news/samsung-workers-leaked-company-secrets-by-using-chatgpt.

[73] Hersteller nach dem Produkthaftungsgesetz ist, wer das Endprodukt in Verkehr bringt.

[74] So hat eine Umfrage des bitkom unter Automobilunternehmen 2017 ergeben, dass nach 41 Prozent der Befragten die Software-Anbieter bei Unfällen mit autonomen Fahrzeugen haften sollten; 21 Prozent sahen den Fahrer und lediglich 19 Prozent die Autohersteller in der Pflicht. 12 Prozent sprachen sich für eine Haftung des Fahrzeughalters aus, vgl. https://www.bitkom.org/Presse/Presseinformation/Wer-haftet-fuer-mein-selbstfahrendes-Auto.html.

[75] Vgl. bspw. Redeker, in: ders., IT-Recht, C. Spezielle Fragen, Rn. 878 m.w.N.

28 September 2022 adressiert, die die Richtlinie 85/374/EWG ersetzen soll.[76] Danach fällt auch reine Software unter den Produktbegriff. Insbesondere sollen nach diesem Vorschlag KI-Systeme und KI-gestützte Waren als „Produkte" aufzufassen sein und in den Anwendungsbereich der Produkthaftungsrichtlinie fallen.[77] Der Richtlinienvorschlag muss jedoch noch das europäische Gesetzgebungsverfahren durchlaufen, bevor die neue Produkthaftungsrichtlinie in Kraft tritt und von den Mitgliedsstaaten umgesetzt werden muss. Ein weiteres Thema sind Dienstleistungen, die mittels Künstlicher Intelligenz erbracht werden – auch Dienstleistungen werden bislang nicht von der Produkthaftung erfasst.

Da die Haftung nach dem Produkthaftungsrecht nur begrenzt Schäden erfasst, ist es naheliegend, auch die Produzentenhaftung auf Künstliche Intelligenz anzuwenden, einschließlich der dortigen Möglichkeiten zur Beweislastumkehr. Hat eine Künstliche Intelligenz nachweislich die Rechtsgüter des Geschädigten verletzt, könnte es somit auch im Rahmen der Verschuldenshaftung zu einer Haftung des Herstellers einer Künstlichen Intelligenz kommen.

In Betracht kommen im Rahmen der Produzentenhaftung insbesondere Verletzungen der sogenannten Produktbeobachtungspflicht:[78] Grundsätzlich ist das Inverkehrbringen eines Produkts der relevante Zeitpunkt für die Frage, ob der Hersteller pflichtgemäß gehandelt hat. Die Pflichten des Produzenten beginnen jedoch schon vor dem Inverkehrbringen und enden nicht mit der Inverkehrgabe.[79] Wird das Produkt hiernach weiterentwickelt bzw. schreitet die Entwicklung vergleichbarer Produkte allgemein voran, begründet das „schlechtere" frühere Produkt an sich noch keinen Haftungsfall; diese sogenannten Entwicklungsrisiken sind zunächst kein Haftungsgrund. Der Hersteller muss allerdings ein Produkt auch nach dessen Inverkehrbringen auf schädliche Eigenschaften hin beobachten und ggf. einschreiten, beispielsweise durch Warnhinweise oder Rückrufe. Unterlässt er dies, besteht ein Haftungsrisiko. Im Falle von Künstlicher Intelligenz könnte ein Hersteller denkbar auch durch Updates einschreiten. Dabei gilt: Je komplexer oder „neuartiger" ein Produkt ist oder je größer das Schädigungspotential des Produkts ist, desto intensiver kann die Produktbeobachtungspflicht sein. Gerade im Fall von KI wird von einer intensiven Produktbeobachtungspflicht auszugehen sein, da die Produkte neuartig sind und wenig Erfahrung mit den von ihnen ausgehenden Risiken besteht.[80] Wirkt Künstliche Intelligenz mit Systemen Dritter zusammen, könnte sich eine Produktbeobachtungspflicht auch auf die Beobachtung dieses Zusammenwirkens beziehen – jedenfalls in einem angemessenen Rahmen.

---

[76] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Haftung für fehlerhafte Produkte (COM/2022/495 final).

[77] https://eur-lex.europa.eu/resource.html?uri=cellar:b9a6a6fe-3ff4-11ed-92ed-01aa75ed71a1.0003.01/DOC_1&format=DOC, vgl. Seite 5.

[78] Ausführlich Eichelberger, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 5 Rn. 32 ff.

[79] Reusch in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, Kapitel 4.1.10 Rn. 144.

[80] Näher hierzu: BGH NJW 1987, 1009 ff. – Honda.

Ebenso könnte es im Zusammenhang mit Künstlicher Intelligenz auch zu besonderen Instruktionspflichten kommen: Gerade bei neuen Technologien, deren Risiken Anwendern noch nicht geläufig sind, könnte es notwendig sein, herstellerseitig auf besondere Risiken der betreffenden Künstlichen Intelligenz hinzuweisen. Zu beachten ist hierbei allerdings, dass gerade bei Instruktions- und Produktbeobachtungspflichten (weil diese nicht den Herstellungsprozess betreffen) der Geschädigte nach derzeitiger Rechtslage die Pflichtverletzung beweisen muss.[81]

Darüber hinaus ist auch eine Verletzung von Immaterialgüterrechten sowie des Allgemeinen Persönlichkeitsrechts durch KI denkbar. Hierauf gehen wir wegen des Sachzusammenhangs im Kapitel 3 „Immaterialgüterrechte“ im Detail ein.

4.3.3 Anwenderhaftung

Weiter ist an die Haftung der Anwender von Künstlicher Intelligenz zu denken. Sofern der Anwender nicht vorsätzlich handelt, käme hier eine Verschuldenshaftung maßgeblich aufgrund der Verletzung von Verkehrssicherungspflichten (insbesondere Überwachungspflichten) in Betracht. Auch hier ist aber zu fragen, wie „intelligent“ bzw. autonom das jeweilige System handelt und ob dies noch dem Anwender im konkreten Einzelfall zuzurechnen ist – oder beispielsweise doch dem Hersteller. Dort, wo es bereits spezialgesetzliche Regelungen für eine Gefährdungshaftung gibt, wie beispielsweise für Fahrzeuge nach § 7 StVG, dürfte diese auch auf Künstliche Intelligenz anzuwenden sein. Dies jedenfalls dann, wenn die Künstliche Intelligenz Teil der betreffenden Gefährdung wird, wie bei autonomen Fahrzeugen.

4.3.4 Vertragliche Haftung

Die vertragliche Haftung wirft vergleichsweise wenig dogmatische Probleme auf, da die Vertragsparteien weitgehend frei sind, das Haftungsregime zu definieren. In der Praxis werden Fragen von Beweislast und Haftungsbegrenzung auch häufig detailliert geregelt. Die – auch in Verträgen häufigen – Kategorien von Vorsatz und Fahrlässigkeit können aber auch in Verträgen Schwierigkeiten bereiten. Beispielsweise sind Anwendungsfälle denkbar, in denen eine KI zuverlässiger arbeitet als ein Mensch, aber dennoch Fehler macht. Hier stellt sich die Frage, ob beispielsweise immer Vorsatz vorliegt, wenn Fehler in Kauf genommen werden, ob also beispielsweise der Sorgfaltsmaßstab derjenige einer optimalen KI sein sollte oder eines fachkundigen Menschen. Ein weiteres Beispiel dafür wäre auch KI, die basierend auf bisherigen Daten Prognoseentscheidungen für die Zukunft abgeben und darauf basierend sinnvolle wirtschaftliche Entscheidungen treffen soll. Hier ist durchaus denkbar, dass eine aus der vorhandenen Datenbasis an sich korrekt hergeleitete Entscheidung einer KI sich dennoch für einen Menschen als zum Entscheidungszeitpunkt offensichtlich falsch erweist, weil ein Mensch aus gänzlich anderen Quellen zusätzliche ausnahmsweise relevante Informationen bezogen hätte (z.B. aus den Nachrichten). Auch hier

---

[81] Vgl. BGH NJW 1981, 1603, 1605 f.

braucht es gegebenenfalls besondere vertragliche Haftungsregelungen und Sorgfaltsmaßstäbe, die beispielsweise die für die KI vorhandene limitierte Datenbasis in die Bewertung mit einfließen lassen, statt auf einen Menschen in vergleichbarer Funktion abzustellen.

