RECHT DER KÜNSTLICHEN INTELLIGENZ UND INTELLIGENTEN ROBOTIK

BEITEN BURKHARDT

RECHT DER KÜNSTLICHEN INTELLIGENZ UND INTELLIGENTEN ROBOTIK

BEITEN BURKHARDT

Vorbemerkung

Künstliche Intelligenz und Roboter dringen in unsere Industrie, Gesellschaft und unser Leben ein.

Mit diesem Buch wollen wir einen knappen Überblick über die aktuelle Rechtslage 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 Januar 2021.

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, Computerprogramme und Anwendungen umfasst.

Dr. Andreas Lober
Rechtsanwalt

Autoren

Dr. Andreas Lober
Susanne Klein
Wojtek Ropel
Dr. Florian Jäkel-Gottmann
Lennart Kriebel

Mitarbeit
Dr. Christina Hackbarth
Peter Tzschentke

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

© BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Alle Rechte vorbehalten 2021

Inhalt

1. Rahmenbedingungen

1.1 Wirtschaftliche Rahmenbedingungen

1.1.1 Initiativen

Im Jahr 2006 startete die Bundesregierung die Innovationsinitiative „Hightech-Strategie“[1]. Sie wurde durch die Initiative „High-Tech 2020“ ergänzt und zuletzt mit der „Hightech-Strategie 2025“ fortgeführt. Die Initiativen zielen darauf ab, Deutschland als einen der führenden Anbieter von Wissenschaft und Technologie in den Bereichen Klima, Energie, Gesundheit, Mobilität, Sicherheit und Kommunikation zu etablieren.

Unter dem Dach der Hightech-Strategie 2025 bündelt die Bundesregierung ressortübergreifend die Förderung von Forschung und Innovation aus insgesamt zwölf Themenfeldern („Missionen“)[2], darunter die Bereiche „Künstliche Intelligenz in die Anwendung bringen“, „Technik für den Menschen“ und „Eine sichere, vernetzte und saubere Mobilität“. Gefördert werden unter anderem der Aufbau von Kompetenzzentren für interaktive Assistenzrobotik[3] und KI-Kompetenzzentren[4], die Forschung von robotischen Assistenzsystemen für die medizinische Diagnostik und Pflege[5] oder KI Projekte zum Schutz von Umwelt, Klima und Ressourcen.[6]

Als wichtiger Bestandteil der Hightech-Strategie 2025 gilt auch die vom Bundesministerium für Wirtschaft und Energie (**BMWi**), dem Bundesministerium für Bildung und Forschung (**BMBF**) und dem Bundesministerium für Arbeit und Soziales (**BMAS**) ausgearbeitete und im November 2018 verabschiedete „Strategie Künstliche Intelligenz der Bundesregierung“, mit der Deutschland als Forschungsstandort für KI gestärkt und die Anwendung von KI in der Industrie, insbesondere bei kleinen und mittleren Unternehmen (**KMU**), gezielt gefördert werden soll.[7]

Im Juli 2019 veröffentlichte das BMBF zusammen mit dem BMWi und dem Bundesministerium für Verkehr und digitale Infrastruktur (**BMVI**) den Aktionsplan „Forschung für autonomes Fahren“. Mit diesem wurden Leitlinien und ein gemeinsamer Rahmen für die Forschung zum autonomen Fahren festgelegt.[8] Aktuelle Forschungsthemen sind unter anderem die Projekte „UNICARagil“ (Entwicklung vollständig fahrerloser elektrischer Fahrzeuge höchster Automatisierungsstufe, Förderungssumme: 26 Mio. Euro) und „IMAGinE“ (Entwicklung innovativer Assistenzsysteme für das „kooperative Fahren der Zukunft“, Förderungssumme: 17,9 Mio. Euro).

---

1 http://www.hightech-strategie.de/.
2 Eine Übersicht zu den Themenfeldern findet sich unter: https://www.hightech-strategie.de/de/missionen-1725.html.
3 https://www.technik-zum-menschen-bringen.de/foerderung/bekanntmachungen/ra3.
4 https://www.bmbf.de/de/kuenstliche-intelligenz-mehr-geld-fuer-die-forschung-9518.html.
5 https://www.dlr.de/rm/desktopdefault.aspx/tabid-12535/21858_read-50007/.
6 https://www.z-u-g.org/aufgaben/ki-leuchttuerme/.
7 https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-der-bundesregierung.pdf?__blob=publicationFile&v=8.
8 https://www.bmbf.de/upload_filestore/pub/Aktionsplan_Forschung_fuer_autonomes_Fahren.pdf.

Die EU startete 2014 das Programm „Horizon 2020“[9]. Es ist das größte Forschungs- und Innovationsprogramm der EU mit knapp 80 Mrd. Euro Fördermitteln über sieben Jahre bis 2020 und dient der Förderung von Innovationen aller Art. Es ist Teil der Initiative „Europa 2020“[10], die die globale Wettbewerbsfähigkeit Europas sichern soll. Das „ESMERA Project“, welches KMU dabei unterstützt, Robotik-Lösungen zu entwickeln und auf den Markt zu bringen, ist Teil dieses Programms.[11]

Bereits im April 2015 gaben zudem das BMWi und BMBF gemeinsam[12] den Start der Plattform „**Industrie 4.0**“ bekannt.[13] Diese Plattform ist ein Zusammenschluss von Vertretern aus Politik, Wirtschaft, Verbänden, Wissenschaft und Gewerkschaften[14] mit dem Ziel, die Position Deutschlands als eine der führenden Industrienationen durch die und im Zuge der sogenannten „vierten industriellen Revolution“ zu sichern.

Die EU hat im Rahmen ihrer neuen Digitalstrategie auch Maßnahmen für den Bereich KI angekündigt.[15] In den nächsten zehn Jahren sollen dafür Investitionen von mehr als 20 Milliarden Euro pro Jahr für KI-Technologie bereitgestellt werden. Im Februar 2020 veröffentlichte die Europäische Kommission zudem einen „Bericht über die Auswirkungen Künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung“[16] sowie ein White Paper „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“.[17] Dieses behandelt den politischen und wirtschaftlichen Rahmen des Einsatzes von KI sowie Haftungs- und Sicherheitsfragen.

1.1.2 Finanzausstattung

Im Mai 2019 kündigte die Bundesregierung an, die Förderung Künstlicher Intelligenz mit jeweils zusätzlichen 500 Mio. Euro in den Jahren 2019 und 2020 zu fördern.[18] Der Bund plant, bis einschließlich 2025 etwa 3 Mrd. Euro für die Umsetzung der „Strategie Künstliche Intelligenz der Bundesregierung“ bereitzustellen.[19]

---

9 https://ec.europa.eu/programmes/horizon2020/.
10 http://ec.europa.eu/europe2020/index_en.htm.
11 http://www.esmera-project.eu.
12 http://www.bmwi.de/DE/Presse/pressemitteilungen,did=701050.html.
13 Der Begriff „Industrie 4.0“ beschreibt die weitgehende Digitalisierung und Vernetzung der industriellen Produktion und fasst die jüngst diskutierten Themen Internet der Dinge, Cloud Computing, Big Data und Smart Factory zusammen.
14 Unter der Leitung von Bundeswirtschaftsminister Sigmar Gabriel, Bundesforschungsministerin Johanna Wanka, Spitzenvertretern aus Industrie und Verbänden, der Industriegewerkschaft Metall und des Fraunhofer-Instituts.
15 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_de.
16 https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_de.pdf.
17 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf.
18 https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2019/20190523-bundesregierung-staerkt-die-foerderung-kuenstlicher-intelligenz.html.
19 https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-der-bundesregierung.pdf?__blob=publicationFile&v=8.

Daneben hat das BMWi verschiedene weitere Förderprogramme im Bereich der Robotik und autonomen Systeme („RAS") aufgelegt, darunter „Autonomik für Industrie 4.0",[20] „Smart Service Welt"[21] und „PAiCE".[22]

Das Technologieprogramm „Autonomik für Industrie 4.0" zielte darauf ab, die Entwicklung von Maschinen, Robotern und anderen Systemen der nächsten Generation zu unterstützen, die in der Lage sind, alle Arten von Aufgaben autonom zu bewältigen. Es verfügte über ein Budget von 40 Mio. Euro, das Unternehmen und Forschungseinrichtungen in den Jahren 2013 bis 2017 zur Verfügung stand. Abgelöst wurde es durch das Förderprogramm „PAiCE" für digitale Technologien in der Industrie, welches bis zum Jahr 2021 ein Budget von etwa 50 Mio. Euro für innovative Ansätze in den Bereichen Produktion, Logistik, industrielle 3D-Technologien und Servicerobotik bereitstellt.

Die Förderprogramme „Smart Service Welt" (2016 bis 2019) und „Smart Service Welt II" (2019 bis 2021) sollen Pilotprojekte für intelligente Dienste aus verschiedenen Sektoren, etwa Medizin, Mobilität, Produktion oder Energie, mit einem Finanzbudget von jeweils 50 Mio. Euro fördern.

Auf dem Gebiet der intelligenten Autos und des autonomen Fahrens fördert das BMWi mit dem Programm „Neue Fahrzeug- und Systemtechnologien".[23] Dieses ist mit einer jährlichen Förderungssumme von 60 Mio. Euro ausgestattet. Die Schwerpunkte liegen dabei in den Bereichen „Automatisiertes und vernetztes Fahren" sowie „Innovative Fahrzeuge". Insgesamt fördert das BMBF Projekte zum automatisierten und vernetzten Fahren mit rund 100 Mio. Euro.[24]

1.2 Technische Rahmenbedingungen von Robotern

Initiativen deutscher Institutionen, darunter die oben beschriebenen (vgl. Ziffer 1.1.1), zielen darauf ab, relevante Standards für die Industrie zu schaffen.

Standards können es Robotern erleichtern, mit anderen Robotern und Geräten über standardisierte Schnittstellen (sowohl angebundene als auch drahtlose) in Maschinensprache zu interagieren.

Zuverlässige Standards für die Industrie sind auch von Vorteil, um Investitionen in neue Technologien für Industriezweige zu sichern, in denen solche Investitionen regelmäßig die Interoperabilität mit anderen Maschinen erfordern und Amortisationszeiten von mehreren Jahren umfassen.

Bislang gibt es jedoch noch keine umfassende technische Standardisierung.

---

20 https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AbgeschlosseneProgramme-Projekte/Autonomik-fuer-Industrie40/autonomik-industrie-40.html.
21 https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/smart-service-welt.html.
22 http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/paice-broschuere.pdf?__blob=publicationFile&v=2.
23 https://www.bmwi.de/Redaktion/DE/Artikel/Technologie/fahrzeug-und-systemtechnologien.html.
24 https://www.bmbf.de/de/automatisiertes-fahren-4158.html.

Einige Definitionen finden sich in der von der Internationalen Organisation für Normung (**ISO**) herausgegebenen Normungsdokumentation.[25]

Die ISO veröffentlichte 2012 ein Normungspapier zur Terminologie im Zusammenhang mit Robotern und robotischen Geräten.[26] Nach diesem Normungspapier ist ein „**Roboter**" definiert als „ein in zwei oder mehr Achsen[27] mit einem gewissen Grad an Autonomie programmierbarer Betätigungsmechanismus, der sich innerhalb seiner Umgebung bewegt, um die vorgesehenen Aufgaben auszuführen". Autonomie ist hierbei definiert als „die Fähigkeit, beabsichtigte Aufgaben auf der Grundlage des aktuellen Zustands und der Sensorik ohne menschliches Eingreifen auszuführen".

Neben der Differenzierung zwischen dem Roboter und dem „**Robotikgerät**"[28] unterscheidet das Papier vor allem – abhängig vom Verwendungszweck – zwischen dem Industrieroboter und dem Serviceroboter und definiert den Begriff des intelligenten Roboters. Diese Begriffe werden in der Literatur und auch von der International Federation of Robotics (**IFR**) häufig verwendet.[29]

Der „**Industrieroboter**" wird definiert als ein „automatisch gesteuerter, reprogrammierbarer Mehrzweckmanipulator, programmierbar in drei oder mehr Achsen, der entweder fest installiert oder mobil für den Einsatz in industriellen Automatisierungsanwendungen eingesetzt werden kann".

Der „**Serviceroboter**" hingegen ist definiert als „Roboter, der nützliche Aufgaben für Menschen oder Geräte ausführt, ausgenommen Anwendungen der Industrieautomation".

Ferner definiert das Papier einen „**intelligenten Roboter**" als „Roboter, der in der Lage ist, Aufgaben auszuführen, indem er seine Umgebung wahrnimmt und/oder mit externen Quellen interagiert und sein Verhalten anpasst".

1.3 Bestehender rechtlicher Rahmen

Gegenwärtig gibt es (noch) keinen konkreten und eigens für Künstliche Intelligenz geschaffenen rechtlichen Rahmen. Künstliche Intelligenz verfügt derzeit auch nicht über eine eigene Rechtspersönlichkeit, anhand deren ihr Rechte und Pflichten zuerkannt würden. Vor allem gibt es aktuell noch keine eigenständige Haftung Künstlicher Intelligenz.

Wichtige Regelungen im Zusammenhang mit Künstlicher Intelligenz sind jedoch in folgenden Gesetzen zu finden:

---

25 Weltweite Vereinigung nationaler Normungsorganisationen, gegründet 1947 (http://www.iso.org/).

26 ISO 8373:2012, Roboter und robotische Geräte – Vokabular. (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=55890).

27 Dem Papier zufolge „umfasst ein Roboter das Steuerungssystem und die Schnittstelle des Steuerungssystems".

28 „Ein aktivierter Mechanismus, der die Merkmale eines Industrie- oder eines Serviceroboters erfüllt, dem entweder die Anzahl programmierbarer Achsen oder der Grad der Autonomie fehlt".

29 Internationale Organisation der Robotikindustrie und -forschungsinstitute aus über 15 Ländern, gegründet 1987 (http://www.ifr.org/).

- Bürgerliches Gesetzbuch (**BGB**)
- Strafgesetzbuch (**StGB**)
- Produkthaftungsgesetz (**ProdHaftG**)
- Datenschutz-Grundverordnung (**DSGVO**)
- Bundesdatenschutzgesetz (**BDSG**)
- Telemediengesetz (**TMG**)
- Gesetz gegen den unlauteren Wettbewerb (**UWG**)
- Gesetz zum Schutz von Geschäftsgeheimnissen (**GeschGehG**)
- Gesetz über Urheberrecht und verwandte Schutzrechte (**UrhG**)
- Patentgesetz (**PatG**)
- Designgesetz (**DesignG**)
- Gebrauchsmustergesetz (**GebrMG**)
- Markengesetz (**MarkenG**)
- Gesetz über Medizinprodukte (**MPG**)
- Gesetz zur Durchführung unionsrechtlicher Vorschriften betreffend Medizinprodukte (**MPDG**)
- Verordnung (EU) 2017/745 über Medizinprodukte (**MP-VO**)
- Luftverkehrsgesetz (**LuftVG**)
- Luftverkehrs-Ordnung (**LuftVO**)
- Rechtsakt zur Cybersicherheit (**Cybersecurity Act**)
- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (**IT-Sicherheitsgesetz**)
- Straßenverkehrsgesetz (**StVG**)
- Versicherungsvertragsgesetz (**VVG**)

Das Europäische Parlament (**EU-Parlament**) und die Europäische Kommission (**EU-Kommission**) haben sich intensiv mit den Themen KI und Robotik befasst. Das EU-Parlament forderte 2017 in einer Empfehlung an die Kommission[30] unter anderem die Schaffung gemeinsamer unionsweiter Begriffsbestimmungen für KI und Robotik und die Einführung eines EU-Registrierungssystems für fortschrittliche Roboter sowie ggf. einer Europäischen Agentur für Robotik und Künstliche Intelligenz. Zudem stellte das EU-Parlament hier Erwägungen zu verschiedenen rechtlichen Aspekten der Robotik (Haftung, Datenschutz, Versicherungspflichten), ethischen Grundsätzen und Verhaltenskodizes für Robotikingenieure an. Die EU-Kommission hat im Jahr 2019 „Ethik-Leitlinien für eine vertrauenswürdige KI"[31] vorgelegt. Eine vertrauenswürdige Künstliche Intelligenz muss demnach (1.) rechtmäßig und in Übereinstimmung mit den Gesetzen handeln, (2.) ethische Grundsätze einhalten und (3.) in technischer und sozialer Hinsicht robust und verlässlich sein. Einem Menschen soll stets eindeutig bewusst gemacht werden, wenn er es mit einem KI-System zu tun hat. Zuletzt hat die EU-Kommission ein Whitepaper zur Künstlichen Intelligenz[32] und einen Bericht über die Auswirkungen von Künstlicher Intelligenz und Robotik auf die (Produkt-)Haftung[33] vorgelegt. Das EU-Parlament hat jüngst den Entwurf einer Verordnung zur Haftung von Betreibern von „KI-Systemen" an die EU-Kommission übermittelt, die damit nun aufgefordert ist, einen entsprechenden Rechtsakt vorzuschlagen (wozu sie freilich nicht verpflichtet ist).[34]

Die vorstehenden Veröffentlichungen geben bereits eine erste Vorstellung davon, wie ein zukünftiger europäischer Rechtsrahmen für Künstliche Intelligenz ausgestaltet werden könnte.

Einen Ausblick darauf, wie die Rechtsstellung Künstlicher Intelligenz in Zukunft aussehen könnte, geben wir ab Ziffer 2.6.

---

30 Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)).

31 https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

32 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf.

33 https://ec.europa.eu/info/sites/info/files/report-safety-liability-artificial-intelligence-feb2020_de.pdf.

34 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)).

2. 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 zu den meistdiskutierten rechtlichen Themen bei KI.

2.1 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 für die gesetzliche 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.