4.3.5 Fazit

Die Vielfalt und Komplexität von Künstlicher Intelligenz wird über die bekannten Kriterien und Rechtsfragen hinaus gerade im Bereich der Verschuldenshaftung weitere Detailfragen aufwerfen. Je unabhängiger ein System von den Vorgaben des Produzenten und beispielsweise auf eigenen Erfahrungen oder Nutzereingaben basierend Entscheidungen trifft, desto weniger kann es möglicherweise zu einer Produzentenhaftung kommen. Auch könnte die Komplexität und Opazität von Künstlicher Intelligenz in Zukunft möglicherweise vermehrt zu (ggf. sehr spezifischen) Beweiserleichterungen führen. Auch eine Ausweitung der Produkthaftung auf die Besonderheiten von Künstlicher Intelligenz erscheint denkbar. Weiterhin könnten der Verursachungsgrad und die Beherrschbarkeit von Gefahren durch den Hersteller/Anbieter einerseits oder den Anwender des jeweiligen Systems andererseits Berücksichtigung finden, beispielsweise bei der Frage, ob ein Mitverschulden des Anwenders vorliegt (wenn dieser den Hersteller in Anspruch nehmen will) oder wie sehr ein Anwender die Gefahr beherrschen konnte, die er geschaffen hat (wenn er gegenüber Dritten haften soll).

4.4 Entwicklungen auf europäischer Ebene

Da sich die Entwicklung autonomer Systeme und Künstlicher Intelligenz nicht auf die Grenzen einzelner Mitgliedstaaten beschränkt, ist die Europäische Union bestrebt, den entsprechenden Haftungsrahmen zu vereinheitlichen. Hierfür liegen bereits mehrere Vorschläge für Richtlinien und Verordnungen vor, die sich jedoch noch im Gesetzgebungsverfahren der Europäischen Union befinden. Es bleibt abzuwarten, mit welchem Inhalt die verschiedenen Rechtsakte in Kraft treten werden – die gesetzliche Regelung befindet sich insoweit im Fluss. Nachstehend sollen die einzelnen Gesetzesinitiativen und Regelungsvorschläge auf europäischer Ebene kurz vorgestellt werden.

4.4.1 Vorschläge Expertengruppe der EU-Kommission 2019

Eine Expertengruppe der EU-Kommission machte 2019 Vorschläge zu einem Haftungsregime für Künstliche Intelligenz. Diese Vorschläge unterscheiden unter anderem nach der Gefährlichkeit der eingesetzten Systeme für Dritte und nach dem Grad, wie ein Anwender oder Anbieter ein System beherrschen kann. Zudem sollen Verwender von autonomen Systemen für diese ähnlich haften wie für menschliche Gehilfen (dies wäre in Deutschland die Haftung für Erfüllungs- oder Verrichtungsgehilfen). Hersteller von Produkten, die sich verändernde digitale Technologien beinhalten, sollten auch für Herstellerupdates haften können. Ebenso könnten Pflichtversicherungen für Technologien mit erhöhtem Risiko ebenso wie Beweiserleichterungen für

Geschädigte vorgesehen werden. Die Zuerkennung einer (Teil-)Rechtsfähigkeit für autonome Systeme sei jedoch nicht notwendig, da entstehende Schäden natürlichen oder juristischen Personen zugerechnet werden könnten (und sollten).[82]

4.4.2 Whitepaper der EU-Kommission Februar 2020

Auch die EU-Kommission prüft die Anpassung geltender Rechtsvorschriften wie beispielsweise der Produkthaftungsrichtlinie.[83] Hierzu hat sie im Februar 2020 ein Whitepaper veröffentlicht, das auch die Erkenntnisse der Expertengruppe aus 2019 berücksichtigt.[84]

So bergen Systeme, die häufige Software-Updates erfordern oder auf maschinellem Lernen beruhen, nach Auffassung der EU-Kommission das Risiko neuer Gefahrenquellen, welche zum Zeitpunkt des Inverkehrbringens noch nicht bestanden.[85] Diese Risiken[86] sollen in künftigen Rechtsvorschriften stärker berücksichtigt werden, etwa durch Einführung neuer Risikobewertungsverfahren bei derartigen Produkten. Für „KI-Anwendungen mit hohem Risiko", die in risikoreichen Sektoren eingesetzt werden,[87] werden Anforderungen anhand bestimmter Schlüsselmerkmale diskutiert.[88] Auch Unklarheiten über Zuständigkeiten einzelner Wirtschaftsteilnehmer in der Lieferkette sollen minimiert werden.[89]

Eine zentrale Aussage dürfte dabei sein, dass Personen, die infolge der Nutzung von Künstlicher Intelligenz einen Schaden erlitten haben, das gleiche Schutzniveau genießen sollen wie Personen, die durch andere Technologien geschädigt wurden.[90] In diese Richtung ging auch das Europäische Parlament schon 2017. Es war der Auffassung, dass ein künftiges Rechtsinstrument „die Art oder das Ausmaß der Schäden, die abgedeckt werden können, in keiner Weise beschränken" sollte. Ebenfalls sollten die Formen des Schadensersatzes für den Geschädigten nicht allein deshalb beschränkt werden, weil „der Schaden von einem nicht-menschlichen Akteur verursacht wird".[91]

---

82 Vgl. Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence and other emerging technologies, 20119, dot:10 2838/573689.

83 Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte.

84 Weißbuch COM (2020) 65 vom 19. Februar 2020 „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen" (im Folgenden: „EU-Kommission Whitepaper").

85 EU-Kommission Whitepaper, S. 16.

86 Zu weiteren Risiken und Sicherheitsaspekten im Zusammenhang mit Künstlicher Intelligenz s. COM (2020) 64 vom 19. Februar 2020, „Bericht über die Auswirkungen Künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung".

87 EU-Kommission Whitepaper, S. 20 f.

88 EU-Kommission Whitepaper, S. 22 ff.

89 EU-Kommission Whitepaper, S. 16.

90 EU-Kommission Whitepaper, S. 16.

91 Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103), Ziffer 52 (im Folgenden: „EU-Parlament, Entschließung 2015/2103").

Nach Auffassung der Kommission sollen künftig die einzelnen Verpflichtungen demjenigen Akteur obliegen, der am besten in der Lage ist, potenzielle Risiken zu bewältigen. Dies könnten je nach „Phase" (beispielsweise Entwicklung oder Betrieb) unterschiedliche Akteure sein. Für die Haftung gegenüber dem Endnutzer/Geschädigten soll aber weiterhin der Hersteller in Anspruch genommen werden können, gegebenenfalls ergänzt durch andere rechtliche Möglichkeiten im nationalen Recht (wie in Deutschland möglicherweise die Produzentenhaftung).[92]

Diese Tendenzen lassen derzeit vermuten, dass bekannte Mechanismen, insbesondere das Produkthaftungsrecht, fortgesetzt zur Anwendung kommen dürften – wenn auch stellenweise modifiziert, um den Besonderheiten der Künstlichen Intelligenz Rechnung zu tragen. Insoweit ist zu fordern, dass das künftige Haftungsregime kohärent ausgestaltet wird und nicht zu einer weiteren Zersplitterung der Rechtsordnung führt.

4.4.3 Entwurf einer Entschließung des EU-Parlaments mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz Künstlicher Intelligenz 2020

Das EU-Parlament hat der EU-Kommission im Oktober 2020 einen Regelungsvorschlag zur Haftung von Betreibern Künstlicher Intelligenz unterbreitet.[93] Damit hat es die Kommission aufgefordert, geeignete Vorschläge zur Ausarbeitung eines entsprechenden Unionsakts zu machen, wie es Art. 225 AEUV vorsieht.

Das Parlament erachtet einen einheitlichen Rechtsrahmen als notwendig und hat daher die Rechtsform einer Verordnung gewählt. Die Haftung von Herstellern soll dabei aber weiterhin Gegenstand der Produkthaftungsrichtlinie sein, die nach Auffassung des Parlaments ebenfalls zu einer Verordnung umgewandelt werden sollte. Eine Rechtspersönlichkeit von „KI-Systemen" (so die Terminologie des Entwurfs) wird explizit als nicht erforderlich erachtet.

Erfasst werden sollen Schäden an Leben, Gesundheit, Eigentum einer natürlichen oder juristischen Person sowie immaterielle Schäden.

Der Entwurf unterscheidet zwischen „KI-Systemen mit hohem Risiko" und „anderen KI-Systemen". Betreiber von „KI-Systemen mit hohem Risiko" sollen verschuldensunabhängig haften und sich nicht dadurch aus der Haftung befreien können, dass sie eine hinreichende eigene Sorgfalt oder autonome Handlung des Systems nachweisen. Betreiber von „anderen KI-Systemen" sollen hingegen verschuldensabhängig haften. Hierzu sieht der Entwurf Tatbestände vor, nach denen sich der Betreiber aus einer möglichen Haftung befreien kann, wenn der Betreiber nachweisen kann, dass die jeweiligen Voraussetzungen vorliegen. Ein Beispiel hierfür ist ein Haftungsausschluss

---

92 EU-Kommission Whitepaper, S. 27.

93 Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz Künstlicher Intelligenz (2020/2014(INL)).

bei Aktivierung des KI-Systems ohne Kenntnis des Betreibers, wenn er gegen diese Aktivierung „alle erforderlichen und angemessenen Maßnahmen getroffen" hatte. Insoweit handelt es sich zwar um eine verschuldensabhängige Haftung, jedoch mit einer teilweise umgekehrten Beweislast.

Die vorgeschlagene Verordnung nennt bei „KI-Systemen mit hohem Risiko" explizit „Frontend-" und „Backend-Betreiber" als Verpflichtete. Mehrere Betreiber sollen gegebenenfalls gesamtschuldnerisch haften, mit der Möglichkeit, im Innenverhältnis Regress zu nehmen.

Frontend-Betreiber sollen eine ausreichende Haftpflichtversicherung vorsehen. Backend-Betreiber sollen sicherstellen, dass sie durch eine Betriebshaftpflicht- oder Produkthaftpflichtversicherung abgesichert sind. Die Haftungssummen sollen bis zu zwei Mio. Euro für Personenschäden und bis zu einer Mio. Euro für immateriellen Schaden betragen (wenn letzterer zu einem „nachweisbaren wirtschaftlichen Verlust" führt). Ist der Frontend-Betreiber auch Hersteller, soll die Verordnung vorrangig vor der (allgemeinen) Produkthaftungsrichtlinie gelten.

Das Mitverschulden von betroffenen natürlichen Personen soll bei der Haftung des Betreibers eines KI-Systems gegebenenfalls berücksichtigt werden.

Zunächst handelt es sich bei diesem Entwurf zwar lediglich um einen Vorschlag des Parlaments, mit dem dieses die EU-Kommission zum Entwurf eines Unionsaktes aufgefordert hat (Art. 225 AEUV). Einen finalen Entwurf zu einem Rechtsakt oder gar einen beschlossenen Rechtsakt stellt der Entwurf damit nicht dar. Er gibt aber einige Anhaltspunkte dafür, wie eine europäische Regulierung künftig aussehen könnte: mit einer grundsätzlichen Unterscheidung zwischen Herstellern und Betreibern und einer ebenso grundsätzlichen Unterscheidung zwischen besonders „risikoreichen" Systemen Künstlicher Intelligenz und weniger risikoreichen Systemen. Im Einzelnen folgt der Entwurf durchaus bewährten Pfaden, wenn beispielsweise das Mitverschulden der betroffenen Personen berücksichtigt werden oder mehrere Betreiber als Gesamtschuldner haften sollen.

Sollte die EU-Kommission den Vorschlag bei der Schaffung eines entsprechenden Unionsaktes berücksichtigen, wäre dennoch im Einzelnen noch viel Detailarbeit nötig. Dies gilt insbesondere dann, wenn es wie vorgeschlagen zu einer Verordnung kommen sollte, die einheitlich in allen Mitgliedstaaten gilt. Vorschläge wie eine abschließende Liste aller „KI-Systeme mit hohem Risiko", die spätestens alle sechs Monate überprüft und ggf. erneuert werden sollte, wirken praktisch noch unausgereift und zu kasuistisch, um ein kohärentes, dynamisches und zukunftsfähiges Regime darstellen zu können. Auch die Beweislastverteilung für die verschuldensabhängige Haftung von Betreibern „anderer KI-Systeme" wäre noch klarer zu fassen.

Gegenüber den vorherigen Empfehlungen und Berichten von Expertengruppen und anderen Stellen geht das Parlament mit diesem Entwurf jedoch nun einen Schritt weiter in Richtung eines unionsweiten Rechtsakts zur Haftung im Zusammenhang mit Künstlicher Intelligenz.

4.4.4. Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz, so genannter AI Act)

Im April 2021 hat die EU-Kommission einen Vorschlag für eine Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz[94], auch bekannt als „AI Act“) vorgelegt.

Die EU-Kommission schlägt darin vor, eine technologieneutrale Definition von KI-Systemen in EU-Recht zu verankern. Darüber hinaus empfiehlt die Kommission, unterschiedliche Regelsätze auf der Basis eines risikobasierten Ansatzes mit vier Risikostufen zu verabschieden:

1. **KI mit unannehmbarem Risiko:**
   Verwendungen von KI, die gegen EU-Werte verstoßen (wie beispielsweise Praktiken, die ein erhebliches Potential haben, Personen zu manipulieren, indem sie auf Techniken zur unterschwelligen Beeinflussung zugreifen oder das Social Scoring durch Behörden), sind wegen des inakzeptablen Risikos, das sie schaffen, verboten;

2. **Hochrisiko-KI-Systeme:**
   Eine Reihe von KI-Systemen (aufgelistet in einem Anhang), die sich negativ auf die Gesundheit und Sicherheit der Menschen oder ihre Grundrechte auswirken, gelten als hochriskant. Um Vertrauen und einen konsequent hohen Schutz von Sicherheit und Grundrechten zu gewährleisten, sollen eine Reihe von verpflichtenden Anforderungen (einschließlich einer Konformitätsbewertung) für alle Hochrisiko-Systeme gelten;

3. **KI-Systeme mit geringem Risiko:**
   Derartige KI-Systeme unterliegen begrenzten Verpflichtungen wie beispielsweise Transparenzpflichten;

4. **Sonstige KI:**
   Alle anderen KI-Systeme können in der EU ohne zusätzliche rechtliche Verpflichtungen als die bestehende Gesetzgebung entwickelt und genutzt werden.

Der EU-Rat hat seinen gemeinsamen Standpunkt zum AI Act am 6. Dezember 2022 angenommen. Der Text des Rates umfasst unter anderem folgende Punkte:

- eine Einschränkung der Definition auf Systeme, die auf maschinellem Lernen und logik- und wissensbasierten Ansätzen basieren;

- eine Ausweitung des Verbots der Verwendung von KI für die soziale Bewertung auf private Akteure;

---

[94] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union (2021/206 (COM)), vgl. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52021PC0206.

- eine horizontale Ebene über die Klassifizierung von KI-Systemen als Hochrisiko-Systeme, um sicherzustellen, dass KI-Systeme, die voraussichtlich keine schwerwiegenden Verletzungen der Grundrechte oder andere bedeutende Risiken verursachen, nicht erfasst werden;

- eine Klärung der Anforderungen an Hochrisiko-KI-Systeme;

- neue Bestimmungen zur Berücksichtigung von Situationen, in denen KI-Systeme für viele verschiedene Zwecke verwendet werden können (KI mit allgemeinem Verwendungszweck);

- eine Klärung des Anwendungsbereichs des KI-Gesetzes (z.B. ausdrücklicher Ausschluss von nationaler Sicherheit, Verteidigung und militärischen Zwecken aus dem Anwendungsbereich des KI-Gesetzes) und Bestimmungen in Bezug auf Strafverfolgungsbehörden;

- eine Vereinfachung des Compliance-Rahmens für das KI-Gesetz;

- neue Bestimmungen zur Erhöhung der Transparenz und zur Berücksichtigung von Benutzerbeschwerden;

- substantielle Änderungen der Bestimmungen zur Unterstützung von Innovationen (z.B. KI-regulatorische Sandkästen).

Mitte Mai 2023 haben die zuständigen Ausschüsse des EU-Parlaments nunmehr sogenannte Kompromissänderungen für den Entwurf des Berichts zum AI Act genehmigt. Nach der Plenarabstimmung im EU-Parlament Mitte Juni 2023 begann die letzte Phase des sogenannten Trilogs, in der die drei Hauptakteure – der EU-Rat, die EU-Kommission und das EU-Parlament – die letzten Details des AI Acts ausarbeiten. Es dürfte davon auszugehen sein, dass das Gesetz voraussichtlich noch vor Ende 2023 in Kraft treten wird.

Der jüngste Vorschlag des EU-Parlaments beinhaltet neue Details zu den Grenzen von KI-Systemen für biometrische Identifikation, Kategorisierung und Überwachungszwecke. Auch Systeme zur Einflussnahme auf Wahlen sind nun explizit in die Liste der Hochrisikosysteme aufgenommen worden. Zudem wurden verschiedene Bestimmungen stärker an die DSGVO angelehnt.

Das EU-Parlament schlägt vor, neue allgemeine Prinzipien für die Entwicklung und Nutzung aller KI-Systeme in einen neuen Art. 4 a) AI Act aufzunehmen, wie etwa „menschliches Handeln und Kontrolle“, „technische Robustheit und Sicherheit“, „Privatsphäre und Datenschutz“, „Transparenz“, „Vielfalt, Nicht-Diskriminierung und Fairness“ sowie „soziales und Umweltwohl“. Regulatorische Anforderungen sollten klar und verständlich sein.

Der Vorschlag sieht ferner in Art. 5 ein generelles Verbot für „die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen“ respektive für Gesichtserkennung vor.

Weiter hat das EU-Parlament Sonderregelungen für freie Software beschlossen. Laut Begründung 12 a–c des AI Acts sollen diese Regelungen nicht für „freie und open source KI-Komponenten" gelten, es sei denn, sie werden als hochriskante Systeme eingestuft. Auf diese Weise möchte das EU-Parlament die Entwicklung und den Einsatz von KI insbesondere durch kleine und mittlere Unternehmen (KMUs), Start-ups, die akademische Forschung und Einzelpersonen fördern.