2.2 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**.

2.2.1 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 durch ein Produkt erlitten hat, also zunächst nachweisen, dass diese Schäden auf ein vorsätzliches oder fahrlässiges und zugleich rechtswidriges Verhalten des Herstellers zurückzuführen sind.

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. 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.

2.2.2 Gefährdungshaftung

Die 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.[35] 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. 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 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.[36]

2.3 Anwendung auf Künstliche Intelligenz

2.3.1 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.[37]

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).

---

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

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

37 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.

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.[38]

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.[39] Vielmehr können sich Schäden durch Künstliche Intelligenz als Ergebnis fehlerhafter Software, durch die Software erlernter Erfahrungen, 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 werden. Bei Künstlicher Intelligenz und autonomen Systemen stellen sich neuartige Fragen. Autonome Fahrzeuge, die einen Unfall verursachen, werden häufig diskutiert.[40]

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[41] oder Verletzungen von geistigem Eigentum durch Künstliche Intelligenz in viralem Marketing.

2.3.2 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[42] 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

---

38 Vgl. Bräutigam/Klindt, NJW 2015, 1137, 1139.

39 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."

40 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.

41 Algorithmic Decision Making.

42 Hersteller nach dem Produkthaftungsgesetz ist, wer das Endprodukt in Verkehr bringt.

„zusammengesetzten" Produkten aus Hard- und Software wie beispielsweise autonomen Fahrzeugen dies naturgemäß anders beurteilen mögen.[43] 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.[44] 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**:[45] Grundsätzlich ist das Inverkehrbringen eines Produkts der relevante Zeitpunkt für die Frage, ob der Hersteller pflichtgemäß gehandelt hat. Wird das Produkt hiernach weiterentwickelt bzw. schreitet die Entwicklung vergleichbarer Produkte allgemein voran, begründet das „schlechtere" frühere Produkt 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, desto intensiver kann die Produktbeobachtungspflicht sein. Wirkt Künstliche Intelligenz mit Systemen Dritter zusammen, könnte sich eine Produktbeobachtungspflicht auch auf die Beobachtung dieses Zusammenwirkens beziehen – jedenfalls in einem angemessenen Rahmen.

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.[46]

---

[43] 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.

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

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

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

2.3.3 Anwenderhaftung

Ein weiteres Feld ist die Haftung der Anwender von Künstlicher Intelligenz. 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.

2.3.4 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 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.

2.3.5 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 mehr ein System unabhängig 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).

2.4 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.

2.4.1 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).[47]

2.4.2 Whitepaper der EU-Kommission Februar 2020

Auch die EU-Kommission prüft die Anpassung geltender Rechtsvorschriften wie beispielsweise der Produkthaftungsrichtlinie.[48] Hierzu hat sie im Februar 2020 ein Whitepaper veröffentlicht, das auch die Erkenntnisse der Expertengruppe aus 2019 berücksichtigt.[49]

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.[50] Diese Risiken[51] 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,[52] werden Anforderungen anhand bestimmter Schlüsselmerkmale diskutiert.[53] Auch Unklarheiten über Zuständigkeiten einzelner Wirtschaftsteilnehmer in der Lieferkette sollen minimiert werden.[54]

---

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

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

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

50 EU-Kommission Whitepaper, S. 16.

51 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".

52 EU-Kommission Whitepaper, S. 20 f.

53 EU-Kommission Whitepaper, S. 22 ff.

54 EU-Kommission Whitepaper, S. 16.

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.[55] In diese Richtung ging auch das Europäische Parlament schon 2017. Dieses 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".[56]

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 rechtlichen Möglichkeiten im nationalen Recht (wie in Deutschland möglicherweise die Produzentenhaftung).[57]

Diese Tendenzen lassen derzeit vermuten, dass bekannte Mechanismen, insbesondere das Produkthaftungsrecht, fortgesetzt zur Anwendung kommen dürften – wenn auch an einigen Stellen modifiziert für Besonderheiten der Künstlichen Intelligenz. Insoweit ist zu fordern, dass das künftige Haftungsregime kohärent ausgestaltet wird und nicht zu einer weiteren Zersplitterung der Rechtsordnung führt. Abzuwarten bleibt zudem, wie zukunftssicher das künftige Haftungsregime ausgestaltet wird und nicht ob, sondern wann bereits der nächste Bedarf für weitergehende Änderungen entstehen wird.

2.4.3 Verordnungsentwurf des EU-Parlaments zur Haftung von KI-Betreibern 2020

Das EU-Parlament hat der EU-Kommission im Oktober 2020 einen Regelungsvorschlag zur Haftung von Betreibern Künstlicher Intelligenz unterbreitet.[58] 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.

---

55 EU-Kommission Whitepaper, S. 16.

56 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").

57 EU-Kommission Whitepaper, S. 27.

58 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)).

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 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.

2.5 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.[59] 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. Für kleine Drohnen sind Versicherungen in Deutschland hingegen bereits verfügbar (und auch obligatorisch). Sie decken in der Regel auch autonome Flugbetriebsarten ab. Insbesondere Mähroboter scheinen zudem das Portfolio von Versicherern erweitert zu haben. Über diese plastischen Beispiele hinaus sind viele Anwendungen von Künstlicher Intelligenz derzeit noch so individuell und einem stetigen Wandel unterworfen, dass es hierfür keine Standardprodukte von Versicherern gibt. Zusätzlich können Versicherer aber auch bereits vor Eintritt von Haftungsfällen, nämlich im Rahmen der Risikoeinschätzung und Schadensvermeidung, eine Rolle spielen.[60]

Diskutiert wird die Frage einer Pflichtversicherung. Für Fahrzeuge gibt es aufgrund deren abstrakter Gefährlichkeit und der potenziell hohen Schäden bereits seit langem Pflichthaftpflichtversicherungen. 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."[61] 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.[62] Zusätzlich erwog das EU-Parlament einen Versicherungsfonds für Schäden, für die kein Versicherungsschutz besteht.[63]

In seinem aktuellen Entwurf einer Verordnung zur Haftung der Betreiber von „KI-Systemen"[64] (s. oben Ziffer 2.4.3) hat sich das EU-Parlament nun gegen einen „mit öffentlichen Mitteln finanzierten Entschädigungsmechanismus auf Unionsebene" ausgesprochen. Das Parlament hat

---

59 Ebert, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 16 Rn. 6, 28 ff.
60 Ebert, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 16 Rn. 41.
61 Expert Group on Liability and New Technologies – New Technologies Formation, Liability for Artificial Intelligence and other emerging technologies, 20119, dot:10 2838/573689, Key Finding No. 33.
62 EU-Parlament, Entschließung 2015/2103, Ziffer 57.
63 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.
64 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)).

jedoch die Kommission aufgefordert, diese solle „eng mit dem Versicherungsmarkt zusammenarbeiten, um innovative Versicherungsprodukte zu entwickeln, mit denen die Versicherungslücke geschlossen werden kann." Der Verordnungsentwurf 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.

2.6 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 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 2.6.3 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.

2.6.1 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.[65] 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

[65] 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.

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.[66]

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. 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 Tonnen 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,[67] also eine Art „Haftungspersönlichkeit" (hierzu sogleich auch Ziffer 2.6.3).

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 mehr auch von ihrem jeweiligen Input, von ihren „Erlebnissen" geprägt werden. Dieser Input wird üblicherweise dem Hersteller entzogen sein. Neuronale Netze beruhen auf dem Prinzip von „try and error". Je mehr sich Deep

---

66 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.

67 Schirmer, JZ 2019, 17.

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.

2.6.2 Insbesondere: Haftung intelligenter oder autonomer 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. 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.

2.6.3 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 nicht in der Form existiert, in der sie zu existieren scheint (d. h. als Person im eigentlichen Wortsinn), jedoch in ihrer Wirkung teilweise 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. Das Strafrecht soll jedoch in gewissem Umfang auf juristische Personen ausgedehnt werden („Unternehmensstrafrecht").[68]

---

[68] 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".

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

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.[69] 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 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.

2.6.4 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.[70]

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

---

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

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.

3. Geistiges Eigentum und gewerbliche Schutzrechte

Geistiges Eigentum und gewerbliche Schutzrechte sind relevant, wenn es um den Schutz oder die Schutzfähigkeit der KI-Technologie geht – aber auch für den Schutz von durch Künstliche Intelligenz geschaffenen Arbeitsergebnissen.

3.1 Schutz der KI-Technologie

Die KI-Technologie unterscheidet sich nicht grundlegend von anderen Technologien. Alle Arten von geistigen und gewerblichen Schutzrechten können Anwendung finden.

3.1.1 Schutz durch Patente und Gebrauchsmuster

Das deutsche Patentgesetz (**PatG**) schützt nur neue technische Erfindungen und unterscheidet zwischen dem Recht an einer Erfindung, dem Recht auf das Patent, dem Recht auf Erteilung des Patents und den Rechten aus dem Patent.

Das Patentrecht ist auf EU-Ebene noch nicht harmonisiert. Dies könnte sich jedoch in naher Zukunft ändern. Ein europäisches Patent mit einheitlicher Wirkung befindet sich derzeit in einem fortgeschrittenen Stadium der Verabschiedung bzw. Einführung in den Mitgliedstaaten der EU.[71]

Derzeit gilt noch das 1973 verabschiedete Europäische Patentübereinkommen (**EPÜ**).[72] Danach werden Patente durch ein Verfahren beim Europäischen Patentamt (**EPA**) erteilt. Wird das Patent vom EPA erteilt, gewährt es in jedem benannten EPÜ-Land die gleichen Rechte, wie sie das nationale Patentrecht gewähren würde.

Die Voraussetzung für das Entstehen der geschützten Rechte ist neben der Neuheit eine technische Erfindung (§ 1 Abs. 1 PatG). Was dies umfasst, wird nicht positiv definiert, allerdings enthält das Gesetz Angaben darüber, was nicht geschützt wird (§ 1 Abs. 3 PatG).

Keine technischen Erfindungen sind dabei in der Regel:[73]

- Entdeckungen (Auffindung von etwas Vorhandenem, z. B. Magnetismus, Röntgen-Strahlen);
- wissenschaftliche Theorien;
- mathematische Methoden;
- ästhetische Formschöpfungen (hier käme Designschutz in Frage);

---

71 Verordnung (EU) Nr. 1257/2012 vom 17. Dezember 2012 und Verordnung (EU) Nr. 1260/2012 des Rates vom 17. Dezember 2012.

72 Ein Abkommen aus dem Jahr 1973 zwischen Österreich, Belgien, der Schweiz, Zypern, Deutschland, Dänemark, Spanien, Finnland, Frankreich, Griechenland, Irland, Italien, Liechtenstein, Luxemburg, Monaco, den Niederlanden, Portugal, Schweden, der Türkei und dem Vereinigten Königreich.

73 https://www.dpma.de/patente/patentschutz/schutzvoraussetzungen/index.html.

- Pläne, Regeln und Verfahren für gedankliche Tätigkeiten, für Spiele oder für geschäftliche Tätigkeiten;

- Programme für Datenverarbeitungsanlagen und die Wiedergabe von Informationen.

Im Bereich der KI ist vor allem relevant, dass reine Computerprogramme „als solche" grundsätzlich nicht patentierbar sind, dafür aber sogenannte „computerimplementierte Erfindungen". Die Abgrenzung ist im Einzelfall schwierig. Eine erste Orientierung bietet die vom Deutsche Patent- und Markenamt (**DPMA**) eingerichtete Informationsseite zum Thema.[74]

Die Erfindung neuer Roboter oder robotischer Systeme kann daher durch ein Patent schützbar sein, bei der reinen KI-Software ist dies weniger naheliegend.

Eine Erfindung ist nur dann neu, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik umfasst alle Kenntnisse, die vor der Anmeldung der betreffenden Erfindung weltweit in irgendeiner Weise der Öffentlichkeit zugänglich waren. Dies kann unter anderem durch Beschreibungen, Benutzung oder Ausstellung der Fall sein.

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 an Dritte mit starken Geheimhaltungsvereinbarungen absichern.

Wie das Patent setzt das Gebrauchsmuster – oft als „kleiner Bruder" des Patents bezeichnet – eine gewerblich nutzbare, neue technische Erfindung voraus. Die Einschränkungen in Bezug auf den Schutz von Software als solcher gelten also auch hier. Anders als beim Patent werden die sachlichen Schutzvoraussetzungen nicht vor der Eintragung geprüft. Auf europäischer Ebene gibt es den Gebrauchsmusterschutz nicht.

3.1.2 Halbleiter

Nach dem Halbleiterschutzgesetz (**HalblSchG**)[75] 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.[76]

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.[77]

---

74 https://www.dpma.de/patente/patentschutz/schutzvoraussetzungen/schutz_computerprogramme/index.html.
75 Umsetzung der Europäischen Richtlinie 87/54/EWG.
76 Klett/Sonntag/Wilske, Intellectual Property Law in Germany, Seite 51.
77 Richtlinie 87/54/EWG des Rates vom 16. Dezember 1986 über den Rechtsschutz der Topographien von Halbleitererzeugnissen.

3.1.3 Urheberrecht und eingetragene Geschmacksmuster bzw. Designs

Das deutsche Gesetz über Urheberrecht und verwandte Schutzrechte (**UrhG**)[78] 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 beim Register beantragt werden. Das Gesetz erstreckt sich nicht nur auf eigenschöpferische Werke wie Kunstwerke oder musikalische Darbietungen, sondern auch auf Computerprogramme und Datenbanken (siehe nachfolgende Ziffer 4.2 für weitere Einzelheiten zu Datenbanken). Es ist daher für den Schutz von KI in allen Ausprägungen hoch relevant.

Das deutsche Urheberrecht ist teilweise harmonisiert und wurde mehrfach geändert und angepasst, um rechtliche Vorgaben europäischer Richtlinien umzusetzen.

Der Geschmacksmusterschutz nach dem deutschen Gesetz über den Schutz von Mustern und Modellen (jetzt: Designgesetz – **DesignG**) ist dem Schutz des Urheberrechts sehr ähnlich. Ein wesentlicher Unterschied zum Schutz des Urheberrechts besteht allerdings darin, dass für den Schutz von Geschmacksmustern eine Eintragung des Geschmacksmusters erforderlich ist, § 27 DesignG. Ein schutzfähiges Geschmacksmuster liegt bei zweidimensionalen Mustern oder dreidimensionalen Modellen vor, welche eine Neuheit darstellen und Eigenart besitzen. Das schutzfähige Muster oder Modell kann sich nur auf ein Erzeugnis beziehen. 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, neu gefasst als Designverordnung vom 2. Januar 2014.[79]

3.1.4 Marken

Künstliche Intelligenz, die kommerziell vertrieben wird, kann durch Marken geschützt werden. Marken dienen als Herkunftshinweis für den Hersteller..

In Deutschland können Marken nach dem Gesetz über den Schutz von Marken und sonstigen Kennzeichen (**MarkenG**) beim Deutschen Patent- und Markenamt (**DPMA**) eingetragen werden. Marken sind nur dann eintragungsfähig, wenn sie bestimmte Voraussetzungen erfüllen, z. B. dass das Zeichen unterscheidungskräftig und nicht rein beschreibend ist. Neben Wortmarken und Bildmarken können auch andere Zeichen geschützt werden, darunter Hörmarken, dreidimensionale Gestaltungen, die Form der Ware oder ihrer Verpackung sowie sonstige Umhüllungen, einschließlich Farben und Farbkombinationen, § 3 MarkenG.

---

[78] 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).

[79] BGBl. I, S. 18.

Nicht eingetragene Marken können sind geschützt, wenn der Inhaber nachweisen kann, dass die Marke allgemein bekannt geworden ist, § 4 Nr. 2 MarkenG. Die Hürden dafür sind hoch.

Schutz kann auch durch die Eintragung einer Marke als Gemeinschaftsmarke/Unionsmarke beim Amt der Europäischen Union für geistiges Eigentum Harmonisierungsamt für den Binnenmarkt (**EUIPO**) – früher: Harmonisierungsamt für den Binnenmarkt – oder durch eine internationale Registrierung bei der Weltorganisation für geistiges Eigentum (**WIPO**) erlangt werden. Die Eintragung als Unionsmarke gewährt Schutz in allen Mitgliedstaaten der Europäischen Union.

Marken werden für bestimmte Waren und Dienstleistungen eingetragen, die wiederum verschiedenen Klassen zugeordnet sind. Software fällt beispielsweise in Klasse 9 der sog. Nizza-Klassifikation.

Je nach Funktionalität und Verwendung kann auch eine andere Klassifizierung in Betracht kommen, beispielsweise wenn die Künstliche Intelligenz in ein bestimmtes Gerät eingebaut ist. Die Schutzfähigkeit dreidimensionaler Gestaltungen ist für die Abrundung des Schutzes von Robotern interessant, wenn diese eine charakteristische Formensprache aufweisen. Die Voraussetzungen einer Schutzfähigkeit sind aber nicht leicht zu erfüllen (§ 8 MarkenG).

3.1.5 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.

Das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (**TRIPS**)[80] fordert die Einführung eines Mindestschutzstandards für Informationen mit wirtschaftlichem Wert. Alle Mitgliedstaaten, wie auch die Europäische Union als Ganzes, haben sich an dieses Abkommen gebunden.

Die Europäische Union hat am 8. Juni 2016 die Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung erlassen.[81]

[80] Abkommen von 1994, umgesetzt im Allgemeinen Zoll- und Handelsabkommen (GATT) https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

[81] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0943&from=DE.