Die Veröffentlichung mehrerer generativer KI-Systeme wie ChatGPT und Midjourney Ende des Jahres 2022 hatten diese Systeme in den Mittelpunkt der öffentlichen Diskussionen gerückt. So verwundert es nicht, dass der Vorschlag des EU-Parlaments vom Mai 2023 nunmehr auch neue Regeln für generative KI enthalten.

Die Definition dieses neu eingeführten Begriffs ist als solche nicht Teil des Definitionskatalogs in Art. 3, sondern versteckt sich in Art. 28 b) Abs. 4 des AI Acts: Dort wird Bezug genommen auf „Grundmodelle, die in KI-Systemen verwendet werden, die speziell dazu bestimmt sind, Inhalte wie komplexen Text, Bilder, Audio oder Video („generative KI") mit unterschiedlichen Autonomiegraden zu erzeugen".

Art. 28 b) AI Act legt die Pflichten für Anbieter eines solchen Grundmodells fest. Es sind sieben grundlegende Anforderungen zu erfüllen:

- Ein Risikomanagementsystem durch Design, Test und Analyse einrichten;
- geeignete Datensätze verwenden, um mögliche Vorurteile zu vermeiden;
- geeignete Qualität (Leistung, Vorhersehbarkeit, Sicherheit) durch geeignete Methoden bewerten;
- Energieeffizienzstandards anwenden;
- angemessene technische Dokumentation und Gebrauchsanweisungen erstellen;
- ein Qualitätsmanagementsystem einrichten, und
- das Grundmodell registrieren, welches die Beschreibung der in der Entwicklung verwendeten Datenquellen, der verwendeten Schulungsressourcen usw. beinhaltet.

Zusätzlich wurden drei weitere Pflichten für generative KI-Systeme festgeschrieben. Sie müssen

- Transparenzpflichten gemäß Art. 52 Abs. 1 AI Act-E erfüllen,
- angemessene Vorkehrungen gegen die Erzeugung von Inhalten, die gegen EU-Recht verstoßen, treffen und
- eine Zusammenfassung der Verwendung von unter Urheberrecht geschützten Trainingsdaten öffentlich dokumentieren.

Die vorgesehenen Sanktionen sind erheblich: Geldbußen für nicht konforme Grundmodelle von bis zu 10 Millionen Euro, bei Unternehmen bis zu 2 Prozent des weltweiten jährlichen Umsatzes, je nachdem, welcher Betrag höher ist.

Es bleibt abzuwarten, welche Regelungen sich nun im Trilog durchsetzen und in Gesetzeskraft erwachsen werden.

4.4.5 Vorschlag einer Richtlinie über KI-Haftung vom 28. September 2022

Die Europäische Kommission hat am 28. September 2022 einen Vorschlag für eine Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an Künstliche Intelligenz (Richtlinie über KI-Haftung) angenommen.[95]

Am selben Tag wurde auch der bereits erwähnte Vorschlag für eine neue Produkthaftungsrichtlinie (siehe oben Kapitel 2.3.2) von der Europäischen Kommission angenommen. Der Zweck der Richtlinie über KI-Haftung besteht darin, einheitliche Regeln für den Zugang zu Informationen und die Erleichterung der Beweislast im Zusammenhang mit durch KI-Systeme verursachten Schäden festzulegen.

Die Richtlinie über KI-Haftung findet auf Ansprüche Anwendung, die nicht in den Anwendungsbereich der vorgenannten Produkthaftungsrichtlinie fallen, also die nicht auf ein fehlerhaftes Produkt zurückzuführen sind. Sie betrifft damit Fälle, in denen Schäden durch Fehlverhalten des Anbieters der KI verursacht werden. Dies umfasst beispielsweise Verletzungen der Privatsphäre oder Schäden, die durch Sicherheitsprobleme verursacht wurden.[96]

Die Richtlinie normiert keine konkreten Schadensersatzansprüche, sondern legt Beweiserleichterungen und widerlegbare Vermutungen für (potentielle) Kläger fest. Sie erleichtert damit die gerichtliche Durchsetzung von Schadensersatzansprüchen aufgrund von Schäden, die durch eine KI verursacht wurden.

Zunächst gibt Artikel 3 Abs. 1 des Richtlinienentwurfs Gerichten die Möglichkeit, auf Antrag eines (potenziellen) Klägers anzuordnen, dass einschlägige Beweismittel zu einem bestimmtem Hochrisiko-KI-System[97] offengelegt werden, das im Verdacht steht, einen Schaden verursacht zu haben. Voraussetzung hierfür ist, dass der (potenzielle) Kläger die Plausibilität seines Schadensersatzanspruchs ausreichend belegt.

---

[95] Die VO (EU) 2019/945 wurde bereits mit der Delegierten Verordnung (EU) 2020/1058 der Kommission vom 27. April 2020 (VO (EU) 2020/1058) erstmalig abgeändert. Die VO (EU) 2020/1058 führte insbesondere die zusätzlichen Drohnenklassen C5 und C6 ein.

[96] https://ec.europa.eu/commission/presscorner/detail/de/ip_22_5807.

[97] Der Entwurf knüpft an den Begriff des Hochrisiko-KI-Systems an, der in Artikel 6 des Vorschlags eines Gesetzes über künstliche Intelligenz (2021/0106 (COD)) definiert wird als ein KI-System, das erhebliche Risiken für die Gesundheit und Sicherheit oder die Grundrechte von Personen birgt, vgl. Seite 4, Ziffer 1.1 der Begründng (https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.01/DOC_1&format=DOC.

Zuvor muss der (potenzielle) Kläger alle angemessenen Anstrengungen unternommen haben, die Beweismittel zu beschaffen, Artikel 3 Abs. 2 des Richtlinienvorschlags. Bei seiner Entscheidung muss das Gericht die Interessen aller Parteien gegeneinander abwägen. Die Gerichte sollen insbesondere den Schutz etwaiger Geschäftsgeheimnisse berücksichtigen.

Artikel 3 Abs. 5 des Richtlinienentwurfs enthält ein Druckmittel bereit, um den Anbieter eines Hochrisiko-KI-Systems zur Offenlegung der angeforderten Informationen anzuhalten. Danach wird ein Verstoß gegen einschlägige Sorgfaltspflichten widerlegbar vermutet, wenn der gerichtlichen Anordnung nicht Folge geleistet wird.

Artikel 4 des Richtlinienentwurfs sieht darüber hinaus eine widerlegbare Vermutung für die Ursächlichkeit einer Sorgfaltspflichtverletzung für ein bestimmtes Ergebnis eines KI-Systems vor. Im Gegensatz zu Artikel 3 gilt Artikel 4 Abs. 1 des Richtlinienentwurfs auch für KI-Systeme die keine Hochrisiko-KI-Systeme sind. Trotz dieser widerlegbaren Vermutung muss der Kläger immer noch einen Verstoß gegen eine Sorgfaltspflicht nachweisen (sofern diese nicht ebenfalls vermutet wird, beispielsweise nach dem oben erwähnten Artikel 3 Abs. 5).

Artikel 4 Abs. 2 und 3 des Richtlinienentwurfs enthält eine abschließende Aufzählung von möglichen Sorgfaltspflichtverletzungen, die die widerlegbare Vermutung für die Ursächlichkeit der Sorgfaltspflichtverletzung für ein bestimmtes Ergebnis eines Hochrisiko-KI-Systems auslösen können.

4.5 Versicherungen

Die Frage, inwieweit Künstliche Intelligenz versicherbar ist bzw. versicherungspflichtig sein sollte, wird derzeit noch umfangreich diskutiert. Nachfolgend soll es dabei nur um die Versicherung von Künstlicher Intelligenz gehen, nicht die Nutzung von Künstlicher Intelligenz durch Versicherer.

Die Versicherungswirtschaft befindet sich mit Blick auf Künstliche Intelligenz noch am Anfang eines umfangreichen Prozesses.[98] Es gilt, versicherungsrelevante Akteure, Produkte, Prozesse und Haftungsrisiken zu identifizieren.

Klassische Versicherungen können dabei insbesondere für vergleichsweise einfach zu erfassende Produkte abgeschlossen werden. So können Industrieroboter gegenwärtig durch eine Maschinenversicherung abgesichert werden. Für besondere Aspekte Künstlicher Intelligenz sind diese Versicherungen aber üblicherweise nicht gedacht. Manche Versicherer bieten modulare Systeme an, welche die Risiken in den verschiedenen Stadien der Entwicklung und der Implementierung autonomer Systeme abdecken.

---

[98] Ebert, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 16 Rn. 6, 28 ff.