In Deutschland wurde die Richtlinie mit dem Gesetz zum Schutz von Geschäftsgeheimnissen (**GeschGehG**) umgesetzt. Das „Geschäftsgeheimnis" ist definiert als 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) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und*
>
> *c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht.*"

Unternehmen müssen nun also „*angemessene Geheimhaltungsmaßnahmen*" (etwa rechtlicher, technischer und organisatorischer Art) ergreifen, wenn sie Informationen als Geschäftsgeheimnis nach der neuen Rechtslage schützen wollen. Informationen können den Geheimnisschutz damit auch jederzeit wieder verlieren.

Neben dem GeschGehG bestehen in Deutschland auch einige Sonderregelungen in anderen Gesetzen, insbesondere im Strafgesetzbuch.[82] 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.

3.2 Schutz der von Künstlicher Intelligenz geschaffenen Arbeitsergebnisse

Künstliche Intelligenz kann Arbeitsergebnisse schaffen, die durch geistige Eigentumsrechte geschützt werden könnten, wenn sie von Menschen produziert würden, wie z. B. Software, Datenbanken, Musik, Grafiken, Texte und sogar andere Künstliche Intelligenz.

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 de Edmond de Belamy. Auf breiter Ebene wird mit KI experimentiert, teilweise auch provoziert – von Gebrauchstexten über Gedichte bis hin zu einfachen Computerspielen. 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.

Nach geltendem Recht ist es Künstlicher Intelligenz jedoch nicht möglich, geistiges oder gewerbliches Eigentum zu besitzen. Auch Roboter werden nur als Sachen betrachtet und daher nur als Werkzeuge angesehen, die von Menschen bedient werden, nicht als Inhaber von Rechten (vgl. obige Ziffer 1.3 und Ziff. 2.6.1.

---

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

Weniger eindeutig ist jedoch, 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 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.

Von einer Künstlichen Intelligenz geschaffene Zeichen können unproblematisch von Menschen oder juristischen Personen als Marken eingetragen werden.

Schwieriger ist dagegen die Situation bei Erfindungen (Patentgesetz und Gebrauchsmustergesetz)sowie urheberechtlichen Werken: Bei Patenten wird jede Erfindung nach dem Zuordnungsgrundsatz dem Erfinder zugeordnet.[83] Die Rechtfertigung für eine solche Zuweisung ist die schöpferische Leistung einer kreativen Persönlichkeit.[84] Daher kann weder eine juristische Person noch ein Computerprogramm nach dem Patentrecht ein Erfinder sein.[85] Wenn eine Erfindung mit Hilfe von Computersoftware gemacht wird, gilt die natürliche Person als Erfinder, die das Programm geschaffen, die Ergebnisse ausgewertet und festgestellt hat, dass dies die Lösung für ein Problem darstellt.[86]

Gleiches gilt für Gebrauchsmuster, die ebenfalls eine Erfindung voraussetzen. Der Gebrauchsmusterschutz kann daher dem Menschen nur aus den gleichen Gründen gewährt werden.

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.

Um durch das Urheberrecht geschützt zu werden, muss ein Werk das Ergebnis des geistigen Schaffensprozesses sein, § 2 Abs. 2 UrhG. Dies kann nur von einem Menschen erfüllt werden, wenn auch mit Hilfe von Maschinen und Computern.

Der Schutz eines Geschmacksmusters setzt voraus, dass eine natürliche Person ein solches Geschmacksmuster geschaffen hat, das die Verwirklichung einer schöpferischen Idee darstellt.[87]

Geistiges Eigentum, das sich aus den Handlungen einer Künstlichen Intelligenz ergibt, ist damit entweder überhaupt nicht geschützt oder wird als ein Werk der Person angesehen, die die Künstliche Intelligenz bedient hat. Für derartige Arbeitsergebnisse gar keinen Schutz zu gewähren, erscheint jedenfalls auf den ersten Blick als unbefriedigend. Sie einer natürlichen Person zuzuschreiben, bereitet dagegen ebenfalls Schwierigkeiten. In Betracht kommen hier beispielsweise:

- der Schöpfer des Computerprogramms als „Herz" der KI – wohl aber insbesondere, wenn die Arbeitsergebnisse der KI im Computerprogramm bereits auch in kreativer Hinsicht „angelegt" sind, was (insbesondere bei autonomen künstlichen Intelligenzen) nur selten der Fall sein wird;

---

83 Mellulis in: Benkard, Patentgesetz, 11. Auflage, § 6 Rn. 1.
84 Mellulis in: Benkard, Patentgesetz, 11. Auflage, § 6 Rn. 1.
85 Mellulis in: Benkard, Patentgesetz, 11. Auflage, § 6 Rn. 30.
86 Mellulis in: Benkard, Patentgesetz, 11. Auflage, § 6 Rn. 32.
87 Eichmann in Eichmann/von Falckenstein/Kühne, Designgesetz, § 7 Rn. 4.

- der „Trainer“ von neuronalen Netzen – soweit hier eine kreative Leistung zu verorten ist;

- derjenige, der letztlich die Auswahl unter den von der KI geschaffenen Arbeitsergebnissen trifft.

Von den damit teilweise verbundenen Beweisschwierigkeiten abgesehen, erscheinen diese Ansatzpunkte teilweise wie „juristische Krücken“, weil die eigene geistige bzw. schöpferische Leistung dieser Personen teilweise sehr konstruiert erscheint, wenn die Rolle der KI über die eines reinen Werkzeugs hinausgeht. Hier zeigt sich, dass insbesondere das deutsche Urheberrecht – anders als das angelsächsische – den Schutz des Urhebers und nicht den Investitionsschutz im Blick hat.

Umgekehrt fragt sich, 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 vernichten. Wenn mit einem umgekehrten Ansatz beispielsweise versucht würde, urheberrechtlich schutzfähige Werke zu schaffen, könnte dies ebenfalls zu unangemessenen Ergebnissen führen.

Je mehr wichtige Arbeitsergebnisse weitgehend autonom von KI geschaffen werden, desto dringlicher werden wir uns der Frage der Schutzfähigkeit stellen müssen. Nach geltendem Recht scheint auch das Gesetz gegen den Unlauteren Wettbewerb als flexibleres Instrument für manche Bereiche geeignet (§ 4 UWG), auch wenn sich der Anwendungsbereich des Mitbewerberschutzes in den letzten Jahren eher verkleinert hat.

Darüber hinaus würden nach deutschem Recht alle materiellen Ergebnisse der schöpferischen Arbeit eines Roboters als „Früchte“ im Sinne des § 99 Abs. 1 BGB gelten.

> *„Früchte einer Sache sind die Erzeugnisse der Sache und die sonstige Ausbeute, welche aus der Sache ihrer Bestimmung gemäß gewonnen wird.“*

Solche „Früchte“ gehören dem Eigentümer des Roboters. Diese Vorschrift im deutschen Bürgerlichen Gesetzbuch war offensichtlich nicht zur Regelung von Robotern gedacht, aber sie scheint derzeit die geeignetste Bestimmung in diesem Zusammenhang zu sein. Die Anwendung auf „Früchte“ einer reinen KI-Software ist dagegen fraglich, da die Sacheigenschaft von Software nach wie vor umstritten ist.[88]

[88] Der Bundesgerichtshof sieht Software zumindest als Sache an, wenn diese auf einem Datenträger verkörpert ist. Die Gegenansicht unterscheidet zwischen dem (verkörperten) Datenträger und dem dort gespeicherten (unverkörperten) Computerprogramm. Zum Streitstand: BeckOK BGB, § 90 Rn. 26.

4. Schutz der von einer Künstlichen Intelligenz verarbeiteten Daten

Der Einsatz von Künstlicher Intelligenz ist nur auf Grundlage umfangreicher Datenverarbeitungen möglich. So vermessen etwa Roboter ihre Umgebung mittels Sensoren zur Orientierung und Navigation. Auch in Bereichen des maschinellen Lernens können Algorithmen von umfangreichen Trainingsdatensätzen profitieren. Wo zusätzliche Datenbestände zu einer beschleunigten und überlegenen Entscheidungsfindung beitragen, besteht für die Industrie der Anreiz zur Verarbeitung von immer größeren Datenbeständen. Hierbei sind die europäischen und deutschen Datenschutzgesetze zu beachten.

4.1 Der Schutz von personenbezogenen Daten

4.1.1 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 Person 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 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.

4.1.2 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[89] 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. Die betroffene Person ist 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 eine 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 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 des Roboters erfasst werden. Häufig hängt die Zulässigkeit der Datenverarbeitung dann von dem Ergebnis einer Interessenabwägung ab, in der die berechtigten Interessen des Verantwortlichen oder eines Dritten (an dem Betrieb des Roboters) den Interessen der betroffenen Personen (an dem Schutz der 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.[90] Der vermehrte Einsatz von Robotersystemen mit spezifischen Aufgabenzuweisungen im öffentlichen Raum und die

[89] 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.

[90] Vgl. Erwägungsgrund 47 DSGVO.

fortschreitende Sensibilisierung der Öffentlichkeit für deren Funktionsweise könnten langfristig dazu führen, dass diese Interessenabwägung zunehmend zugunsten der Betreiber von Robotersystemen ausfällt, insbesondere wenn sich die 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 ist, 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 Robotersystemen zulässig, soweit das System für die Durchführung des Arbeitsverhältnisses erforderlich ist, § 26 Abs. 1 S. 1 BDSG. Hierzu können „intelligente" Werkzeuge, etwa Datenbrillen oder vernetzte Handschuhe, und der Einsatz von Industrierobotern gehören,[91] wenn dadurch der Gesundheits- und Gefahrenschutz für die Beschäftigten deutlich verbessert wird. Das Tracking von Arbeitsleistungen oder Anwesenheitszeiten der Beschäftigten steht hingegen regelmäßig in Widerspruch zu diesem originären Zweck, selbst wenn es durch den Einsatz des intelligenten Systems technisch erheblich erleichtert werden sollte. Vielmehr müssen derartige Überwachungs- und Kontrollhandlungen bzgl. Mitarbeitern stets gesondert auf ihre Rechtmäßigkeit geprüft werden und bedürfen für die damit verbundenen Datenverarbeitungen einer gesonderten Rechtsgrundlage, die sich (erneut) an dem konkreten Zweck orientieren muss.

Sensible Daten, etwa Gesundheitsdaten, biometrischen 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 „einfache" Daten. Die Verarbeitung dieser Daten ist nur zulässig, wenn eine Rechtsgrundlage nach Art. 6 DSGVO vorliegt und *zusätzlich* 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. Für nähere Ausführungen hierzu wird auf Ziffer 6.4 verwiesen.

4.1.3 Pflichten des Verantwortlichen

Wer über die Auswahl, den Zweck und die Mittel der Datenverarbeitung entscheidet, ist für die Einhaltung des Datenschutzes „verantwortlich", Art. 4 Nr. 7 DSGVO. Bei Robotersystemen kann die Verantwortlichkeit etwa bei dem Eigentümer, Betreiber, Hersteller und/oder Entwickler[92] 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,

---

[91] Beispiele nach *Gola* in Gola/Heckmann, Bundesdatenschutzgesetz, 13. Auflage 2019, § 26 Rn. 78.

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

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 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 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, sofern die Verletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt, Art. 33 DSGVO. Ein solches Risiko wird regelmäßig vorliegen, wenn Dritte unberechtigten Zugriff auf die Künstliche Intelligenz und die in ihr liegenden, umfangreichen Datenbestände erlangen. Liegt ein hohes Risiko vor, ist zudem die betroffene Person zu informieren, Art. 34 DSGVO.

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

4.1.4 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 gesonderten 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.

4.1.5 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 letzten Jahres 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 nicht ausreichend. Das Urteil gilt ebenso für die Übermittlung von Daten in andere Staaten außerhalb des Europäischen Wirtschaftsraums, für die kein Angemessenheitsbeschluss besteht.

Liegt ein Angemessenheitsbeschluss nicht vor, wie nun 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 Standarddatenschutzklauseln der Europäischen Kommission oder, für konzerninterne Datenübermittlungen, auf verbindliche interne Datenschutzvorschriften der eigenen Unternehmensgruppe (sog. Binding Corporate Rules) zurückgegriffen.

Es bestehen nach der jüngsten 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.

Kurzfristig könnte Antwort in der zusätzlichen technischen Absicherung der Daten bzw. des Datentransfers liegen. Sind die übermittelten Daten hinreichend verschlüsselt, können der Zugriff und die Auswertung dieser Daten durch staatliche Behörden zumindest faktisch erschwert werden.

Hilfestellung geben die Richtlinien des Europäischen Datenschutzausschusses („EDSA") vom 10. November 2020, in denen die Inhalte und Auswirkungen des Schrems II-Urteils erläutert und auf einige Praxisfälle angewandt werden.[93]

4.1.6 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. 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.[94]

---

93 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

94 So auch Buchner in Kühling/Buchner, DSGVO/BDSG, Art. 22 DSGVO, Rn. 1.

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),[95] Entscheidungsbefugnis in einem Gerichts- oder Verwaltungsverfahren innehat,[96] 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.

4.2 Eigentum an Daten

Es stellt sich 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 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

---

[95] 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.

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

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.

4.3 Datensicherheit

Datensicherheit ist ein wesentlicher Bestandteil aller Datenschutzbemühungen. 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 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, einschließlich 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.[97]

Die Europäische Union hat sich zuletzt mit dem Erlass der Cybersecurity-Verordnung[98] der Aufgabe verschrieben, ein europäisches Zertifizierungssystem für die Sicherheit von IT-Systemen zu etablieren. Die Zertifizierungsschemata sehen unterschiedliche Anforderungsniveaus („hoch", „mittel" und „niedrig") vor, abhängig von dem jeweiligen Verwendungsrisiko, und werden für spezifische IT-Prozesse bzw. Dienste entwickelt.[99] 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" 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.

---

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

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

99 Für weitere Informationen vgl. Kipker/Scholz in MMR-Aktuell 2019, 414986.

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.

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.[100] 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.[101]

---

[100] 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.

[101] 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.

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.

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.[102] 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 2.6.3).

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

6. Künstliche Intelligenz im Gesundheitswesen

6.1 Allgemeiner Ansatz

Künstliche Intelligenz, die in Deutschland im Gesundheitssektor eingesetzt wird, kann dem für Medizinprodukte geltenden Regelwerk, insbesondere dem noch geltenden Medizinproduktegesetz (**MPG**), unterliegen. Das MPG hat die Richtlinie 93/42/EWG über Medizinprodukte, die Richtlinie 90/385/EWG über aktive implantierbare medizinische Geräte und die Richtlinie 98/79/EG über In-vitro-Diagnostika umgesetzt.

Das MPG wird ab dem 26. Mai 2021 schrittweise durch das neue Gesetz zur Durchführung unionsrechtlicher Vorschriften betreffend Medizinprodukte (**MPDG**) ersetzt. Das MPDG ergänzt die neue Verordnung (EU) 2017/745 über Medizinprodukte (**MP-VO**), Geltungsbeginn am 26. Mai 2021, und die neue Verordnung (EU) 2017/746 über In-vitro-Diagnostika, Geltungsbeginn 26. Mai 2022. Die EU Verordnungen heben zugleich die vorbenannten Richtlinien auf.

Damit sind die Vorschriften für Medizinprodukte auf EU-Ebene nahezu harmonisiert.

Nach der neuen Rechtslage ist ein „**Medizinprodukt**" definiert als Instrument, Apparat, Gerät, Software usw., das dem Hersteller zufolge für Menschen bestimmt ist und einen oder mehrere der aufgeführten spezifischen medizinischen Zwecke erfüllen soll, § 3 MPDG i.V.m. Art. 2 Nr. 1 MP-VO.

Diese Definition gilt für alle Mitgliedstaaten der Europäischen Union und sollte aufgrund der generalisierten Formulierung und der ausdrücklichen Einbeziehung von „Software" auch Gesundheitsroboter umfassen. Auch bei Gesundheits-Apps handelt es sich um Medizinprodukte, wenn sie der Diagnose oder Therapie einer Erkrankung dienen.[103] Hingegen ist Software, die zwar im Gesundheitswesen eingesetzt wird, aber allgemeinen Zwecken dient oder für Zwecke in den Bereichen Lifestyle oder Wohlbefinden eingesetzt wird, nicht als Medizinprodukt einzustufen.[104] Für die Einstufung von Robotersystemen dürfte ein ähnlicher Maßstab anzusetzen sein.

Darüber hinaus regelt die Medizinprodukte-Betreiberverordnung (**MPBetreibV**) derzeit das Errichten, Betreiben, Anwenden und die Wartung von Medizinprodukten sowie die entsprechende Dokumentation. Dies wird auch nach Geltungsbeginn der MP-VO und des MPDG in Rechtsverordnungen der entsprechenden Bundesministerien geregelt werden, vgl. § 88 Abs. 1 Nr. 6 MPDG.

6.2 Inverkehrbringen von Medizinprodukten

Medizinprodukte dürfen auch nach der neuen Rechtslage nur in Verkehr gebracht werden, wenn sie eine sogenannte CE-Kennzeichnung tragen, Art. 10 Abs. 6 und 5 Abs. 1 MP-VO. Die CE-Kennzeichnung wird nur dann erteilt, wenn die Medizinprodukte die zahlreichen und strengen Anforderungen der MP-VO erfüllen. Die jeweiligen Anforderungen richten sich nach dem poten-

---

103 So Katzenmeier in Big Data, E-Health, M-Health, KI und Robotik in der Medizin, MedR 2019, 259.
104 Erwägungsgrund 19 der Verordnung EU 2017/745.

tiellen Gesundheitsrisiko des Medizinproduktes, Art. 51 Abs. 1 und Anhang VIII MP-VO. Abhängig von dieser risikobasierten Einstufung sieht Art. 52 MP-VO mehrere Konformitätsbewertungsverfahren vor.