Diskutiert wird die Frage einer Pflichtversicherung. Für Fahrzeuge gibt es aufgrund deren abstrakter Gefährlichkeit und der potenziell hohen Schäden bereits seit langem gesetzlich vorgeschriebene Haftpflichtversicherungen. Auch im Rahmen von Künstlicher Intelligenz wird dies entsprechend erwogen. So hielt die von der EU-Kommission eingesetzte Expertengruppe 2019 u.a. fest: „The more frequent or severe potential harm resulting from emerging digital technology, and the less likely the operator is able to indemnify victims individually, the more suitable mandatory liability insurance for such risks may be."[99] Das EU-Parlament hatte zuvor bereits im Jahr 2017 festgestellt, dass der Hersteller, Eigentümer oder Benutzer eines Roboters verpflichtet werden könnte, für jeden autonomen Roboter eine Versicherung abzuschließen. Dabei sollte jedoch im Gegensatz zum (menschenbezogenen) Versicherungssystem für den Straßenverkehr allen potenziellen Verantwortlichkeiten in der Kette Rechnung getragen werden.[100] Zusätzlich erwog das EU-Parlament einen Versicherungsfonds für Schäden, für die kein Versicherungsschutz besteht.[101]

In seinem aktuellen Entwurf einer Richtlinie zur Haftung der Betreiber von KI-Systemen[102] (s. oben Ziffer 4.4.4) hat sich das EU-Parlament nun gegen einen „mit öffentlichen Mitteln finanzierten Entschädigungsmechanismus auf Unionsebene" ausgesprochen. Das Parlament hat jedoch die Kommission aufgefordert, diese solle „eng mit dem Versicherungsmarkt zusammenarbeiten, um innovative Versicherungsprodukte zu entwickeln, mit denen die Versicherungslücke geschlossen werden kann." Der Richtlinienentwurf selbst sieht Versicherungspflichten für Frontend- und Backend-Betreiber von „KI-Systemen" vor.

Angesichts der dargestellten Entwicklungen ist es nicht unwahrscheinlich, dass in Zukunft jedenfalls für besonders gefahrgeneigte Künstliche Intelligenz eine entsprechende Versicherung, möglicherweise sogar eine Pflichtversicherung, vorzusehen ist. Auch dürften Versicherungen verschiedenster Risiken auf verschiedenen Ebenen relevant werden – beispielsweise dann, wenn aufgrund von Fehlern autonomer Fahrzeuge verstärkt die Hersteller, nicht die Halter in die Haftung genommen würden.

4.6 Ein Blick in die Zukunft

Die voranstehenden Ausführungen bilden den status quo und die nähere Zukunft des Haftungsregimes für Künstliche Intelligenz ab.

Angesichts der derzeitigen Erscheinungsformen Künstlicher Intelligenz dürften bekannte Mechanismen wie die Gefährdungs- und Verschuldenshaftung, gegebenenfalls

---

[99] Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelli- gence and other emerging technologies, 20119, dot:10 2838/573689, Key Finding No. 33.

[100] EU-Parlament, Entschließung 2015/2103, Ziffer 57.

[101] EU-Parlament, Entschließung 2015/2103, Ziffer 58; zur Kritik an einer Fondslösung Eichelberger, in: Ebers/ Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 5 Rn. 70 m.w.N.

[102] Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission für eine Regelung der zivilrechtlichen Haftung beim Einsatz Künstlicher Intelligenz (2020/2014(INL)).

modifiziert, im Wesentlichen (noch) einen hinreichenden Haftungsrahmen bieten. Dabei wird das „Verhalten“ einer Künstlichen Intelligenz letztlich immer auf den Hersteller, gegebenenfalls auch den Betreiber (wie insbesondere im Falle automatisierter Fahrzeuge), zurückgeführt. Dieser haftet für die „Gefahrenquelle“, die er mit der Künstlichen Intelligenz beziehungsweise deren Betrieb geschaffen hat.

Je autonomer Künstliche Intelligenz in Zukunft handeln und „entscheiden“ wird, desto zweifelhafter erscheint es allerdings, die Haftung auf den jeweiligen Hersteller zurückzuführen.

Um hier dennoch keine Haftungslücken entstehen zu lassen, wird diskutiert, Künstlicher Intelligenz eine eigene Rechtspersönlichkeit zuzuerkennen. Diese könnte, wie unter Ziffer 4.6 skizziert, beispielsweise zu einer „Künstlichen Intelligenz mit beschränkter Haftung“ führen, die mit einem eigenen Haftungskapital für Verletzungen Dritter haftet.

Es bleibt in jedem Fall abzuwarten, ob es ausreicht, bekannte Mechanismen immer wieder neu an die Entwicklungen Künstlicher Intelligenz anzupassen – oder ob es hier nicht weitergehender, neuartiger Ansätze bedarf.

Ein paar dieser Ansätze wollen wir nachfolgend darstellen.

4.6.1 Rechtspersönlichkeit von Künstlicher Intelligenz

Das deutsche Recht kennt derzeit keine Rechtspersönlichkeit von Künstlicher Intelligenz. Es unterscheidet vielmehr nur zwischen natürlichen und juristischen Personen als möglichen Trägern von Rechten.

Der technische Fortschritt erfordert eine Überprüfung dieses Konzepts. Aus heutiger Sicht mag es zwar immer noch weit hergeholt erscheinen, über die Gewährung von Rechten und die Auferlegung von Pflichten für Künstliche Intelligenz nachzudenken. Künstliche Intelligenz wird aber immer autonomer, anpassungs- und lernfähiger und damit unberechenbarer. Sie wird in absehbarer Zukunft ein Maß an Unabhängigkeit erreichen, das neue Rechtskonzepte erfordern könnte, insbesondere wenn die bisherigen Ansätze des Machine Learning, wie das Deep Learning mittels neuronaler Netze, konsequent weiterentwickelt werden.

Eine der spannendsten Fragen ist daher, ob und inwieweit Künstlicher Intelligenz bzw. intelligenten oder autonomen Systemen eine eigene Rechtspersönlichkeit – und damit Rechte und Pflichten – zuerkannt werden sollte. Für eine eigene Rechtspersönlichkeit könnte eine Reihe von Gründen sprechen:

Künstliche Intelligenz wird immer komplexer und unabhängiger. Natürlich könnte man argumentieren, dass Künstliche Intelligenz keine echten Entscheidungen, wie sie von Menschen getroffen werden, trifft, sondern dass sie nur infolge von „WENN-DANN“-Funktionen oder in einem anderen determinierten Rahmen agiert. Aber mit zunehmender Komplexität und Autonomie wird es immer schwieriger, die „Entscheidungen“

einer Künstlichen Intelligenz „einzuprogrammieren“ oder gar zuverlässig vorherzusagen. Gerade die Entwicklung von Künstlicher Intelligenz mittels neuronaler Netze hat nicht mehr viel gemein mit der Programmierung über klassische „WENN-DANN“-Funktionen und kann unerwartete Ergebnisse hervorbringen. Das Vorhersagen der Ergebnisse von Künstlichen „Denkprozessen“ wird dadurch erschwert oder gar unmöglich und basiert maßgeblich auf dem, was die Künstliche Intelligenz bis dahin jeweils gelernt hat. Da sich bei diesen Verfahren Künstliche Intelligenz auch durchaus gegenseitig trainiert (Beispiel: Ein Schachprogramm spielt gegen andere Versionen von sich selbst und lernt daraus), tritt der Mensch auch als Lehrer zunehmend in den Hintergrund.

Mit jeder Variable und Erfahrung, die dem Entscheidungsprozess einer Künstlichen Intelligenz hinzugefügt wird, wird es schwieriger, die Entscheidung, die die Künstliche Intelligenz darauf basierend treffen wird, vorherzusagen oder zu verstehen. Dabei hat Künstliche Intelligenz in vergleichsweise einfachen Brettspielen wie Schach oder Go bereits bewiesen, dass sie durch eigenständiges Erlernen des Spiels und der besten Strategien in teilweise nur wenigen Stunden oder Tagen (in denen sie allerdings Millionen Trainingsspiele absolvieren) nicht nur bisheriger klassischer Software, sondern selbst den bisher besten menschlichen Spielern weit überlegen ist.[103] Wenn also eine Künstliche Intelligenz selbst die besten menschlichen Spieler durch Züge überraschen und besiegen kann, an die zuvor kein Mensch gedacht hat, so ist absehbar, dass das menschliche Gehirn auch in anderen komplizierteren Bereichen nicht mehr in der Lage sein wird, vorherzusagen, wie eine Künstliche Intelligenz in bestimmten Situationen reagieren wird, weil sie beispielsweise intelligentere und hoffentlich damit auch bessere Handlungsmöglichkeiten erkennen wird, als es ein Mensch kann.

Wir stehen hier erst ganz am Anfang einer Entwicklung, die nach und nach in viele Lebensbereiche Einzug halten wird und bei der sich der Mensch zunehmend von der Vorstellung wird verabschieden müssen, dass er bestimmte Situationen besser beurteilen kann als eine Künstliche Intelligenz.