Es ist festzustellen, dass die Anforderungen an Medizinprodukte mit der Einführung der MP-VO und des MPDG insgesamt erhöht wurden. So wurden verschärfte Kriterien für die Benennung der Zulassungsstellen („Benannte Stellen") sowie zusätzliche Kontrollverfahren und Überwachungspflichten eingeführt. Hinzu kommen strengere Klassifizierungsregeln.[105] Gesundheits-Apps für Diagnose- und Therapiezwecke wurden etwa in die Risikoklasse IIa hochgestuft. Hersteller von medizinischen Apps haben daher zukünftig Benannte Stellen für die Durchführung des Konformitätsverfahrens hinzuzuziehen.[106] Die bevorstehende Verschärfung der regulatorischen Anforderungen führte dazu, dass der Geltungsbeginn der MP-VO, ursprünglich der 26. Mai 2020, um ein Jahr verschoben wurde, um drohenden Versorgungsengpässen von Medizinprodukten während der COVID-19 Pandemie vorzubeugen.

6.3 Haftung

Die Nutzung von Künstlicher Intelligenz im medizinischen Bereich besitzt auch umfangreiche haftungsrechtliche Implikationen. Grundlegend soll dazu nachfolgend zwischen der Haftung des Anwenders (Arzt, Klinik) und der Haftung des Herstellers unterschieden werden.

Eine Haftung der Künstlichen Intelligenz selbst kommt derzeit hingegen nicht in Betracht, da sie keine eigene Rechtspersönlichkeit besitzt (hierzu bereits oben unter Ziffer 2).

6.3.1 Anwenderhaftung

Für Behandlungsfehler, die sich im Zusammenhang mit der Verwendung von Künstlicher Intelligenz ergeben können, kommt grundsätzlich eine Haftung des Arztes (oder ggf. des Trägers einer Klinik) nach allgemeinen Grundsätzen in Betracht, d. h. sowohl aus Vertrag (§ 280 BGB i. V. m. §§ 630a ff. BGB) als auch aus Gesetz (§ 823 BGB). Die Behandlung hat „nach den zum Zeitpunkt der Behandlung bestehenden, allgemein anerkannten fachlichen Standards zu erfolgen" (§ 630a Abs. 2 BGB); der Patient muss umfassend aufgeklärt worden sein und eingewilligt haben.

Gerade hinsichtlich etwaiger Schäden, die auf eine zuvor nicht bekannte Fehlfunktion Künstlicher Intelligenz zurückzuführen sind, ist fraglich, inwieweit dies zur Haftung des Arztes führen kann. Soweit der Haftungsfall nicht durch eine unsachgemäße Bedienung ausgelöst wird, kommen insoweit maßgeblich Verletzungen einer Aufklärungspflicht in Betracht. Hinsichtlich gänzlich unerwarteter und außergewöhnlicher Risiken, die auf die Entscheidung des Patienten zur Durchführung der Behandlung keinen Einfluss haben, dürften Aufklärungspflichtverletzungen eher nicht anzunehmen sein.[107]

---

[105] Eine Übersicht über die wesentlichen Neuerungen ist abrufbar unter https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/neue-eu-verordnungen.html.

[106] Schmidt in Das neue europäische Medizinproduktrecht und das deutsche Lauterkeitsrecht, WRP 2020, 700.

[107] Rammos/Lange/Clausen, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 28 Rn. 23.

Auch wenn die Anwendung von „nicht allgemein anerkannten, den Korridor des medizinischen Standards verlassenden Behandlungskonzepten“ nicht in jedem Fall zu einem Behandlungsfehler führt, bedarf dies aber einer besonderen Rechtfertigung und Aufklärung des Patienten, insbesondere hinsichtlich unbekannter Risiken.[108] Dies sollte auch bei einer Behandlung unter Nutzung von Künstlicher Intelligenz berücksichtigt werden, insbesondere bei besonders innovativen und damit möglicherweise nicht etablierten Methoden bzw. Produkten.

Auch hinsichtlich einer Arzthaftung stellen sich indes Fragen nach der Beweislast. Zwar sieht § 630h BGB für vertragliche Ansprüche eine Beweislasterleichterung hinsichtlich der Pflichtverletzung des Arztes vor. Um in deren Genuss zu kommen, muss der Patient jedoch beweisen, dass sich ein Risiko, das für den Arzt voll beherrschbar war, verwirklicht und zu der betreffenden Verletzung geführt hat, § 630h Abs. 1 BGB. Diesen Beweis zu führen, insbesondere dass das Risiko durch den Arzt voll beherrschbar war, könnte im Zusammenhang mit Künstlicher Intelligenz schwierig für den Geschädigten sein.[109] Insoweit erscheint es jedenfalls denkbar, dass im Wege der Rechtsfortbildung künftig weitere Beweiserleichterungen für Arzthaftungsfälle im Zusammenhang mit Künstlicher Intelligenz geschaffen werden.

6.3.2 Herstellerhaftung (Produkthaftung)

Das MPDG enthält ebenso wenig wie das MPG eigene Bestimmungen über die Haftung des Herstellers für durch Medizinprodukte verursachte Schäden. Es sieht jedoch für klinische Prüfungen und sonstige klinische Prüfungen eine Versicherungspflicht für gewisse Haftungsfälle vor (Tötung oder Verletzungen von Körper und Gesundheit sowie Gewährung von Leistungen, „wenn kein anderer haftet“), § 26 Abs. 2 MDPG.

Die Haftung des Herstellers eines Produkts, das Künstliche Intelligenz beinhaltet, kommt daher zunächst im Wege der verschuldensunabhängigen Haftung nach dem Produkthaftungsgesetz (**Produkthaftung**) in Betracht (insgesamt siehe hierzu oben Ziffer 2). Reine Software hingegen unterfällt derzeit (noch) nicht der Produkthaftung, auch wenn sich hierzu Stimmen mehren, die dies ändern wollen. Der Hersteller des in Verkehr gebrachten Endprodukts oder der Zulieferer eines Teilprodukts, auf dem er sich selbst kenntlich gemacht hat, haften hiernach.

Hinsichtlich der Fehler kann, wie im Rahmen der Produzentenhaftung, nach **Konstruktions-, Fabrikations- und Instruktionsfehlern** unterschieden werden (Details hierzu sogleich).[110] Der Geschädigte hat den Fehler, den Schaden und den ursächlichen Zusammenhang zwischen Fehler und Schaden zu beweisen. Ein Haftungsausschluss des Herstellers kann insbesondere dann vorliegen, wenn der Hersteller gesetzliche Vorgaben beachtet hat und der Fehler hierauf beruht, § 1 Abs. 2 Nr. 4 ProdHaftG, oder der Fehler nach dem Stand der Wissenschaft und Technik nicht erkannt werden konnte, § 1 Abs. 2 Nr. 5 ProdHaftG. In letzterem Fall könnten aber Ansprüche wegen späterer Verletzung einer Produktbeobachtungspflicht nach der Produzentenhaftung in Betracht kommen (hierzu sogleich).

---

[108] BGH NJW 2020, 1358, 1359 f.; vgl. insoweit auch die diversen „Robodoc“-Entscheidungen, bspw. BGH NJW 2006, 2477; OLG Dresden NJOZ 2008, 247; LG Hannover Urt. v. 10.1.2011 – 19 O 161/07.

[109] Rammos/Lange/Clausen, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 28 Rn. 24.

[110] MüKoBGB/Wagner, 8. Aufl. 2020 Rn. 41, ProdHaftG § 3 Rn. 41.

Daneben kommen auch Ansprüche nach der verschuldensabhängigen **Produzentenhaftung** in Betracht. Auch hier gelten die bereits erwähnten Kategorien, d. h. insbesondere Konstruktions-, Fabrikations- und Instruktionsfehler sowie Produktbeobachtungspflichten. Der Geschädigte muss im Rahmen der Produzentenhaftung grundsätzlich alle Anspruchsvoraussetzungen beweisen, somit auch die Pflichtverletzung und das Verschulden des Herstellers. Hierbei könnten ihm angesichts der Komplexität und Opazität automatisierter Systeme im Einzelfall aber Beweiserleichterungen zugutekommen.

Ein „**Konstruktionsfehler**" liegt vor, wenn das Produkt schon seiner Konzeption nach unter dem gebotenen Sicherheitsstandard bleibt, d. h. bereits im Rahmen seiner Entwicklung die gebotenen Sicherheitsvorkehrungen unterblieben sind.[111] Fraglich ist insoweit, welche sogenannte Konstruktionssorgfalt geschuldet wird. In vielen Fällen dürften aber Verstöße gegen technische Normen einschließlich der einschlägigen EN- und DIN-Normen als haftungsbegründender Pflichtverstoß des Herstellers gelten. Werden technische Standards eingehalten, bedeutet dies allerdings nicht in jedem Fall eine Enthaftung des Herstellers. Vielmehr dürften auch hier Produktbeobachtungspflichten bestehen.

Ein „**Fabrikationsfehler**" ist die Abweichung von den definierten Sicherheitsstandards der Produktserie.[112] Insoweit trägt der Hersteller ein gewisses „Ausreißerrisiko".

Ein „**Instruktionsfehler**" wird angenommen, wenn der Verwender nicht oder nur unzureichend über die Art und Weise der Verwendung und die damit verbundenen Gefahren aufgeklärt wird.[113] Insoweit können bei Medizinprodukten gesteigerte Informationspflichten bestehen. In jedem Fall muss der Hersteller sicherstellen, dass der Anwender so über die mitunter komplexen Funktionen informiert wird, dass er sie angemessen nachvollziehen und das Produkt sicher bedienen kann.

Zu **Produktbeobachtungspflichten** siehe bereits oben unter Ziffer 2. Stellt der Hersteller im Rahmen seiner Produktbeobachtung einen erheblichen Fehler fest, muss er im Einzelfall unter Umständen eingreifen und eine Warnung aussprechen oder einen Rückruf, gegebenenfalls unter Durchführung von Updates, vornehmen.

Anders als bei der Produkthaftung können nach der Produzentenhaftung auch Hersteller von **Software** in Anspruch genommen werden. Hierunter können auch Gesundheits-Apps fallen, insbesondere wenn diese als Medizinprodukte gelten. Wirbt der Hersteller mit der App als Ersatz für eine ärztliche Behandlung, soll der Sorgfaltsmaßstab für den Hersteller am sogenannten Facharztstandard zu messen sein.[114]

Ein Verstoß gegen die Konformitäts- und Produktanforderungen der nunmehr geltenden Medizinprodukteverordnung[115] (insbesondere Art. 5 Abs. 1, 2 MP-VO) und des MPDG (vgl. §§ 11 bis 13 MPDG) oder die Regelungen zu Installation, Betrieb, Verwendung und Instandhaltung nach den

---

111 BGH NJW 2013, 1302, 1303.
112 MüKoBGB/Wagner, 8. Aufl. 2020, ProdHaftG § 3 Rn. 42.
113 MüKoBGB/Wagner, 8. Aufl. 2020, ProdHaftG § 3 Rn. 46.
114 Rammos/Lange/Clausen, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 1. Aufl. 2020, § 28 Rn. 19.
115 Verordnung (EU) 2017/745 des Europäischen Parlamentes und des Rates vom 5. April 2017.

erlassenen Rechtsverordnungen kann zudem eine Haftung wegen Verletzung eines Schutzgesetzes nach § 823 Abs. 2 BGB nach sich ziehen. Hier muss der Geschädigte allerdings die Anspruchsvoraussetzungen, einschließlich eines Verschuldens, beweisen.

6.4 Datenschutzrecht

Die für den medizinischen Betrieb besonders relevanten Gesundheitsdaten unterliegen, ebenso wie genetische oder biometrische Daten sowie Daten zum Sexualleben, besonders strengen Datenschutzvorschriften. Wie in Ziffer 4.1.2 bereits dargestellt, ist die Verarbeitung dieser besonderen Kategorien von personenbezogenen Daten nur in den Ausnahmefällen des Art. 9 Abs. 2 bis 4 DSGVO überhaupt zulässig.

An die Einwilligung einer betroffenen Person in die Verarbeitung von besonderen Kategorien personenbezogener Daten sind erhöhte Anforderungen zu stellen, Art. 9 Abs. 2 lit. a) DSGVO. Die Einwilligung ist nur wirksam, wenn sie ausdrücklich erteilt wird und sich dabei gerade auch auf die Verarbeitung dieser sensiblen Daten bezieht; stillschweigende oder konkludente Handlungen sind hierfür nicht ausreichend. Die betroffene Person ist auf die besondere Sensitivität der Daten hinzuweisen. An den Inhalt der Einwilligungserklärung ist deshalb ein gesteigertes Maß an Bestimmtheit, Transparenz und Genauigkeit anzulegen.[116]

Die gesetzlichen Ausnahmetatbestände nach Art. 9 Abs. 2 lit. b) bis j) DSGVO erlauben unter anderem die Verarbeitung von besonderen Kategorien personenbezogener Daten, wenn die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben, die Verarbeitung aber zum Schutz lebenswichtiger Interessen erforderlich ist. Dies umfasst insbesondere medizinische Notfallsituationen, in denen eine Einwilligung der betroffenen Person nicht (rechtzeitig) eingeholt werden kann. Die Verarbeitung von besonderen Kategorien personenbezogener Daten kann ferner zulässig sein, wenn dies zum Zwecke der Gesundheitsvorsorge, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich ist. Es muss jeweils im Einzelfall bestimmt werden, ob die angestrebte Datenverarbeitung für diese Diagnose-, Versorgungs- oder Verwaltungszwecke tatsächlich erforderlich ist. Die Verarbeitung von Gesundheitsdaten ist hiernach jedenfalls nur unter der Verantwortung einer Person zulässig, die dem Berufsgeheimnis oder einer äquivalenten Geheimhaltungspflicht unterfällt. In Deutschland ergibt sich diese Geheimhaltungspflicht für Ärzte, Angehörige von Heilberufen, Mitarbeiter von Versicherungsunternehmen und andere mitwirkende Personen aus § 203 StGB.

Besondere Kategorien von personenbezogenen Daten dürfen unter bestimmten Voraussetzungen zudem für wissenschaftliche Forschungszwecke verarbeitet werden, vgl. Art. 9 Abs. 2 lit. j) DSGVO in Verbindung mit § 27 BDSG. Auf diese Weise dürfen im Einzelfall etwa Gesundheitsdaten zur Durchführung von klinischen Studien, die im öffentlichen Interesse liegen, verarbeitet werden, ohne dass es einer Einwilligung der betroffenen Studienteilnehmer bedarf. Dies gilt allerdings nur, wenn die Datenverarbeitung zu diesen Zwecken **erforderlich** ist und die Interessen des Verantwortlichen die Interessen der Studienteilnehmer **erheblich** überwiegen. Zudem muss

[116] Weichert in Kühling/Buchner DSGVO/BDSG, Art. 9 Rn. 47.

der Verantwortliche angemessene und spezifische Maßnahmen zur Wahrung der Interessen der Studienteilnehmer treffen, § 27 Abs. 1 BDSG. Die Studiendaten sind etwa getrennt von jeglichen identifizierenden Daten aufzubewahren und zum frühestmöglichen Zeitpunkt zu anonymisieren. Studien zu kommerziellen Zwecken sind hiervon ausgenommen.[117]

Die allgemeinen Grundsätze für die Auftragsverarbeitung durch Dritte und für die Übermittlung personenbezogener Daten an Drittstaaten außerhalb der EU/des EWR gelten auch für Gesundheitsdaten (vgl. Ziffer 4.1.5). Bei der Beurteilung der Angemessenheit des Schutzniveaus in einem Drittland ist jedoch insbesondere die Art der Daten zu beachten, die tendenziell höhere Standards erfordert, wenn es sich um derart sensible Daten handelt.

[117] Kühling/Buchner, BDSG, 3. Auflage 2020, § 27 Rn. 5 ff.

7. Drohnen und Überwachungsroboter für den zivilen Einsatz

7.1 Einführung

Die Internationale Zivilluftfahrt-Organisation (**ICAO**) hat **zivile Drohnen** als „unbemannte Luftfahrzeuge" (**UAV**) oder „ferngesteuerte Luftfahrtsysteme" (**RPAS**) definiert. Der Begriff zivile Drohne wird nur umgangssprachlich verwendet.

Das deutsche Luftverkehrsgesetz (**LuftVG**) unterscheidet Drohnen nach ihrem jeweiligen Verwendungszweck: Drohnen für Sport- und Freizeitzwecke sind „Flugmodelle", im Übrigen gelten Drohnen als „unbemannte Luftfahrtsysteme". Beide Begriffe umfassen ausschließlich unbemannte Fluggeräte, unabhängig von ihrer Größe oder Antriebsart.[118] Das LuftVG stuft Flugmodelle und unbemannte Luftfahrtsysteme als „Luftfahrzeug" ein, vgl. § 1 Abs. 2 LuftVG.

Nach dem Verständnis des europäischen Gesetzgebers wird die Drohne als „unbemanntes Luftfahrzeug" („*unmanned aircraft*" **UA**)[119] und die Drohne mitsamt der Ausrüstung für deren Fernsteuerung als „unbemanntes Luftfahrzeugsystem" („*unmanned aircraft system*" **UAS**) bezeichnet.[120]

7.2 Allgemeiner Rechtsrahmen

7.2.1 Europäisches Recht

Die Europäische Agentur für Flugsicherheit (**EASA**) entwirft im Auftrag der EU Kommission einen europaweit vereinheitlichten Rechtsrahmen zur Regulierung von zivilen Drohnen. Das Fundament bildet die Verordnung (EU) 2018/1139 (**EASA-Grundverordnung**), die unter anderem die grundlegenden Anforderungen an die Konstruktion, Herstellung, Instandhaltung und den Betrieb von Drohnen vorsieht.[121] Betreiber und Piloten müssen die geltenden Vorschriften kennen und in der Lage sein, die Sicherheit des Betriebs zu gewährleisten. Drohnensysteme müssen so konstruiert und gebaut sein, dass ein Betrieb ohne Gefährdung von Personen möglich ist und sie erforderlichenfalls auch nach dem Ausfall einzelner Systeme sicher steuerbar und manövrierbar bleiben. Abhängig von den jeweiligen Risiken ist die Konstruktion, Herstellung, Instandhaltung und der Betrieb von unbemannten Luftfahrtsystemen nur mit entsprechenden Zertifizierungen zulässig. Es besteht eine Registrierungspflicht für bestimmte Drohnen und vereinzelt auch deren Betreiber. Die EU-Kommission wird in Art. 57 und Art. 58 EASA-Grundverordnung außerdem zum Erlass von Durchführungsakten und delegierten Rechtsakten ermächtigt. Hiermit sollen die allgemeinen Anforderungen der EASA-Grundverordnung detailliert ausgestaltet werden.

---

118 Lampe in Erbs/Kohlhasas, Strafrechtliche Nebengesetze, LuftVG, § 1 Rn. 6.

119 Dies ist ein „Luftfahrzeug, das ohne einen an Bord befindlichen Piloten autonom oder ferngesteuert betrieben wird oder dafür konstruiert ist", Art. 3 Nr. 30 Verordnung (EU) 2018/1139 des europäischen Parlaments und des Rates vom 4. Juli 2018.

120 Art. 2 Nr. 1 Durchführungsverordnung (EU) 2019/947 der Kommission vom 24. Mai 2019.

121 Eine Übersicht zu den grundlegenden Anforderungen gibt *Josipovic* in Europäische Regulierung des Betriebs unbemannter Luftfahrzeuge, NVwZ 2019, 438.

Mit dem Erlass der Delegierten Verordnung (EU) 2019/945 (**VO (EU) 2019/945**)[122] und der Durchführungsverordnung (EU) 2019/947 (**VO (EU) 2019/947**) hat die EU-Kommission von dieser Ermächtigung Gebrauch gemacht. Diese Verordnungen traten zum 31. Dezember 2020 in Kraft und werden verschiedene nationale Vorschriften, darunter die drohnenspezifischen Regelungen der LuftVO und des LuftVZO, verdrängen. Seitdem werden Drohnen risikobasiert in die Klassen C0 bis C6 eingeteilt[123] und der Betrieb von Drohnen wird bestimmten Kategorien („offen", „speziell", „zulassungspflichtig")[124] zugewiesen. Abhängig von der Drohnenklasse und der Betriebskategorie werden unterschiedliche Anforderungen an Hersteller, Betreiber und Piloten gestellt.

Der Betrieb einer Drohne in der „offenen" Kategorie ist grundsätzlich nur im Sichtbereich zulässig und erfordert keine Betriebsgenehmigung. Ab einer Startmasse von 250 g müssen Piloten aber zumindest einen „Online-Lehrgang" und eine „Online-Theorieprüfung" absolviert haben. Für solche Drohnen liegt das Mindestalter der Piloten bei 16 Jahren. Der Betrieb einer Drohne in der „speziellen" Kategorie erfordert im Regelfall eine Genehmigung, die nach einer individuellen Risikobewertung von der zuständigen Behörde erteilt wird. Die Genehmigung enthält dann auch die weiteren Anforderungen, die an die Drohne und deren Betrieb im konkreten Einzelfall zu stellen sind.[125] Unterfällt der geplante Drohnenbetrieb bestimmten Standardszenarien, die mit einem geringen Risiko bewertet und in denen diese Anforderungen bereits festgelegt wurden, kann es aber ausreichend sein, den geplanten Drohnenbetrieb in einer Erklärung bei der zuständigen Behörde anzuzeigen. Die behördliche Genehmigung oder Erklärung kann zudem durch eine Zertifizierung des Betreibers[126] ersetzt werden. Der „zulassungspflichtige" Betrieb, der auch die Beförderung von Menschen umfassen kann, ist mit den Risiken der bemannten Luftfahrt vergleichbar.[127] Er unterfällt nach Art. 7 Abs. 3 VO (EU) 2019/947 auch den aus der bemannten Luftfahrt bekannten Zertifizierungsanforderungen.

Die EU-Kommission bereitet mit den Verordnungen zudem die Umsetzung des geplanten „**U-Space-Systems**"[128] vor. Das U-Space-System soll die Infrastruktur, Dienste und spezifischen Verfahren bereitstellen, mit deren Hilfe eine große Anzahl von Drohnen einen sicheren, effizienten und geschützten Zugang zum Luftraum erhalten. Mit dem U-Space sollen die Voraussetzungen

---

122 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.

123 Die Einordnung erfolgt anhand der technischen Spezifikationen und den hieraus resultierenden Risiken. Drohnen der Klasse „C0" dürfen etwa nur eine höchstzulässige Startmasse von unter 250 g, Drohnen der Klassen „C3" bis „C6" eine höchstzulässige Startmasse von unter 25 kg aufweisen.

124 Die „offene" Kategorie umfasst den Betrieb von Drohnen mit geringem Risiko und einer Startmasse von unter 25 kg. Die „zulassungspflichtige" Kategorie umfasst dagegen Betriebsszenarien mit hohem Risiko, etwa wenn eine Drohne Menschen oder gefährliche Güter befördern soll oder besonders große Drohnen (Abmessung von über 3 m) Menschenmengen überfliegen sollen. Die „spezielle" Kategorie umfasst die übrigen Einsatzszenarien.

125 Die Betriebsgenehmigung enthält u. a. Angaben zu den technischen Merkmalen und der Zulassung der Drohne, der geforderten Kompetenz des Piloten sowie zu den Betriebsbeschränkungen, vgl. Art. 12 Abs. 4 VO (EU) 2019/947.

126 Es wird ein Betreiberzeugnis für Leicht-UAS benötigt, vgl. Art. 5 Abs. 6 VO (EU) 2019/947.

127 Vgl. auch Krumm in Der neue europäische Rechtsrahmen für unbemannte Luftfahrzeuge, EuZW 2019, 114 (117).

128 Die EASA hat in der Opinion No 01/2020 bereits den Verordnungsentwurf zur Regulierung des europäischen U-Spaces erarbeitet, der derzeit bei der EU-Kommission liegt. Der Erlass der Verordnung wird für 2021 erwartet, vgl. Kilian/Gebhardt in Der neue EASA-Verordnungsentwurf, EuZW 2020, 735 (740).

für einen sicheren routinemäßigen Einsatz von Drohnen geschaffen werden.[129] Als wesentliche Grundpfeiler des U-Space-Systems gelten Maßnahmen zur Fernidentifizierung, Registrierung und Geo-Sensibilisierung von Drohnen.[130]

So müssen Drohnen, die für den Einsatz unterhalb einer Flughöhe von 120 m bestimmt sind, ab der Klasse C1, d. h. ab einer Startmasse von 250 g, grundsätzlich mit einem System zur Fernidentifizierung („*direct remote identification*") ausgestattet sein, welches u. a. die Betreiber- und Seriennummer, die geografische Position, Geschwindigkeit und den Streckenverlauf der Drohne und die geografische Position des Piloten oder den Startpunkt während der gesamten Flugdauer überträgt. Die Übertragung erfolgt in einem offenen und dokumentierten Protokoll, das innerhalb des Sendebereichs von Mobilfunkgeräten direkt empfangen werden kann.[131] Dieser Fernzugriff – vergleichbar mit einem „elektronischen Nummernschild"[132] – soll Privatpersonen die Durchsetzung ihrer Rechte gegenüber dem Drohnenpiloten und Strafverfolgungsbehörden die Ahndung von Ordnungswidrigkeiten erleichtern. Ab der Klasse C1 müssen Drohnen zudem registriert werden. Die Mitgliedstaaten sollen hierzu digitale und interoperable Registrierungssysteme betreiben, die einen gegenseitigen Datenaustausch ermöglichen. Schließlich müssen zumindest Drohnen der Klasse C1 bis C3 mit einem System zur Geo-Sensibilisierung ausgestattet sein, welches den Piloten unter anderem vor einer bevorstehenden Verletzung von Luftraumgrenzen, etwa bei Annäherung an eine militärische Anlage, warnt.[133] Die Mitgliedstaaten können diese Luftraumgrenzen selbstständig festlegen.

7.2.2 Deutsches Recht

Obwohl der Drohnenbetrieb seit dem 1. Januar 2021 ganz überwiegend nach europäischem Recht reguliert wird, verbleiben einzelne Regelungsbereiche bei den Mitgliedstaaten. Hierzu gehört die Einrichtung spezifischer Luftraumgrenzen. In der Bundesrepublik Deutschland waren bei Erstellung dieses Werkes noch keine an die neuen EU-Vorgaben angepassten Vorschriften erlassen. Damit dürften die bislang bestehenden nationalen Vorschriften in Bezug auf Luftraumgrenzen übergangsweise weiterhin gelten, sofern sie nicht in Widerspruch zu den europäischen Vorschriften stehen. Die Luftverkehrs-Ordnung (LuftVO) sieht vor, dass der Drohnenbetrieb über und in einem seitlichen Abstand von 100 Metern von Menschenansammlungen, Unglücksorten, Katastrophengebieten, Industrieanlagen, Justizvollzugsanstalten, militärischen Anlagen, Bundesfernstraßen, Bahnanlagen und zahlreichen weiteren Einrichtungen grundsätzlich unzulässig ist, vgl. § 21b Abs. 1 LuftVO. Der Betrieb einer Drohne über Wohngrundstücken ist verboten, wenn die Drohne die Startmasse von 250 g überschreitet oder in der Lage ist, optische, akustische oder Funksignale zu übertragen oder aufzuzeichnen, sofern der Überflug durch den Nutzungsberechtigten nicht ausdrücklich gestattet wurde. Neben diesen spezifischen Luftraumgrenzen gelten auch nationale Vorschriften zur Versicherungspflicht weiterhin, vgl. § 43 LuftVG.

---

129 SESAR Joint Undertaking, U-Space Blueprint, S. 2.
130 Vgl. Erwägungsgrund 26 zu VO (EU) 2019/947.
131 Teil 2 ff. der VO (EU) 2020/1058.
132 So auch Krumm in Der neue europäische Rechtrahmen für unbemannte Luftfahrzeuge, EuZW 2019, 118.
133 Die Mitgliedstaaten können den Zugang zum Luftraum in festgelegten Gebieten („geografische UAS-Gebiete") von bestimmten technischen Merkmalen der Drohne, etwa der Ausrüstung mit einem Geo-Sensibilisierungssystem, abhängig machen, vgl. Art. 15 Abs. 1 lit. d) EU (VO) 2019/947. Für den Betrieb in solchen Gebieten müssten dann auch die weiteren Drohnenklassen mit einem Geo-Sensibilisierungssystem ausgestattet sein.

7.3 Datenschutzrecht

Die meisten Drohnen sind mit Kameras ausgestattet, deren Betrieb eine Datenverarbeitung mittels Videoüberwachung darstellt. Erfolgt der Einsatz dieser Drohnen nicht zur Ausübung von ausschließlich persönlichen oder familiären Tätigkeiten, richtet sich die Zulässigkeit dieser Videoüberwachung nach den Vorschriften der DSGVO und des BDSG. Dies ist insbesondere der Fall, wenn Drohnen gewerblich genutzt werden sollen.

Die Datenschutzkonferenz[134] ist der Auffassung, dass der Einsatz von Kameradrohnen häufig schwerwiegender in das Recht auf Schutz der personenbezogenen Daten der betroffenen, nämlich aufgezeichneten Personen eingreift, als der Einsatz von stationären (Sicherheits-)Kameras.[135] So kann der Verantwortliche während des Drohneneinsatzes den Informationspflichten aus Art. 13, 14 DSGVO in der Regel nicht hinreichend nachkommen. Für die betroffenen Personen ist dann nicht zu erkennen, wer für die Videoüberwachung verantwortlich ist und zu welchem Zweck die Daten verarbeitet werden. Die Geltendmachung von Betroffenenrechten wird dadurch erheblich erschwert.

Unbeschadet der Erfüllung von Informationspflichten stellt sich die Frage nach der Rechtsgrundlage für die Erhebung und Verarbeitung der in den Videoaufzeichnungen enthaltenen personenbezogenen Daten. Zwar könnte man meinen, dass die Videoüberwachung mithilfe einer Kameradrohne nach den Vorschriften der DSGVO grundsätzlich nur mit einer Einwilligung der betroffenen Personen zulässig sein soll. Jedoch ist kaum erkennbar, wie die Einwilligung von Personen eingeholt werden soll, die bei einem Drohnen-Überflug – mehr oder weniger zufällig – aufgezeichnet werden. Beschränkt sich die Videoüberwachung bzw. -aufzeichnung nicht auf einen vorab definierten und abgegrenzten Bereich, dürfte das Einholen von Einwilligungen unrealistisch sein. Darüber hinaus kann die Videoüberwachung grundsätzlich auch aufgrund von berechtigten Interessen des Drohnenbetreibers oder seines Auftraggebers zulässig sein, wenn dieser besonders schutzwürdige Einsatzzwecke verfolgt. Sehr häufig werden aber die Interessen und Grundrechte der betroffenen Personen überwiegen. Dies gilt insbesondere, wenn das Bildmaterial im Internet frei veröffentlicht werden soll. In jedem Fall ist eine konkrete Interessensabwägung unter Berücksichtigung von Art und Umfang der Aufnahmen der Betroffenen und der konkreten Verarbeitungszwecke sowie der geplanten Speicherdauer durchzuführen und zu dokumentieren.

Bei Drohnen, die in der Lage sind, Bilder und Videos aufzunehmen, besteht häufig die Möglichkeit, solche Aufnahmen während des Fluges auf dem Gerät des Drohnenbetreibers oder sogar in einem vom Drohnenhersteller betriebenen oder durch ihn genutzten Cloud-Speicher zu speichern. Die allgemeinen Grundsätze für die Auftragsverarbeitung durch Dritte und für die Übermittlung personenbezogener Daten an Drittstaaten außerhalb der EU/des EWR gelten auch für Daten, die von einer Drohne gesammelt und auf den Servern eines Anbieters mit Sitz in einem Drittland gespeichert werden (vgl. Ziffer 4.1.5).

---

[134] Die Datenschutzkonferenz („DSK") ist das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.

[135] Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen vom 16. Januar 2019, abrufbar unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Videoueberwachung/Positionspapier-Kameradrohnen.pdf.

7.4 Kunsturhebergesetz

Die Veröffentlichung und Verbreitung von Aufnahmen einer natürlichen Person ist zudem nach § 22 KunstUrhG einem besonderen Verbot unterworfen und im Grundsatz nur mit Einwilligung der betroffenen Person zulässig. Dieses Verbot gilt unabhängig von dem Anwendungsbereich der DSGVO[136] und damit auch, wenn der Drohnenflug ausschließlich persönliche oder familiäre Zwecke verfolgt. Hiervon ausgenommen sind Bildnisse von Personen der Zeitgeschichte und ihren Begleitern, Bildnisse von Landschaften und Örtlichkeiten, auf denen die Person in den Hintergrund (als „Beiwerk") tritt, Bildnisse von Versammlungen oder Aufzügen und Bildnisse, die einem höheren Kunstinteresse dienen, jeweils unter der Voraussetzung, dass die Veröffentlichung und Verbreitung kein berechtigtes Interesse des Abgebildeten verletzt.

7.5 Allgemeines Persönlichkeitsrecht

Das Anfertigen von Bild- oder Videomaterial einer natürlichen Person kann zudem einen Eingriff in das Allgemeine Persönlichkeitsrecht darstellen, vgl. Art. 2 Abs. 1, 1 Abs. 1 GG. Im Anwendungsbereich der DSGVO und/oder des KunstUrhG ist ein Rückgriff auf das Allgemeine Persönlichkeitsrecht häufig nicht erforderlich. Es verbleibt aber insbesondere in Fällen relevant, in denen die Drohne nur zu persönlichen oder familiären Zwecken betrieben wird, so dass der Anwendungsbereich der DSGVO nicht eröffnet ist, von den Aufnahmen jedoch andere natürliche Personen betroffen sind. Im Verhältnis zum KUG erfasst das Allgemeine Persönlichkeitsrecht zudem bereits die Anfertigung, nicht erst die Verbreitung bzw. Veröffentlichung von Bild- oder Videomaterial. Letztlich gewährt das Allgemeine Persönlichkeitsrecht einen umfassenderen Schutz als die DSGVO und das KunstUrhG und schützt etwa auch die Ehre der abgebildeten Person.

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. So stellen etwa Wohngrundstücke, die von angrenzenden öffentlichen Flächen und Privatgrundstücken nicht einsehbar sind, typische Rückzugsorte dar und sind der Privatsphäre des jeweiligen Nutzers zuzurechnen. Bereits die Aufnahme solcher nicht von außen einsehbaren Flächen durch eine Drohnenkamera dürfte im Regelfall eine Rechtsverletzung darstellen. Besonders schwere Rechtsverletzungen drohen, wenn ein Drohnenüberflug (auch) Einblicke in Schlaf- oder Badezimmer, d. h. Bereiche, die der Intimsphäre zuzuordnen sind, ermöglicht. Dem Verletzten stehen in der Folge verschiedene zivilrechtliche Ansprüche, etwa auf Unterlassung oder Schadensersatz, zu. In besonders gravierenden Fällen droht eine strafrechtliche Verfolgung.