Vorhersagen werden ebenso unmöglich, wenn Entwickler bewusst Zufallsentscheidungen hinzufügen, und noch mehr, wenn solche Zufallsentscheidungen auf den früheren Erkenntnissen einer Künstlichen Intelligenz basieren, die auf Daten gründet, die sie möglicherweise bereits gesammelt hat. Das zeigt besonders plastisch der von Microsoft entwickelte und bei Twitter eingesetzte Chatbot „Tay“: Dieser sollte sich mit Menschen unterhalten können und von ihnen lernen. Tatsächlich lernte Tay binnen kürzester Zeit von den Informationen, die ihm die Nutzer zukommen ließen. Dies führte allerdings dazu, dass Tay nach kurzer Zeit rassistisch und sexistisch äußerte. Tay wurde daraufhin von Microsoft deaktiviert.[104] Ein ähnlicher Vorgang spielte sich Anfang 2023 ab, als Microsoft eingreifen und den Bing A.I. Chatbot einschränken musste, weil die Diskussionen mit dem Chatbot gelegentlich schon nach

---

[103] Beispiele für solche Software sind „AlphaGo“, „AlphaGo Zero“ oder „AlphaZero“ des Entwicklers DeepMind; https://www.sueddeutsche.de/digital/kuenstliche-intelligenz-champion-aus-dem-nichts-1.3713570.

[104] Hierzu bspw. SZ Online vom 3. April 2016, https://www.sueddeutsche.de/digital/microsoft-programm-tay-rassistischer-chat-roboter-mit-falschen-werten-bombardiert-1.2928421.

einer geringen Anzahl von aufeinander aufbauenden Fragen „aus dem Ruder liefen" und unerwartete und für die Nutzer teils beunruhigende Verläufe nahmen.[105]

Gewöhnlich wird davon ausgegangen, dass eine Künstliche Intelligenz immer die „beste" Entscheidung treffen wird. Objektiv ist aber zum einen nicht stets vorhersehbar, was eigentlich die „beste" Entscheidung sein wird, u.a. weil dies von subjektiven Bewertungskriterien abhängt und zudem die Folgen vieler Entscheidungen auch von unzähligen Faktoren abhängen, die sich außerhalb der Kontroll- oder auch nur Wahrnehmungssphäre des Entscheiders abspielen. Die Schaffung Künstlicher Intelligenz kann zum anderen auch erfordern, den Abläufen dieser Künstlichen Intelligenz bewusst eine Zufallskomponente hinzuzufügen. Dies alles führt aber im Ergebnis dazu, dass die Entscheidungen einer Künstlichen Intelligenz in zahlreichen Fällen für Menschen nicht vorhersehbar sind oder es sein werden.

Entsprechend wird es auch nicht immer möglich sein, das Verhalten eines autonomen Systems zu kontrollieren oder vorherzusagen. Mit fortschreitender Autonomie wird es daher immer schwieriger werden, die Handlungen einer autonomen Künstlichen Intelligenz einem Menschen zuzuschreiben, der für ihre Handlungen die Verantwortung übernehmen soll. Menschen werden nicht immer in der Lage sein, den Grund für das jeweilige (Fehl-)Verhalten einer Künstlichen Intelligenz (z.B. unüberschaubare Lerndaten, Benutzereingaben, Manipulation durch Dritte, Ergebnis eines Hacks, zufällige Entscheidung, fehlerhafte Software usw.) zuverlässig zu bestimmen, geschweige denn verlässlich vorherzusagen. Damit kann es jedoch auch unmöglich werden, Schäden in der Kausalkette auf eine bestimmte natürliche oder juristische Person als Verursacher zurückzuführen. Auch eine einwandfrei programmierte Künstliche Intelligenz kann eine schwerwiegende Fehlentscheidung treffen, weil die Künstliche Intelligenz zuvor während ihres Betriebs für die später zu treffende Entscheidung ungünstige Erfahrungen gesammelt und daraus gelernt hat.

Eine Lösung für diese Fälle könnte daher darin bestehen, Künstlicher Intelligenz eine Rechtspersönlichkeit zuzuerkennen und sie damit zu einem Rechtssubjekt zu machen. Die Menschen könnten akzeptieren, dass eine Künstliche Intelligenz ihre eigenen autonomen Entscheidungen treffen und z.B. einen Verkehrsunfall verursachen, jemanden verletzen oder zwei Hektoliter Milch anstelle von zwei Flaschen bestellen kann. Solche Entscheidungen können sogar auf früheren Lernprozessen der Künstlichen Intelligenz beruhen. Denkbar wäre es dabei unter anderem, Künstlicher Intelligenz jedenfalls teilweise eine Rechtspersönlichkeit insoweit einzuräumen, wie sie zur Haftung der Künstlichen Intelligenz notwendig ist,[106] also eine Art „Haftungspersönlichkeit" (hierzu sogleich auch Ziffer 4.6).

Zwar könnte man auch hier der Ansicht sein, dass letztlich immer ein „Programm" hinter der Künstlichen Intelligenz steht, für dessen Folgen der Schöpfer haftbar zu machen ist. Allerdings wird das Verhalten von Künstlicher Intelligenz eben immer

---

[105] Siehe hierzu bspw. https://www.cnbc.com/2023/02/17/microsoft-limits-bing-ai-chats-after-the-chatbot-had-some-unsettling-conversations.html.

[106] Schirmer, JZ 2019, 17.

mehr auch von ihrem jeweiligen Input, von ihren „Lerndaten“ geprägt werden. Dieser Input wird üblicherweise dem Hersteller entzogen sein, insbesondere wenn man davon ausgeht, dass Künstliche Intelligenzen zunehmend selbständig in der Lage sein werden, neue Lerndaten ohne menschliche Kontrolle zu beschaffen (und sei es nur über Crawler im Internet oder Sensoren zur Erfassung der Umgebung). Neuronale Netze beruhen auf dem Prinzip von „try and error“. Je mehr sich Deep Learning bei Künstlicher Intelligenz durchsetzen wird, desto geringer ist der Einfluss des Herstellers auf die „Entscheidungen“ der Künstlichen Intelligenz – und damit auch auf deren Folgen.

Auch die bisweilen anzutreffende Aussage, anhand der vielen Daten, die bei der Nutzung einer Künstlichen Intelligenz anfielen, sei eine Produktbeobachtung künftig einfacher als je zuvor, verfängt in der Praxis nicht: Es ist keinesfalls gesagt, dass sich aus den „gesammelten“ Daten hinreichende Informationen ergeben; dazu müssten sie ihrerseits entsprechend auswertbar sein. Noch weniger ist damit gesagt, dass diese Daten mit Blick auf den Schutz persönlicher Daten oder Geschäftsgeheimnisse überhaupt vom Hersteller erhoben werden dürfen. Entsprechend wäre auch der Rückgriff auf Produktbeobachtungspflichten, jedenfalls bei autonomen Systemen, künftig nicht in jedem Fall ein wirksamer Ansatzpunkt für eine Haftung.

Mit steigender Autonomie könnte vielmehr eine (gegebenenfalls beschränkte) Rechtsfähigkeit von Künstlicher Intelligenz zahlreiche Rechtsprobleme lösen, während bisherige Zurechnungsmodelle an ihre Grenzen stoßen oder zumindest eine Weiterentwicklung oder Nutzung von Künstlicher Intelligenz wegen unüberschaubarer Risiken behindern könnten. Umgekehrt würde eine solche (beschränkte) Rechtsfähigkeit der damit ausgestatteten Künstlichen Intelligenz mittelfristig wohl auch ein erhöhtes wirtschaftliches und soziales Gewicht geben, wie dies auch bei juristischen Personen der Fall ist, beispielsweise bei Kapitalgesellschaften. Ob dies gesellschaftlich gewollt ist, sollte breit diskutiert werden.

4.6.2 Insbesondere: intelligente oder autonome Roboter

Das Vorangestellte wird insbesondere bei intelligenten oder autonomen Robotern deutlich: Bislang stellen diese allenfalls eine Sache im Sinne des BGB dar. Sachen haben aber keine eigenen Rechte und Pflichten. Ebenso hat die Software, die Künstliche Intelligenz, die dem Roboter innewohnt, keine Rechte und Pflichten. Auch ein autonomer und lernfähiger Roboter ist eine Sache und kann daher nach geltendem Recht nicht für seine Handlungen verantwortlich gemacht werden. Daher ist es bislang immer erforderlich, die Ursache für die Handlungen eines Roboters auf einen Menschen zurückzuführen, der dafür verantwortlich gemacht wird.

Eine mögliche Änderung dieses Ansatzes könnte eine Unterscheidung sein, die auf der Frage beruht, ob die Handlungen des Roboters aus der Sicht einer objektiven Person autonom und das Ergebnis eines adaptiven Entscheidungsprozesses zu sein scheinen oder nicht. Wenn sie nicht autonom sind, werden sie wahrscheinlich in irgendeiner Weise von einem Menschen gesteuert, so dass ein solcher Roboter ein Werkzeug ist und als eine Sache behandelt werden sollte. Entsprechend wäre eine

durch den Roboter verursachte Haftung allenfalls auf eine „hinter ihm“ stehende Person zurückzuführen, nicht aber auf den Roboter selbst.