7.6 Eigentumsrecht

Der Überflug mit einer Drohne kann den Inhaber des darunterliegenden Grundstücks zudem in dessen Eigentumsrecht im Sinne des Art. 14 GG verletzen. Denn das Eigentum an einem Grundstück erstreckt sich auch auf den Raum über der Erdoberfläche, vgl. § 905 BGB. Wenn ein Luftfahrzeug diesen Luftraum in zulässiger Weise nutzt (§ 1 Abs. 1 LuftVG), muss der Eigentümer

[136] Seit Einführung der DSGVO ist umstritten, ob das KUG (auch) im konkreten Anwendungsbereich der DSGVO noch anwendbar ist.

dies dulden. Für (bestimmte) Drohnen wird die Nutzung des Luftraums aber in vielen Gebieten, etwa über Wohngrundstücken, durch § 21b LuftVO stark eingeschränkt oder untersagt (vgl. Ziffer 7.2). Verletzt der Drohnenpilot diese Vorschriften der LuftVO, ist der Grundstückseigentümer nicht mehr zur Duldung eines Überflugs verpflichtet. In der Folge können dem verletzten Grundstückseigentümer zivilrechtliche Abwehr-, Unterlassungs- und Schadensersatzansprüche zustehen.

7.7 Urheberrecht

Das Anfertigen von Bildern und Videos mit einer Drohne kann auch Urheberrechte verletzen.

Das deutsche Urheberrecht erlaubt die Aufzeichnung der Außenansicht von öffentlichen Gebäuden von öffentlichen Plätzen aus, die sogenannte Panoramafreiheit, § 59 UrhG. Gemeinsames Verständnis des Begriffs „öffentlicher Ort" in diesem Zusammenhang ist die Zugänglichkeit für jedermann ohne Hilfsmittel. Es gab zwar eine Debatte im Zusammenhang mit Google Street View, wenn Bilder von einer höheren Position aus mit Hilfe eines Objektivs aufgenommen werden, aber Luftbilder werden eindeutig nicht durch die Panoramafreiheit abgedeckt.[137] Der primäre Nutzen von Drohnenaufnahmen besteht jedoch in erster Linie in der Möglichkeit, Luftaufnahmen zu machen. Für diese Aufnahmen gilt die Panoramafreiheit nicht, und jede Aufnahme kann eine Verletzung des Urheberrechts darstellen, wenn ein urheberrechtlich geschütztes Werk abgebildet wird.

7.8 Strafrecht

7.8.1 Unternehmensspionage

Das Anfertigen von Aufnahmen, die in der Absicht erstellt werden, geschützte Informationen zu erlangen, kann eine Verletzung von Geschäftsgeheimnissen gemäß §§ 4, 23 GeschGehG darstellen und daher strafbar sein. Dies kann insbesondere Aufnahmen von Betriebsgeländen oder Geschäftsräumen umfassen, die mithilfe einer zivilen Drohne erstellt werden. Nähere Ausführungen zu dem Schutz von Geschäftsgeheimnissen finden sich unter Ziffer 3.1.5.

7.8.2 Verletzung des persönlichen Lebensbereichs und Stalking

Das „allgemeine Recht auf Privatsphäre im persönlichen Lebensbereich" zählt zu den stärksten Rechten im deutschen Recht. Daher können unerlaubte Aufzeichnungen von Personen in geschützten Bereichen nach dem deutschen Strafgesetzbuch strafbar sein.[138]

Häufige Aufnahmen von Personen mit einer Drohne können auch zu einer Strafverfolgung wegen Nachstellung (sog. „Stalking") führen, § 238 StGB.

---

[137] Grübler in: Ahlberg/ Götting, commentary on the copyright act, § 59 Rn. 6.
[138] Umstritten ist, ob bereits die Beobachtung nach § 201a StGB strafbar ist.

7.9 Aktive Verteidigung

Die deutsche und die europäische Gesetzgebung lässt nur in einem engen Rahmen Selbstverteidigung zu. So ist zum Beispiel der Einsatz eines GPS-Störsenders generell verboten.

Das Opfer einer illegalen Drohnenüberwachung kann den Drohnenbetreiber zur Unterlassung auffordern, § 1004 BGB und 823 BGB.[139]

Ein Angriff auf die Drohne selbst oder gar auf den Drohnenpiloten ist in der Regel nur als *ultima ratio* gerechtfertigt, d. h. wenn er zum Schutz substanziell gefährdeter Rechte notwendig ist. Dem (durch die Drohnenüberwachung) Verletzten darf kein milderes und gleich bzw. besser geeignetes Mittel zur Abwehr der Rechtsverletzung zur Verfügung stehen. Der (rechtfertigende) Notstand erfordert zudem zusätzlich auch eine Interessenabwägung. Liegen diese Voraussetzungen im konkreten Einzelfall nicht vor, kann der Einsatz von Gewalt durch den Verletzten selbst strafrechtlich geahndet werden.[141]

Einzelne Gerichte haben sich bereits mit der Selbstverteidigung gegen Drohnen befasst: In einem Urteil des AG Riesa[142] wurde der Abschuss einer ca. 1.500 Euro teuren Drohne mit einem Luftgewehr als Notstandshandlung (§ 228 BGB und § 34 StGB) als gerechtfertigt erachtet. Diese Bewertung kann aber nicht pauschal auf andere Sachverhalte übertragen werden.

7.10 Haftung und Versicherungen

Für Drohnen als „Luftfahrzeuge" im Sinne des LuftVG gelten ähnliche Regeln wie für Kfz, nämlich eine Haftung des Halters, § 33 LuftVG. Das LuftVG sieht auch Regeln für ein Mitverschulden des Geschädigten ebenso wie für Haftungshöchstsummen vor. Die 2017 eingeführte Drohnen-VO enthält keine eigenen Haftungstatbestände.

Unabhängig von ihrem Zweck oder ihrer Größe bzw. Gewicht müssen alle Inhaber ziviler Drohnen eine Haftpflichtversicherung abschließen, § 43 LuftVG. Einige allgemeine Haftpflichtversicherungen, insbesondere ältere Policen, decken Schäden durch Drohnen nicht ab. Daher hat sich ein Markt für spezielle Versicherungen auch für Drohnen herausgebildet.

---

139 Z. B. Urteil vom 16. April 2015, Amtsgericht Potsdam, BeckRS 2016, 00017.

140 §§ 32 ff. StGB und §§ 227 ff. BGB könnten Angriffe auf die Drohne oder ihren Piloten rechtfertigen, z. B. aus Gründen der Selbstverteidigung; insbesondere nach § 34 StGB und § 228 BGB.

141 Angriffe gegen die Drohne sind in der Regel nach § 303 StGB strafbar; Angriffe gegen den Piloten werden z. B. nach §§ 223 ff. StGB oder § 240 StGB bestraft.

142 Urteil vom 24. April 2019 des AG Riesa (9 Cs 926 Js 3044/19): Abschuss der Drohne mit einem Luftgewehr.

8. Intelligente Autos (Smart Cars)

8.1 Aktueller Stand

Roboter im Mobilitätssektor werden bereits seit einigen Jahren in kontrolliertem Umfeld zur Personenbeförderung erprobt und eingesetzt.[143] Erheblich komplexer gestaltet sich jedoch die Entwicklung von autonomen Autos, sog. intelligente Autos oder auch „Smart Cars", die weitgehend uneingeschränkt im gesamten öffentlichen Verkehr eingesetzt werden sollen.

Es gibt verschiedene Definitionsansätze für diese intelligenten Autos. Eine international anerkannte Grundlage ist die 5-stufige Einteilung nach sog. „SAE J3016", einem von der SAE International[144] erarbeiteten Standard.

Bei den niedrigsten beiden Stufen assistiert das Fahrzeugsystem bei einzelnen Vorgängen wie Einparken, Spurhalten, Beschleunigen und Abbremsen bzw. übernimmt diese. Die Vorgänge muss der Fahrer allerdings ständig im Blick behalten und bei Bedarf korrigieren. Die Beaufsichtigung des Fahrzeugs durch den Fahrer ist bei der Stufe 3, dem „hochautomatisierten Fahren", bereits gelockert. Das System übernimmt die Fahrzeugführung, sodass der Fahrer nur bereit sein muss, auf Aufforderung des Systems die Führung zu übernehmen. Bei Stufe 4, dem „vollautomatisierten Fahren", wird das Fahrzeug automatisiert in einem risikominimierenden Betrieb zurückgefahren, z. B. zum Anhalten, wenn die Fahraufgaben vom System nicht mehr bewältigt werden können und der Fahrer trotz Aufforderung nicht die Kontrolle übernimmt. Die fünfte und höchste Stufe ist das „autonome Fahren" im eigentlichen Sinne, bei dem im Fahrzeug kein Fahrer vorhanden sein muss. Alle Insassen sind hier lediglich Passagiere. Bis auf das Starten des Systems und die Eingabe eines Ziels ist kein menschliches Handeln mehr erforderlich; das System kann die Fahraufgaben allesamt eigenständig ausführen.

An dieser Stufeneinteilung hat sich auch der deutsche Gesetzgeber, etwa in §§ 1a und 1b StVG, orientiert, obgleich er bislang die fünfte Stufe noch nicht geregelt hat.[145]

Während Teilautomatisierungssysteme wie Spurhaltesysteme, Notbremsassistenten und Adaptive Cruise Control-Systeme[146] bereits auf der alltäglichen Fahrt vielfach zum Einsatz kommen,[147] befinden sich Fahrzeuge mit Automatisierungsgrad von Stufe 3 (oder höher) in Deutschland aktuell nur in Testphasen. Erste Versuche, Fahrzeuge mit den entsprechenden Funktionen zum „hochautomatisierten Fahren" (Stufe 3) in den Verkehr zu bringen, sind bislang an der Zulassung

---

143 Z. B. Autonome U-Bahnen in Nürnberg: https://www.sueddeutsche.de/bayern/verkehr-so-funktioniert-die-fahrerlose-u-bahn-in-nuernberg-1.3445130 und Tests von fahrerlosen Minibussen wie auf dem Campus der Berliner Charité: https://www.charite.de/service/pressemitteilung/artikel/detail/bvg_und_charite_testen_autonome_kleinbusse/.

144 Internationale Berufsvereinigung von Ingenieuren, die Standards für Mobilitätstechnologien entwickelt, https://www.sae.org/.

145 BTDrs. 18/11300, S.12 f; BMVI: https://www.bmvi.de/SharedDocs/DE/Publikationen/G/kompakt-automatisiertes-fahren.pdf?__blob=publicationFile.

146 Automatische Abstandsregelungssysteme, die mittlerweile auch für Motorräder eingesetzt werden, z. B. von BMW, https://www.bmw-motorrad.de/de/engineering/detail/comfort-ergonomics/acc.html#/section-de45b78f-section.

147 Notbrems- und Geschwindigkeitsassistenz sind ab 6. Juli 2022 für neu zugelassene Fahrzeuge vorgeschrieben, Art. 6 ff. der Verordnung (EU) 2019/2144.

gescheitert.[148] In Deutschland gibt es mittlerweile mehrere Teststrecken für vernetzte und automatisierte Fahrzeuge. So etwa in Hamburg, wo eine ca. neun Kilometer lange Strecke entstand, deren Errichtung vom BMVI mit 10,7 Mio. Euro gefördert wurde.[149] Wann vollautomatisierte Systeme marktreif sind, lässt sich derzeit aber weiterhin nicht zuverlässig prognostizieren.

8.2 Fahrzeug-Registrierung

8.2.1 Wiener Übereinkommen über den Straßenverkehr

Auf internationaler Ebene gibt das Wiener Übereinkommen über den Straßenverkehr[150] einen groben Rahmen für die Zulassung von automatisierten Fahrzeugen vor, dem nationale Regelungen entsprechen müssen. Das Wiener Übereinkommen folgt dem Grundgedanken, dass jedes Fahrzeug einen verantwortlichen Fahrzeugführer haben muss. Seit 2016 dürfen bestimmte Fahrzeugsysteme die Führung eines Fahrzeugs aber zumindest beeinflussen.[151] Voraussetzung dafür ist, dass diese Fahrzeugsysteme den internationalen Rechtsvorschriften für Kraftfahrzeuge entsprechen oder vom Fahrer überbrückt bzw. ausgeschaltet werden können. Für Lenkanlagen von Fahrzeugen ist die UN/ECE-Regelung Nr. 79[152] maßgeblich, die bestimmte automatisierte Anlagen zulässt, allerdings die Hauptverantwortlichkeit beim Fahrer belässt, der über die Vorgänge der Lenkanlage informiert werden und diese jederzeit deaktivieren können muss.

Der Fahrer muss daher grundsätzlich weiterhin jederzeit den Betrieb des Fahrzeugs überwachen. Das „autonome Fahren" (Stufe 5) ist nach den internationalen Regelungen nach wie vor unzulässig.

Als internationaler Vertrag bindet das Wiener Übereinkommen die Bundesrepublik Deutschland nicht direkt, verpflichtet sie aber zur Umsetzung der Vorschriften.

Die UN/ECE hat überdies im Oktober 2019 Empfehlungen zur Unterstützung des sicheren, weltweiten Einsatzes von hoch- und vollautomatisierten Fahrzeugen im Straßenverkehr veröffentlicht.[153]

8.2.2 Aktuelle Rechtslage in Deutschland

Nach § 3 der deutschen Fahrzeugzulassungsverordnung (**FZV**) benötigt jedes Fahrzeug eine Zulassung zum Straßenverkehr, wofür das Fahrzeug entweder über eine EG-Typgenehmigung nach der europäischen Verordnung (EU) 2018/858 oder eine allgemeine Betriebserlaubnis nach der Straßenverkehrs-Zulassungs-Ordnung verfügt.

---

148 https://www.faz.net/aktuell/wirtschaft/fahren-ohne-lenkrad-autonomes-auto-16605395.html.
149 https://www.bmvi.de/SharedDocs/DE/Artikel/K/teststrecke-hamburg-automatisiertes-fahren.html.
150 Ratifiziert von Deutschland 1998, zuvor von der ehemaligen BRD und DDR 1982.
151 Art. 8 Abs. 5[bis] des Wiener Übereinkommens über den Straßenverkehr trat am 23. März 2016 in Kraft und ist seither für die Vertragsstaaten völkerrechtlich verbindlich.
152 Die UN/ECE-Regeln sind ein Regelwerk der Wirtschaftskommission für Europa der Vereinten Nationen („United Nations Economic Commission for Europe", **UNECE**), das grenzüberschreitende technische Standards für die Zulässigkeit von Fahrzeugen, Teilen und Ausrüstungsgegenständen schaffen soll. Die Regelungen sind für die Mitgliedstaaten der Europäische Union verbindlich. Zur UN/ECE-Regelung Nr. 79, https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2018/R079r4e.pdf.
153 Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic, https://www.unece.org/fileadmin/DAM/trans/main/wp1/wp1doc/WP1_Resolution_Brochure_EN_web.pdf.

Mit dem Achten Gesetz zur Änderung des Straßenverkehrsgesetzes wurden Regelungen zum Fahren von Kfz mit hoch- und vollautomatisierter Fahrfunktion (§§ 1a, 1b, 1c StVG) in die StVG eingefügt. Darin wird festgelegt, dass Kfz mit hoch- oder vollautomatisierten Systemen im Verkehr auf öffentlichen Straßen eingesetzt und genutzt werden können, wenn der Fahrzeugführer dem System unter bestimmten Umständen die Steuerung des Fahrzeugs übergeben kann. Der Betrieb eines Kraftfahrzeugs durch hoch- oder vollautomatisierte Fahrfunktionen ist nur dann zulässig, wenn die Funktionen bestimmungsgemäß verwendet werden. Sieht die Systembeschreibung des Herstellers für eine automatisierte Fahrfunktion etwa nur den Einsatz auf Autobahnen vor, handelt es sich nicht um eine bestimmungsgemäße Verwendung, wenn diese Fahrfunktion auf anderen Straßenarten genutzt wird. Der Fahrer ist verpflichtet, sich über den bestimmungsgemäßen Gebrauch zu informieren.[154]

8.2.3 Ausblick

Hinsichtlich einer Zulassung der höchsten Automatisierungsstufe, dem „autonomen Fahren", müsste das Wiener Übereinkommen geändert werden, oder Deutschland muss das Wiener Übereinkommen „außer Kraft setzen"[155] und seine nationale Gesetzgebung ändern, da dem Wiener Übereinkommen nach wie vor die Vorstellung zugrunde liegt, dass jedes Fahrzeug einen Fahrzeugführer benötigt. Das Wiener Übereinkommen wurde in der Vergangenheit bereits mehrfach, zuletzt im Jahr 2014 mit Blick auf die Zulassung von teilautomatisierten Fahrfunktionen, geändert. Wir halten es für wahrscheinlich, dass diese Änderungen nur Zwischenschritte auf dem Weg zu der Zulassung von vollautomatisierten Fahrzeugen darstellen.

8.3 Haftung

8.3.1 Haftung des Fahrzeughalters – Haftung des Fahrzeugführers

Grundsätzlich ist der **Halter** eines Fahrzeugs für Personen- und Sachschäden schadenersatzpflichtig, § 7 StVG. Er haftet daher auch für Schäden, die durch die Nutzung eines automatisierten Systems entstehen. Der Betrieb von Fahrzeugen mittels „hoch- oder vollautomatisierter Fahrfunktion" ist mittlerweile explizit geregelt (§§ 1a, 1b StVG). Er ist dann zulässig, wenn die jeweilige Funktion „bestimmungsgemäß verwendet wird." Der Fahrzeugführer darf sich gegebenenfalls sogar „vom Verkehrsgeschehen und der Fahrzeugsteuerung abwenden", wenn er hinreichend wahrnehmungsbereit bleibt, um jederzeit die Fahrzeugführung wieder aufzunehmen. Autonome Systeme, die gänzlich fahrerlos funktionieren, sind hingegen nicht gesetzlich erlaubt.[156]

Neben dem Fahrzeughalter kann auch der **Fahrer** für Schäden haftbar gemacht werden. Seine Haftung wird nur dann ausgeschlossen, wenn er nachweisen kann, dass ihm kein Verschulden zur Last fällt, § 18 StVG. Wie oben dargestellt, darf sich der Fahrzeugführer zwar vom Verkehrsgeschehen und der Fahrzeugsteuerung abwenden, wenn er ein hoch- oder vollautomatisiertes System nutzt. Er muss dabei allerdings hinreichend wahrnehmungsbereit bleiben, um jederzeit

---

154 Klink-Straub/Keber, NZV 2020, 113.
155 Möglich nach Abschnitt 50 des Wiener Übereinkommens.
156 Vgl. Hoeren/Böckers, JurPC Web-Dok. 21/2020 Abs. 28.

die Fahrzeugsteuerung wieder zu übernehmen, § 1b StVG. Der Fahrer haftet also gegebenenfalls nach den bisherigen Regelungen, aber sein Sorgfaltsmaßstab wird durch § 1b StVG besonders definiert.

Diese Pflichten des Fahrers, die sich auf „hoch- und vollautomatisierte Fahrfunktionen" beziehen, dürften allerdings nicht das derzeit übliche assistierte oder teilautomatisierte Fahren meinen.[157] Diese Automatisierungsgrade sind vielmehr ohnehin erlaubt. Bezogen auf das sogenannte SAE-Modell[158] decken die Regelungen des StVG die Stufen 3 und 4 ab (vgl. oben Ziffer 8.1), während derzeit übliche Systeme auf den Stufen 1 und 2 angesiedelt sind.[159] Nach dem Modell des Bundesverkehrsministeriums wird zwischen assistiertem, teilautomatisiertem, hochautomatisiertem, vollautomatisiertem und (mittlerweile) autonomem Fahren unterschieden.[160] Auf diese Unterscheidung bezog sich der Gesetzgeber auch bei der Schaffung der §§ 1a und 1b StVG,[161] sodass auch hiernach davon auszugehen ist, dass die derzeit üblichen assistierenden und teilautomatisierten Systeme nicht von §§ 1a, 1b StVG erfasst sind.

Im Einzelfall ist jedoch immer zu prüfen, ob ein System nicht doch der gesetzlichen Definition von hoch- und teilautomatisierten Funktionen unterfällt – und damit der Sorgfaltsmaßstab des Fahrers nach § 1b StVG konkretisiert wird.

8.3.2 Haftung bei Nutzung autonomer Systeme

Wie dargestellt, ist für die Verwendung **gänzlich autonomer Systeme** aktuell noch keine besondere Regelung getroffen. Sie sind damit derzeit unzulässig. Hinsichtlich der Haftung bei solchen Systemen ergäbe sich ggf. auch ein Spannungsfeld zwischen der vermuteten Haftung des „Fahrers" (den es bei autonomen Systemen strenggenommen nicht mehr gibt), der Halterhaftung und einer möglichen Haftung des Herstellers des autonomen Fahrzeugs: Je autonomer die Systeme, desto weniger ist ein Schaden dem „Fahrer"/"Bediener" oder Halter zuzurechnen. Gesetzlich ist bislang gerade nicht vorgesehen, dass Fehler, die von der Beschaffenheit des Fahrzeugs herrühren, zu einem Ausschluss von Haftungsansprüchen führen, vgl. § 17 Abs. 3 StVG.

Für den Fall einer Verwendung autonomer Systeme könnte es notwendig werden, die **Beweisregeln** anzupassen (sofern weiterhin eine Haftung des „Fahrers"/"Bedieners" vorgesehen sein sollte) und/oder spezifische Ausnahmen für die Halterhaftung vorzusehen, wie sie bereits in § 8 StVG für andere Sachverhalte vorgesehen sind. Insoweit erscheint auch der Vorschlag, Black Boxes für autonome System vorzusehen,[162] durchaus diskutabel: Damit könnten möglicherweise ein tatsächlicher Nachweis über das Verschulden geführt und langwierige juristische Auseinandersetzungen potenziell abgekürzt werden.

---

157 So auch Klink-Straub/Keber, NZV 2020, 113, 114.
158 Society of Automotive Engineers (SAE International), Norm J3016., https://www.sae.org.
159 Vgl. Roos/Siegmann, Working Paper Forschungsförderung No. 188: Technologie Roadmap für das automatisierte Autofahren, Juli 2020; Klink-Straub/Keber, NZV 2020, 113, 114.
160 Vgl. Bericht des vom Bundesverkehrsministerium eingesetzen „Runden Tisch Automatisiertes Fahren", 2015; Bericht der Bundesanstalt für Straßenwesen, Heft F83, S. 9 und 32.
161 BT-Drs. 18/11300, S. 12 f.
162 Die von der EU-Kommission eingesetzte High Level Group „GEAR 2030" hat 2017 erwogen, Datenspeicher (Black Boxes) als Voraussetzung für die Typenzulassung eines Fahrzeugs mit automatisierten Systemen zu verlangen, um nach einem Unfall bestimmen zu können, ob der Fahrer oder das Fahrzeug das Fahrzeug führte; High Level Group GEAR 2030, Final Report 2017, S. 44.

8.3.3 Datenspeicherung bei hoch- und vollautomatisierten Funktionen, Haftungshöhe

Der deutsche Gesetzgeber hat bereits 2017 eine **Datenspeicherung** (für „hoch- und vollautomatisierte Fahrfunktionen") gesetzlich festgeschrieben, § 63a StVG.[163] Hiernach sind Positions- und Zeitangaben zu speichern, wenn die Fahrzeugsteuerung zwischen Fahrer und dem automatisierten System gewechselt wird. Die Daten dürfen an Behörden bei Verkehrsverstößen sowie an Dritte in Haftungsfällen übermittelt werden. Viele Einzelheiten hinsichtlich dieser Regelung sind noch unklar, insbesondere ob die Daten im Fahrzeug – wie in einer Black Box – oder außerhalb des Fahrzeugs, beispielsweise beim Hersteller oder Dritten, zu speichern sind. Es ist denkbar, dass der Gesetzgeber hierzu, wie auch zu anderen Einzelfragen zum automatisierten Fahren, von der neu geschaffenen Verordungsermächtigung in § 6 Abs. 4a StVG Gebrauch macht und derlei Details in einer Rechtsverordnung regelt.

Die **Haftungshöhe** wurde ebenfalls angepasst: Wird ein Schaden aufgrund der Verwendung einer hoch- oder vollautomatisierten Fahrfunktion verursacht, gilt ein verdoppelter Höchstbetrag für die Haftung des Ersatzpflichtigen, nämlich von zehn Mio. Euro (Personenschäden) und zwei Mio. Euro (Sachschäden), § 12 Abs. 1 Satz 1 StVG.

8.3.4 Produkt- und Produzentenhaftung

Neben der Halter- und Fahrerhaftung kann auch eine Haftung des Herstellers eines automatisierten Fahrzeugs oder Systems in Betracht kommen.

Wie bereits unter Ziffer 2 dargestellt, sind hier die (verschuldensunabhängige) Herstellerhaftung nach dem ProdHaftG (Produkthaftung) bzw. die (verschuldensabhängige) Produzentenhaftung nach § 823 Abs. 1 BGB einschlägig.

Für Ansprüche aus **Produkthaftung** gilt als Hersteller, wer das (gegebenenfalls zusammengesetzte) Endprodukt in Verkehr bringt. Bei automatisierten Fahrzeugen ist dies üblicherweise der Fahrzeughersteller. Zulieferer, die ein automatisiertes System liefern und dieses als von sich stammend kennzeichnen, können ebenfalls als Hersteller gelten und haften, sofern der Fehler nicht auf den Anforderungen des Herstellers des Endprodukts beruht. Inwieweit Software ein „Produkt" im Sinne des ProdHaftG ist und insoweit der Hersteller von Software hiernach haftet, ist umstritten, wird im Zuge der Digitalisierung aber von einigen Stimmen befürwortet; derzeit unterfällt reine Software nach dem Gesetzeswortlaut allerdings wohl nicht dem ProdHaftG. Entsprechend der oben unter Ziffer 2 dargestellten Entwicklungen auch auf europäischer Ebene könnte Software jedoch in absehbarer Zukunft auch der Produkthaftung unterworfen werden.

Hinsichtlich der Fehler kann, wie im Rahmen der Produzentenhaftung, nach **Konstruktions-, Fabrikations- und Instruktionsfehlern** unterschieden werden (Details hierzu sogleich).[165] Der Geschädigte hat den Fehler, den Schaden und den ursächlichen Zusammenhang zwischen Fehler

---

[163] Fahrer sollen hiermit explizit in die Lage versetzt werden, Schuldvorwürfe gegen sie mittels der Daten entkräften zu können; BT-Drs. 18/11300, S. 24.
[164] Ausführlich Hoeren/Böckers, JurPC Web-Dok. 21/2020 Abs. 51 ff.
[165] MüKoBGB/Wagner, 8. Aufl. 2020 Rn. 41, ProdHaftG § 3 Rn. 41.

und Schaden zu beweisen. Die Haftung könnte für den Hersteller bei automatisierten Fahrzeugen insbesondere dann ausgeschlossen sein, wenn der Hersteller gesetzliche Vorgaben beachtet hat und der Fehler hierauf beruht, § 1 Abs. 2 Nr. 4 ProdHaftG, oder der Fehler nach dem Stand der Wissenschaft und Technik nicht erkannt werden konnte, § 1 Abs. 2 Nr. 5 ProdHaftG. In letzterem Fall könnten aber Ansprüche wegen späterer Verletzung einer Produktbeobachtungspflicht nach der Produzentenhaftung in Betracht kommen (hierzu sogleich).

Auch vorliegend gelten im Rahmen der **Produzentenhaftung** die bekannten Kategorien, d. h. insbesondere Konstruktions-, Fabrikations- und Instruktionsfehler sowie Produktbeobachtungspflichten. Der Geschädigte muss im Rahmen der Produzentenhaftung grundsätzlich alle Anspruchsvoraussetzungen beweisen, somit auch die Pflichtverletzung und das Verschulden des Herstellers. Hierbei könnten ihm angesichts der Komplexität und Opazität automatisierter Systeme im Einzelfall aber Beweiserleichterungen zugutekommen. Eine Rolle könnte dabei bei hoch- und vollautomatisierten Systemen die Pflicht zur Datenspeicherung nach § 63a StVG spielen.

Ein „**Konstruktionsfehler**" liegt vor, wenn das Produkt schon seiner Konzeption nach unter dem gebotenen Sicherheitsstandard bleibt, d. h. bereits im Rahmen seiner Entwicklung die gebotenen Sicherheitsvorkehrungen unterblieben sind.[166] Fraglich ist insoweit, welche sogenannte Konstruktionssorgfalt geschuldet wird. Nicht jeder Unfall kann unmittelbar einen Verstoß gegen die Sorgfaltspflichten des Herstellers bedeuten. In jedem Fall dürften aber Verstöße gegen technische Normen einschließlich der einschlägigen EN- und DIN-Normen als haftungsbegründender Pflichtverstoß des Herstellers gelten. Werden technische Standards eingehalten, bedeutet dies allerdings nicht in jedem Fall eine Enthaftung des Herstellers. Vielmehr dürften auch hier Produktbeobachtungspflichten bestehen.

Ein „**Fabrikationsfehler**" ist die Abweichung von den definierten Sicherheitsstandards der Produktserie.[167]

Ein „**Instruktionsfehler**" wird angenommen, wenn der Verwender nicht oder nur unzureichend über die Art und Weise der Verwendung und die damit verbundenen Gefahren aufgeklärt wird.[168] Insoweit können bei automatisierten Fahrzeugen gesteigerte Informationspflichten bestehen. In jedem Fall muss der Hersteller sicherstellen, dass der Fahrer so über die mitunter komplexen Funktionen informiert wird, dass er sie angemessen nachvollziehen und das Fahrzeug sicher führen kann.[169]

Zu **Produktbeobachtungspflichten** siehe bereits oben unter Ziffer 2. Je mehr (verwertbare) Daten ein Fahrzeug ermittelt, umso „einfacher" könnte sich die Produktbeobachtung gestalten – und umso eher eine solche Pflicht gelten. Gegebenenfalls muss der Hersteller hiernach eingreifen und eine Warnung aussprechen oder einen Rückruf, gegebenenfalls unter Durchführung von Updates, vorzunehmen.

---

166 BGH NJW 2013, 1302, 1303.
167 MüKoBGB/Wagner, 8. Aufl. 2020, ProdHaftG § 3 Rn. 42.
168 MüKoBGB/Wagner, 8. Aufl. 2020, ProdHaftG § 3 Rn. 46.
169 Vgl. Lutz/Tang/Lienkamp, NZV 2013, 57, 61.

8.3.5 Haftung bei automatisierter Beförderung

Sollte es in Zukunft vermehrt zur automatisierten Beförderung kommen, könnten sich auch hierbei vermehrt Haftungsfragen ergeben. Geschädigte dürften in diesen Fällen allerdings zunächst maßgeblich versuchen, vertragliche Ansprüche geltend zu machen: Bei vertraglichen Ansprüchen muss der Geschädigte zwar die Pflichtverletzung beweisen; wenn ihm dies gelingt, muss aber gegebenenfalls der Vertragspartner beweisen, dass er diese Pflichtverletzung nicht verschuldet hat. Dies könnte für den Anspruchsgegner faktisch zu einer Offenlegungspflicht hinsichtlich der entscheidungsrelevanten Systeme führen.

8.3.6 Fazit

Die Haftung für Schäden, die bei dem Einsatz automatisierter Fahrzeuge entstehen, unterscheidet sich strukturell nicht von dem bisher bekannten Haftungsregime. Weiterhin haften grundsätzlich Halter und Fahrer, gegebenenfalls auch der Hersteller. Bereits erfolgte gesetzliche Weiterentwicklungen führen allenfalls zu Modifikationen dieses Haftungssystems. Eine eindeutigere Zuordnung einer Pflichtverletzung – menschliches Versagen oder technischer Fehler – könnte tatsächlich über Datenspeicher erfolgen und dem Geschädigten insbesondere Ansprüche gegen den Hersteller erleichtern (ebenso wie dem Fahrer der Nachweis mangelnden Verschuldens). Beweislastfragen dürften aufgrund der Komplexität und Opazität automatisierter Systeme künftig eine verstärkte Rolle spielen, möglicherweise auch für die Gesetzgebung.

In Deutschland wird derzeit allerdings kein gesetzgeberischer Handlungsbedarf hinsichtlich der Haftung bei einem Unfall mit einem automatisierten Fahrzeug gesehen.[170] Entsprechend dürfte es allenfalls zu Anpassungen seitens der Rechtsprechung kommen. Ob mit einem Anstieg der Herstellerhaftung und einem Rückgang der verschuldensbasierten Fahrerhaftung gerechnet werden kann,[171] ist derzeit noch fraglich, erscheint mit zunehmender Automatisierung aber denkbar.

8.4 Versicherungen

Nach dem deutschen Pflichtversicherungsgesetz (PflVG) muss der Fahrzeughalter eine Versicherung für sich und den Fahrzeugführer abschließen. Der Geschädigte kann Schadenersatz direkt bei der Haftpflichtversicherung geltend machen, § 115 Versicherungsvertragsgesetz (VVG).

Damit auch bei hoch- und vollautomatisierten Fahrzeugen die gesetzliche Versicherungspflicht gewahrt ist, müssen Kfz-Versicherungen auch Fahrzeuge mit hoch- und vollautomatisierten Systemen erfassen. Dies dürfte sich auf die Versicherungsprämien auswirken – im Positiven wie im Negativen, sind hoch- und vollautomatisierte Fahrzeuge doch nicht nur besonders gefahrgeneigt, sondern könnten möglicherweise auch die Zahl und Intensität von Unfällen und damit Haftungsfällen verringern.

---

[170] Klink-Straub/Keber, NZV 2020, 113, 119.
[171] Hilgendorf, JA 2018, 801; Klink-Straub/Keber, NZV 2020, 113, 115.

Wie bereits unter Ziffer 8.3.3 erwähnt, wurde die Haftungshöhe allerdings zunächst gesetzlich erhöht: Wird ein Schaden aufgrund der Verwendung einer hoch- oder vollautomatisierten Fahrfunktion verursacht, gilt ein verdoppelter Höchstbetrag für die Haftung des Ersatzpflichtigen, nämlich von zehn Mio. Euro (Personenschäden) und zwei Mio. Euro (Sachschäden), § 12 Abs. 1 Satz 1 StVG. Dies dürfte entsprechend zunächst zu Erhöhungen der Versicherungsprämien führen.

Sollte sich – neben der Halter- und Fahrerhaftung nach StVG – das Haftungsrisiko für die *Hersteller* von Fahrzeugen mit hochautomatisierten und vollautomatisierten Systemen erhöhen, beispielsweise aufgrund gesetzlicher Änderungen beim Haftungsrahmen oder einer erleichterten Produzentenhaftung, liegt es nahe, dass Versicherungsgesellschaften spezielle Versicherungen für Autohersteller entwickeln werden.

8.5 Ordnungswidrigkeiten und Strafrecht

Sowohl das geltende Gesetz über Ordnungswidrigkeiten als auch das Strafrecht beziehen sich auf eine Verletzung der Sorgfaltspflicht durch den Fahrzeugführer. Wenn das Fahrzeug jedoch von einem hochautomatisierten oder vollautomatisierten System gesteuert wird, ist fraglich, ob den Fahrzeugführer weiterhin eine Sorgfaltsplicht in Bezug auf die Einhaltung der Verkehrsregeln oder die Beobachtung der Verkehrsvorgänge trifft. Wenn das hochautomatisierte oder vollautomatisierte System etwa ein „Stoppschild" oder eine rote Ampel missachtet, kann der Fahrzeugführer eine Sorgfaltsplicht nur dann durch Unterlassen verletzen, wenn er zum Handeln und Eingreifen, z. B. zum manuellen Anhalten oder Abbremsen des Fahrzeugs, verpflichtet gewesen wäre.