Wenn ein Roboter jedoch lernfähig zu sein und autonom zu handeln scheint, könnte dies künftig anders zu beurteilen sein. Eine Sache verhält sich normalerweise nicht auf unerwartete Weise, ein autonomer Roboter kann dies jedoch durchaus tun. Darüber hinaus sind Entscheidungen, die der Roboter trifft, möglicherweise nicht die Folge der ihm von einem Menschen gegebenen Befehle, sondern das Ergebnis des adaptiven Verhaltens des Roboters. Daher könnte ein anderer Rechtsstatus für solche lernfähigen autonomen Roboter geeigneter sein, der den Besonderheiten besser als die Kategorisierung als „Sache“ Rechnung trägt.

Insoweit könnte auch von Menschen, die mit Robotern interagieren, erwartet werden, dass sie sich entsprechend angepasst bzw. angemessen verhalten und sich z.B. bei der Interaktion mit einem Roboter auf unvorhersehbares Verhalten einstellen. Sie könnten weniger darauf vertrauen, dass sie genau wissen, was als nächstes passieren wird, ähnlich wie ein Mensch bei der Interaktion mit Tieren, aber auch mit anderen Menschen.

Neben den Pflichten der Roboter, an die Haftungsfragen anknüpfen, und obwohl Roboter in absehbarer Zeit nicht die gleichen Rechte wie Menschen haben werden, erscheint es nicht undenkbar, Robotern auch angemessene Rechte im Hinblick auf ihre Rolle und Funktion in zukünftigen Gesellschaften einzuräumen. Wie diese Rechte genau auszugestalten sind und wie weit sie reichen dürfen, wird allerdings noch in den nächsten Jahren und Jahrzehnten Gegenstand intensiver und kontroverser Diskussionen sein.

4.6.3 Künstliche Intelligenz und juristische Personen

Die juristische Person ist eine Rechtsperson, die kein Mensch ist, aber ebenfalls verschiedene Rechte und Pflichten besitzt. Das Wesen einer juristischen Person ist nicht durch die Natur vorgegeben. Sie wird allein durch Gesetze definiert und kann daher an neue Bedürfnisse angepasst werden. Man kann daher durchaus von einer „virtuellen“ Person sprechen, da eine juristische Person gerade keine Person im eigentlichen Wortsinn ist, teilweise aber gleiche oder zumindest ähnliche Rechte wie eine natürliche Person hat. Entsprechend kann es sich auch in Bezug auf Künstliche Intelligenz lohnen, einen Blick auf juristische Personen zu werfen.

Juristische Personen wie Körperschaften, Vereine oder Gewerkschaften stellen in gewissem Sinne „virtuelle“ Personen dar, denen bestimmte Rechte eingeräumt werden, wie z.B:

- das Recht, ein eigenes Vermögen zu besitzen;
- das Recht, ein Bankkonto zu eröffnen;
- das Recht, rechtliche Schritte zum Schutz eigener Interessen einzuleiten, und

- das Recht, Schadenersatz für Verluste, einschließlich immaterieller Verluste (Image- oder Rufschädigung), zu erhalten.

Nach deutschem Zivilrecht können juristische Personen haftbar gemacht werden. Das deutsche Strafrecht gilt derzeit nicht für juristische Personen, aber ihre Vertreter können strafrechtlich belangt werden. Es gibt jedoch Bestrebungen, das Strafrecht in gewissem Umfang auf juristische Personen auszudehnen („Unternehmensstrafrecht").[107]

Eine besonders verbreitete juristische Person nach deutschem Recht ist eine Gesellschaft mit beschränkter Haftung (GmbH). Die GmbH, eine sogenannte Kapitalgesellschaft, hat Rechte und Pflichten und handelt durch ihre Vertreter. Sie hat ein Mindestkapital von 25.000 Euro, muss in das Handelsregister eingetragen werden und haftet mit ihrem Vermögen bzw. Kapital.

Die Übertragung der Grundstrukturen und Prinzipien von juristischen Personen auf Künstliche Intelligenz könnte ein Weg sein, um Künstlicher Intelligenz gewisse definierte Rechte und einen Status zu geben, der es ihr erlaubt, bestimmte Funktionen zu erfüllen und dabei gleichzeitig Adressat bestimmter Pflichten zu werden. Die Idee, Künstlicher Intelligenz einen vergleichbaren Status zu geben, ist beispielsweise für Software-Agents diskutiert worden, die zum Abschluss von Verträgen eingesetzt werden.[108] Die Idee kann grundsätzlich aber auch auf alle anderen Formen autonomer Künstlicher Intelligenz angewandt werden.

Insbesondere das Konzept der GmbH könnte auf Künstliche Intelligenz übertragen werden. Hierzu wäre es durchaus denkbar, verpflichtend ein gewisses Kapital für den Betrieb einer Künstlichen Intelligenz vorzusehen, mit der diese gegenüber dem Geschädigten im Falle von „Verletzungen" haftet. Beispielsweise wäre es denkbar, dass der Betreiber, der Hersteller oder eine andere Person hinter der Künstlichen Intelligenz dieses Haftungskapital aufbringen müssten, darüber hinaus aber nicht mit ihrem eigenen Vermögen haften. Auch eine Kapitalbereitstellung über eine entsprechende und dafür geschaffene Haftpflichtversicherung wäre denkbar. Hierdurch würde dann im technischen Sinne eine „Künstliche Intelligenz mit beschränkter Haftung" geschaffen. Das notwendige Haftungskapital könnte sich dabei an der spezifischen Autonomie und dem Gefahrenpotenzial der betreffenden Künstlichen Intelligenz orientieren.

Auch wenn diese beschränkte Haftung zunächst wie eine potenzielle Benachteiligung für Geschädigte wirkt: Haftungsbeschränkungen sind auch dem derzeitigen Produkthaftungsrecht nicht fremd. Und auch die theoretisch „unbeschränkte" Haftung eines Unternehmens nach der Produzentenhaftung kann in der Praxis mangels Haftungsmasse des Unternehmens zu Ausfällen bei dem Geschädigten führen. Versicherungen

---

[107] So hat die Bundesregierung am 16. Juni 2020 einen Gesetzesentwurf zur Bekämpfung von Unternehmenskriminalität verabschiedet, das „Gesetz zur Sanktionierung von verbandsbezogenen Straftaten", das sogenannte Verbandssanktionengesetz, „VerSanG".

[108] Vgl.bspw. Cornelius, MMR 2002, 353; Müller-Hengstenberg/Kirn, MMR 2014, 307.

könnten etwaige Haftungslücken schließen oder jedenfalls die Haftungssummen über das Haftungskapital einer Künstlichen Intelligenz mit beschränkter Haftung hinaus aufstocken. Wie ebenfalls bereits skizziert, könnte sich das jeweilige Haftungskapital auch an dem Autonomiegrad und Gefährdungspotenzial der betreffenden Künstlichen Intelligenz orientieren.

4.6.4 Fazit

Mit der fortschreitenden technischen Entwicklung und dem damit einhergehenden Zuwachs an Autonomie dürfte es nötig werden, einen geeigneten rechtlichen Status für Künstliche Intelligenz zu finden. So wird vertreten, dass nur die Umsetzung spezieller Vorschriften für Roboter geeignet bzw. angemessen sein wird.[109]

Es dürfte dabei nicht ausreichen, einzelne Sonderregelungen für autonome Roboter und andere Formen Künstlicher Intelligenz für verschiedene Rechtsgebiete einzuführen, um die (Rechts-)Fragen zu beantworten, die entstehen werden, wenn Künstliche Intelligenz mehr und mehr autonome Entscheidungen trifft. Solche Regelungen und Anpassungen würden zu einem Flickenteppich von Vorschriften führen.

Insbesondere mit Blick auf Haftungsfragen ist vielmehr ein kohärentes System zu entwickeln. Zwar lassen sich einige bekannte Haftungskonzepte auch auf Künstliche Intelligenz anwenden. Allerdings wird damit den Besonderheiten Künstlicher Intelligenz mitunter nicht hinreichend Rechnung getragen. Dies dürfte in Zukunft umso mehr gelten, je autonomer eine Künstliche Intelligenz handelt und eigene Entscheidungen trifft. Die gängigen Konzepte der Gefährdungs- und Verschuldenshaftung der Hersteller und Produzenten können hier in Zukunft an ihre Grenzen geraten. Je mehr dies der Fall ist, umso mehr ist eine „eigene" Haftung – und umso mehr eine eigene Rechtspersönlichkeit – Künstlicher Intelligenz zu erwägen. Dem sollte eine breite gesellschaftliche Diskussion vorausgehen – ist der Geist einmal aus der Flasche, wird man ihn nur noch schwerlich einfangen können.

5. KI-Verträge

5.1 Verträge für Künstliche Intelligenz

Das deutsche Vertragsrecht erlaubt bereits Verträge in Bezug auf Künstliche Intelligenz (z.B. Kauf, Verkauf, Miete, Leasing und Nutzung von Robotern oder Software). Es basiert auf der Vertragsfreiheit und gibt einige Einschränkungen, z.B. Verbote für Klauseln und Bedingungen, die eine Partei benachteiligen würden (z.B. § 305 ff. BGB). Aber keine sind speziell auf Verträge in Bezug auf Künstliche Intelligenz ausgerichtet.

[109] Beck, in: Hilgendorf/Günther, Robotik und Recht 2, Robotik und Gesetzgebung, S. 239–260.

Gegenwärtig sind die Vertragsparteien daher frei (oder besser gesagt gezwungen), für alle KI-spezifischen Fragen eigenständig vernünftige vertragliche Lösungen zu finden. Zu vertraglichen Haftungsregelungen siehe bereits oben, Abschnitt 2.3.4.

Da Künstliche Intelligenz gefährlich sein kann, gelten einige Einschränkungen. So dürfen beispielsweise Roboter für militärische Zwecke nicht von Privatpersonen erworben werden. Dies ist bereits durch allgemeine Bestimmungen, z.B. durch das Waffengesetz oder das Sprengstoffgesetz, verboten, wird aber wahrscheinlich an neue Entwicklungen angepasst werden, um eventuelle Gesetzeslücken zu schließen.

5.2 Durch Künstliche Intelligenz geschlossene Verträge

Verträge, die „durch Künstliche Intelligenz" abgeschlossen werden, sind ein kontroverses Thema.[110] Die rechtliche Diskussion um dieses Thema basiert auf der Frage, ob die Erklärung eines sogenannten Software-Agenten als Willenserklärung des Software-Agenten oder des Benutzers eingestuft werden kann.

Da der Software-Agent rechtlich gesehen kein Mensch ist, ist er derzeit nicht in der Lage, eine Willenserklärung abzugeben. Nichtsdestotrotz werden Software-Agenten immer autonomer, daher wird diskutiert, ob von Robotern abgegebene Erklärungen mit dem Benutzer assoziiert werden und somit zu Willenserklärungen werden sollen.

Bisher ist der gängigste Ansatz zu fragen, ob eine (elektronisch erzeugte) Computer-Erklärung dem Benutzer zugeordnet werden kann. Dabei wird vielfach argumentiert, dass der Benutzer direkt für die von der Software getroffene Entscheidung verantwortlich ist, da er zumindest die Rahmenbedingungen für eine von der Künstlichen Intelligenz getroffene Entscheidung und Erklärung bestimmt hat.[111]

Folglich sind Verträge, die von Software-Agenten geschlossen werden, derzeit nach deutschem Recht möglich, aber die Erklärungen, die sie abgeben, sind immer mit denen des Benutzers verbunden und werden als solche betrachtet.

Eine andere Lösung für den Einsatz von Software-Agenten kann der vorherige Abschluss eines Rahmenvertrags zwischen den Vertragsparteien sein (etwa bei der Registrierung für eine Dienstleistung), der bestimmte Rechtsfolgen an die Erklärungen eines Software-Agenten knüpft. Mit einem solchen Rahmenvertrag müssen die Erklärungen eines Software-Agenten weder echte Willenserklärungen im rechtlichen Sinne sein, noch müssen sie mit dem Benutzer des Software-Agenten in Verbindung gebracht werden, um ihren Zweck zu erreichen. Aufgrund der Vertragsfreiheit können die beteiligten Parteien einem solchen Verfahren zustimmen.

---

[110] Hengstenberg/Kirn in: Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems – Rechtliche Konsequenzen der „Verselbstständigung" technischer Systeme, MMR 2014, 307; Cornelius in: Vertragsschluss durch autonome elektronische Agenten, MMR 2002, 353; Bräutigam/Klindt in: Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137.

[111] Cornelius in: Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353; Hengstenberg/Kirn in: Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems-Rechtliche Konsequenzen der „Verselbstständigung" technischer Systeme.

Diese Ansätze können allerdings nicht alle Probleme lösen. So sind diese Lösungen nicht geeignet für Software, die in der Lage ist, aus früher getroffenen Entscheidungen zu lernen. Solche Software kann die Rahmenbedingungen von sich aus verändern. Jegliche Verantwortlichkeit für Erklärungen, die von einer solchen lernfähigen Software abgegeben werden, wäre ein unkalkulierbares Risiko.

Eine Idee für den rechtlichen Umgang mit solchen Softwaresystemen wäre es, die Erklärung als eine Erklärung der Software selbst zu betrachten und dann die Vorschriften für Vertreter darauf anzuwenden.[112] Voraussetzung für die Abgabe einer Willenserklärung ist allerdings das Bestehen einer Rechtsfähigkeit und (zumindest beschränkten) Geschäftsfähigkeit des Software-Agenten. Hieran scheitert dieser Ansatz derzeit. Zukünftig wäre es aber etwa denkbar, Software-Agenten einen mit juristischen Personen vergleichbaren Status einzuräumen (siehe im Einzelnen Ziffer 4.6.3).

[112] Sorge in: Softwareagenten, Vertragsschluss, Vertragsstrafe und Reuegeld, Seite 25.

Ihre Ansprechpartner

Dr. Andreas Lober
Rechtsanwalt
Andreas.Lober@advant-beiten.com
T: +49 69 756095-582

Susanne Klein
Rechtsanwältin | LL.M.
Fachanwältin für Informations-technologierecht
Susanne.Klein@advant-beiten.com
T: +49 69 756095-585

Dr. Christina Hackbarth
Rechtsanwältin
Christina.Hackbarth@advant-beiten.com
T: +49 89 35065-1432

Christian Hess
Rechtsanwalt | LL.M.
Fachanwalt für Gewerblichen Rechtsschutz
Christian.Hess@advant-beiten.com
T: +49 89 35065-1421

Dr. Peggy Müller
Rechtsanwältin
Peggy.Mueller@advant-beiten.com
T: +49 69 756095-582

Dr. Birgit Münchbach
Rechtsanwältin
Fachanwältin für Internationales Wirtschaftsrecht, Handels- und Gesellschaftsrecht und Informations-technologierecht
Birgit.Muenchbach@advant-beiten.com
T: +49 761 150984-22

Wojtek Ropel
Rechtsanwalt
Wojtek.Ropel@advant-beiten.com
T: +49 69 756095-582

Jason Komninos
Rechtsanwalt | LL.M.
Fachanwalt für Informations-technologierecht
Jason.Komninos@advant-beiten.com
T: +49 69 756095-585

advant-beiten.com

ADVANT member firm offices:
BEIJING | BERLIN | BRUSSELS | DUSSELDORF | FRANKFURT | FREIBURG | GENOA
HAMBURG | LONDON | MILAN | MOSCOW | MUNICH | PARIS | ROME | SHANGHAI

06/2023

Unsere Büros

BEIJING
Suite 3130 | 31st floor
South Office Tower
Beijing Kerry Centre
1 Guang Hua Road
Chao Yang District
100020 Beijing, China
beijing@advant-beiten.com
T: +86 10 85298110

BERLIN
Lützowplatz 10
10785 Berlin
Deutschland
berlin@advant-beiten.com
T: +49 30 26471-0

BRÜSSEL
Avenue Louise 489
1050 Brüssel
Belgien
brussels@advant-beiten.com
T: +32 2 6390000

DÜSSELDORF
Cecilienallee 7
40474 Düsseldorf
Postfach 30 02 64
40402 Düsseldorf
Deutschland
dusseldorf@advant-beiten.com
T: +49 211 518989-0

FRANKFURT
Mainzer Landstraße 36
60325 Frankfurt am Main
Deutschland
frankfurt@advant-beiten.com
T: +49 69 756095-0

FREIBURG
Heinrich-von-Stephan-Straße 25
79100 Freiburg im Breisgau
Deutschland
freiburg@advant-beiten.com
T: +49 761 150984-0

HAMBURG
Neuer Wall 72
20354 Hamburg
Deutschland
hamburg@advant-beiten.com
T: +49 40 688745-0

MOSKAU
Turchaninov Per. 6/2
119034 Moskau
Russland
moscow@advant-beiten.com
T: +7 495 2329635

MÜNCHEN
Ganghoferstraße 33
80339 München
Postfach 20 03 35
80003 München
Deutschland
munich@advant-beiten.com
T: +49 89 35065-0

Impressum
ADVANT Beiten
Beiten Burkhardt Rechtsanwaltsgesellschaft mbH
(Herausgeber)
Ganghoferstraße 33, 80339 München
AG München HR B 155350/ USt.-Idnr: DE-811218811
Weitere Informationen (Impressumsangaben) unter:
https://www.advant-beiten.com/de/impressum

REDAKTION (verantwortlich):
Dr. Andreas Lober, Susanne Klein

advant-beiten.com

ADVANT member firm offices:
BEIJING | BERLIN | BRUSSELS | DUSSELDORF | FRANKFURT | FREIBURG | GENOA
HAMBURG | LONDON | MILAN | MOSCOW | MUNICH | PARIS | ROME | SHANGHAI

06/2023