Mit § 1 b StVG wurden erstmalig „Rechte und Pflichten des Fahrzeugführers bei Nutzung hoch- oder voll automatisierter Fahrfunktionen" durch den Gesetzgeber geregelt. Danach soll der Fahrzeugführer sich zwar abwenden dürfen, muss aber gleichzeitig wahrnehmungs- und übernahmebereit bleiben. Eine Verletzung dieser Fahrzeugführerpflichten kann eine Sorgfaltspflichtverletzung darstellen und daher zu einer Strafbarkeit führen.

Da durch die technische Entwicklung des automatisierten Fahrens der Kraftfahrzeugführer schrittweise ersetzt werden soll, erscheint es gut vorstellbar, dass die an der Herstellung der Technik befassten Menschen der „Chain of Supply" (Hersteller, Konstrukteure, Programmierer usw.) in den Fokus einer möglichen Strafbarkeit rücken.[172] Relevant sollte hier vorrangig eine Fahrlässigkeitsstrafbarkeit sein. Es wird hierzu teilweise eine Anwendung der Rechtsprechung des BGH zum „Ledersprayfall"[173] und zum „Holzschutzmittelfall"[174] vertreten. Wer danach als Hersteller oder Händler ein Produkt in Verkehr bringt, dessen bestimmungsgemäßer Einsatz entgegen berechtigter Erwartungen die Gefahr eines Schadens begründet, ist zur Schadenabwendung verpflichtet. Dadurch wird eine Garantenstellung begründet, so dass ein Unterlassen letztlich in eine Strafbarkeit münden kann.[175] Der Sorgfaltsmaßstab des Herstellers ist dabei jedoch auf das

[172] Staub: Strafrechtliche Fragen zum Automatisierten Fahren, NZV 2019, 392.
[173] BGHSt 37, 106.
[174] BGHSt 41, 206.
[175] Nehm: Autonomes Fahren – Bremsen Ethik und Recht den Fortschritt aus? , JZ 2018, 398; Staub: Strafrechtliche Fragen zum Automatisierten Fahren, NZV 2019, 392.

erlaubte Risiko[176] begrenzt, solange der Hersteller alles unternimmt, um seine verbauten Systeme im Rahmen des Zumutbaren so sicher wie möglich zu gestalten.[177]

8.6 Eigentum an Fahrzeugdaten

Für intelligente Autos müssen naturgemäß riesige Datenmengen über das Auto selbst, aber auch über seine Umgebung erhoben und verarbeitet werden, um eine sichere Navigation durch den Verkehr zu gewährleisten. Diese Daten können sowohl für den Fahrzeughersteller als auch für andere Parteien wie Fahrzeugvermieter, Versicherer und Fuhrparkmanagement-Betreiber von erheblichem Wert sein. Die Frage des Eigentums an Daten und der daraus erwachsenden (ausschließlichen) Nutzungsrechte an den Daten ist eines der meistdiskutierten Themen im Zeitalter von Big Data.

Die Daten als solches werden regelmäßig keinen Schutz nach dem deutschen Urheberrecht genießen. Zumeist wird das Erfassen und Verwenden der Daten keinen hinreichenden, schöpferischen Akt darstellen, da das Erfassen und Sammeln nur auf einem mechanisch-technischen Vorgang beruht, der durch die technische Funktion des Fahrzeugs vorgeben und damit gerade kein originelles Werk ist.

Im Einzelfall können die Daten zumindest als einfache Datenbank einem eingeschränkten Leistungsschutzrecht nach §§ 87a ff. UrhG unterliegen. Einzeln kommt den Daten nur ein begrenzter Aussagegehalt zu, sodass der wesentliche Wert der Daten erst aus der Sammlung, Aufbereitung und Zuordnung der Daten zum spezifischen Fahrzeugsystem resultiert. Die entsprechend zusammengetragenen Daten können dem Leistungsschutzrecht für Datenbanken unterfallen, wenn bezüglich der auch einzeln informationshaltigen Daten wesentliche Investitionen getätigt werden, um die Daten zu beschaffen, zu überprüfen sowie aufzubereiten und darzustellen. Keine Relevanz haben dabei aber Investitionen zum Erzeugen der Daten, sodass der Aufwand für die Entwicklung, Herstellung und Unterhaltung des Fahrzeugsystems außer Betracht bleibt.[178]

Der Schutz durch das Leistungsschutzrecht ist allerdings begrenzt. Dritten werden nur bestimmte Maßnahmen mit den Daten untersagt, nämlich das Vervielfältigen, Verbreiten oder öffentliche Wiedergeben wesentlicher Teile der Datenbank. Auf andere Art oder mit nur unwesentlichen Teilen der Datenbank können Dritte uneingeschränkt verfahren. Schließlich steht gesetzlich nur dem Hersteller der Datenbank, der die betreffenden Investitionen verantwortet, das Schutzrecht zu. Da ein Automobilhersteller nicht immer eigene Systeme entwickeln und betreiben wird, sollten die Rechte an den Daten und etwaige Zugriffsmöglichkeiten und -beschränkungen in der Regel vertraglich mit dem Hersteller bzw. Betreiber des verbauten Systems geklärt werden.

---

176 Ein Hersteller riskanter technischer Produkte handelt nicht fahrlässig, wenn nach der in der Rechtsgemeinschaft vorherrschenden Meinung der mit den technischen Produkten verbundene Nutzen so groß ist, dass Schädigungen in Kauf genommen werden können. Dies galt z. B. beim sog. „Aschaffenburger Fall", wo es wegen eines funktionierenden Spurhalte-Assistenten zu einem Unfall kam, wobei dieser gleichzeitig eine Vielzahl von Unfällen verhindern kann.

177 Hilgendorf: Automatisiertes Fahren und Recht – ein Überblick, JA 2018, 801.

178 EuGH, Urteil vom 9.11.2004 – Rs. C-203/02.

8.7 Datenschutzrecht

Die Nutzung hochautomatisierter und vollautomatisierter Systeme wirft verschiedene Fragen des Schutzes der Privatsphäre auf.[179] Moderne Fahrzeuge enthalten bereits eine Vielzahl von Sensoren und Steuergeräten, die verschiedenste Daten erfassen,[180] und die Zahl steigt mit zunehmendem technischen Fortschritt. Hinzu kommt, dass eingebaute Systeme immer stärker vernetzt werden. Auf diese Weise können Autos mit ihrer Umgebung (andere Automobile, Fußgänger, Infrastrukturen, Hersteller und Dienstleister) kommunizieren.

Intelligente Autos sind natürlich in der Lage, mittels Sensoren, Kameras, Mikrofonen usw. noch einmal deutlich größere Datenmengen über das Auto selbst, aber auch über seine Umgebung zu verarbeiten, damit sie sicher durch den Verkehr navigieren können. Diese Daten werden in vielen Fällen einen Personenbezug aufweisen, etwa zum Fahrzeugführer, zu Mitfahrern, zu anderen Verkehrsteilnehmern oder sogar zu Nicht-Teilnehmern. Diese personenbezogenen Daten unterfallen den Regelungen der DSGVO und des BDSG (vgl. Ziffer 4.1). Hierzu zählen auch bloße technische Informationen zum Fahrzeug, wenn sie die Identifizierung einer natürlichen Person mithilfe weiterer verfügbarer Daten zulassen. Ein solcher Personenbezug kann je nach Einzelfall z. B. über miterfasste Standortdaten, Log-Files des Fahrzeugs oder mit dem Fahrzeug per Bluetooth verbundene Handys möglich werden.

Die erfassten Daten werden in der Regel auf den Speichermedien der einzelnen Fahrzeuge gespeichert, in vielen Fällen aber auch in einem Cloud-Speicher, der vom oder durch den Fahrzeughersteller bereitgestellt wird. Die DSGVO gilt für diese Fälle gleichermaßen, insbesondere auch, wenn zur Verarbeitung der Daten Server eines Dienstleisters mit Sitz außerhalb der EU bzw. des EWR genutzt werden (vgl. Ziffer 4.1.5).

Wie bereits ausführlich erläutert, dürfen personenbezogene Daten nur erhoben, verarbeitet und genutzt werden, wenn eine gesetzliche Rechtfertigung nach Art. 6 Abs. 1 DSGVO vorliegt (vgl. Ziffer 4.1.2). Von besonderer Relevanz als Rechtfertigungsgrundlage sind auch im Bereich „Smart Cars" die Einwilligung des Betroffenen, die Vorbereitung und Erfüllung eines Vertrages mit dem Betroffenen und überwiegende berechtigte Interessen des Verantwortlichen. Zur Evaluierung der richtigen Rechtsgrundlage müssen die konkreten Verarbeitungsprozesse mitsamt ihrem Umfang und den Zwecken der Verarbeitung untersucht werden.

Besonders komplex gestaltet sich die Rechtfertigung, wenn die erfassten Daten für zusätzliche, über die ursprünglichen Zwecke hinausgehende Ziele genutzt werden sollen, beispielsweise um die Fahrzeugfunktionen weiterzuentwickeln oder gar neue fahrzeugbezogene Dienste wie individualisierte Versicherungstarife zu entwickeln. Wenn solche Zwecke bei der Überlassung des Fahrzeugs gegenüber dem Fahrzeughalter nicht offengelegt wurden, sind die dazu erforderlichen Datenverarbeitungen im Regelfall nicht mehr von dem Vertrag mit dem betroffenen Fahrzeughalter über die Bereitstellung des Fahrzeugs erfasst und zu dessen Erfüllung erforderlich, da sich diese Verträge dann nur auf die gegenwärtig vorhandenen, dem Fahrzeughalter

[179] Lüdemann, Artikel „Connected Cars" in der Zeitschrift für Datenschutz (ZD) 2015, 247.

[180] Einen Einblick gibt der Europäische Datenschutzausschuss, in dem die Datenschutzbehörden auch Hinweise zu den rechtlichen Rahmenbedingungen geben, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

bekannten Dienste beziehen, die er mit dem Fahrzeug erwirbt bzw. in Anspruch nehmen will. Darüber hinausgehende Datenverarbeitungen sind daher regelmäßig nicht mehr zur Vertragserfüllung erforderlich. Eine Einwilligung hierin ist zwar möglich, jedoch nicht immer praktikabel, da die Betroffenen die Einwilligung jederzeit widerrufen und die Löschung der mit ihnen in Zusammenhang stehenden gespeicherten Daten verlangen können, Art. 7 Abs. 3 DSGVO. Auch berechtigte Interessen des Fahrzeugherstellers allein können im Einzelfall nicht ausreichen, wenn die Interessen des betroffenen Fahrzeughalters bzw. -führers am Ausschluss der zusätzlichen Datenverarbeitung überwiegen.[181] Bei besonders sensiblen Daten, wie Standortdaten, die dazu geeignet sind, umfangreiche Bewegungsprofile zu erstellen, wird eine Verarbeitung zur Wahrung berechtigter Interessen des Fahrzeugherstellers zunehmend schwierig. In solchen Fällen wird regelmäßig nur eine Einwilligung in Betracht kommen, selbst wenn sie nicht dauerhaft Rechtssicherheit geben kann.

Darüber hinaus muss jeder Verantwortliche sicherstellen, dass die technischen und organisatorischen Strukturen im Zusammenhang mit dem intelligenten Auto so eingerichtet sind, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten so minimal wie möglich gehalten wird (Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO) und dass von vorneherein nur die wirklich erforderlichen Daten verarbeitet („Privacy by Design", Art. 25 Abs. 1 DSGVO) oder zumindest die datenschutzfreundlichsten Voreinstellungen getroffen werden („Privacy by Default", Art. 25 Abs. 2 DSGVO). Beispielsweise können Aufnahmen der Fahrzeugsensoren zeitnah anonymisiert werden, indem die Aufnahmen auf grobe Umrisse der Objekte und eine Klassifizierung als „Person", „Auto" oder „LKW" reduziert werden,[182] bevor die Aufnahmen weiterverarbeitet werden. Eine weitere Option ist, dass die Daten möglichst nur lokal im Fahrzeug gespeichert und verarbeitet werden, und ein externer Zugriff auf die Daten reduziert ist. Die zur Datenminimierung sinnvollen Maßnahmen müssen jedenfalls den technischen Möglichkeiten und dem Umfang der Datenverarbeitung, aber auch den mit der Datenverarbeitung verfolgten Zwecken Rechnung tragen.

Es bestehen vereinzelt auch verpflichtende Datenverarbeitungen in Zusammenhang mit intelligenten Fahrzeugen. So müssen Fahrzeuge mit hoch- oder vollautomatisierten Fahrfunktionen (Stufe 3 und 4) zwingend die Positions- und Zeitangaben speichern, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt (§ 63a Abs. 1 StVG). Die gespeicherten Daten sind zur Ahndung von Verkehrsverstößen an die zuständigen Behörden oder zur Verfolgung von Rechtsansprüchen, etwa aus Verkehrsunfällen, an Dritte zu übermitteln (§ 63a Abs. 2, 3 StVG). Die Vorschrift dient damit zu Beweiszwecken. Es soll verhindert werden, dass sich Fahrzeugführer einer Haftung oder einer Ahndung von Straftaten oder Ordnungswidrigkeiten entziehen können, indem sie sich pauschal auf technisches Versagen einer automatisierten Fahrfunktion berufen.[183] Diese Datenerhebungen und -übermittlungen sind dann zur Erfüllung einer rechtlichen Pflicht, welcher der Verantwortliche unterliegt, erforderlich und deshalb gerechtfertigt, Art. 6 Abs. 1 lit. c) DSGVO.

---

[181] Anschaulich bereits die Leitlinien 1/2020 des Europäischen Datenschutzausschusses zu Datenverarbeitungen bei vernetzten Fahrzeugen, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

[182] Diese Maßnahme ist in einigen automatisierten Testfahrzeugen bereits im Einsatz, siehe z. B. https://www.bmw.com/en/footer/data-processing-automated-vehicles/data-processing-automated-vehicles-de.html.

[183] Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 1. Auflage 2019, § 16 Rn. 53.

Schließlich müssen die meisten Neufahrzeuge nach den Vorgaben der Verordnung (EU) 2015/758 (sog. „eCall-VO") mit einem bordeigenen eCall-System ausgestattet sein. Es handelt sich um ein Notrufsystem, welches mittels Fahrzeugsensoren bei schweren Unfällen aktiviert wird und über das Mobilfunknetz einen Notruf auslöst. Auch die hierdurch ausgelösten Datenverarbeitungen sind zur Erfüllung rechtlicher Verpflichtungen erforderlich, ohne dass es einer Einwilligung des Betroffenen bedarf. Dies ist nicht nur datenschutzrechtlich gerechtfertigt, sondern auch im Übrigen sinnvoll, weil gerade in einem solchen Notfall der betroffene Fahrzeughalter oder -fahrer häufig nicht mehr in der Lage sein wird, eine Einwilligung zu erteilen.

Nicht zuletzt kann die automatisierte Entscheidungsfindung (insbesondere in Zukunft) auch im Kontext der viel diskutierten „Dilemmasituation"[184] bei autonomen Fahrzeugen eine Rolle spielen: Muss die Software eines autonom gesteuerten Fahrzeugs bei einem unmittelbar bevorstehenden und unabwendbaren Unfall entscheiden, welche Person tödlich verletzt wird (etwa Passant A *oder* Passant B), dürfte diese Entscheidung nicht auf etwaig vom Fahrzeug erhobenen personenbezogenen Daten (Passant A, 84 Jahre, chronisch krank *oder* Passant B, 14 Jahre, gesund) beruhen. Juristisch ist die Auflösung dieser Situation nicht möglich, da das Rechtsgut Leben einer qualitativen und quantitativen Abwägung entzogen ist.[185] Aus diesem Grund kann der Gesetzgeber auch keine gesonderte Rechtsgrundlage im Sinne von Art. 22 Abs. 2 DSGVO erlassen, die eine Verarbeitung personenbezogener Daten in diesem konkreten Einzelfall erlauben würde.

Die Konsequenz ist, dass die Software für das automatisierte Fahren eine Entscheidung nicht auf der Grundlage von personenbezogenen Daten treffen darf.[186] Auch die Ethik-Kommission zum autonomen und vernetzten Fahren ist der Ansicht, dass derartige Dilemmasituationen nicht eindeutig normierbar seien. In jedem Fall seien bei unausweichlichen Unfallsituationen eine Unterscheidung nach persönlichen Merkmalen und eine Aufrechnung von Opfern untersagt. Eine allgemeine Programmierung auf eine Minderung der Zahl von Personenschäden wird aber für vertretbar erachtet.[187]

---

184 Für eine strafrechtliche Betrachtung etwa Weber in Dilemmasituation beim autonomen Fahren, NZV 2016, 249.

185 Vgl. Neumann in Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Auflage, § 34 Rn. 74.

186 Dem Softwareentwickler ist die Antizipation und Entscheidungsgewalt über diese Situation insoweit entzogen. Zulässig wäre ggf. die Implementierung einer Zufallsentscheidung oder die Rückgabe der Kontrolle an den menschlichen Fahrer im letzten Moment.

187 Ethik-Kommission zum autonomen und vernetzten Fahren, Bericht Juni 2017, S. 11.

Ihre Ansprechpartner

Dr. Andreas Lober
Rechtsanwalt
Andreas.Lober@bblaw.com
Tel.: +49 69 756095-582

Susanne Klein
Rechtsanwältin | LL.M.
Fachanwältin für Informations-
technologierecht
Susanne.Klein@bblaw.com
Tel.: +49 69 756095-582

Wojtek Ropel
Rechtsanwalt
Wojtek.Ropel@bblaw.com
Tel.: +49 69 756095-582

Dr. Florian Jäkel-Gottmann
Rechtsanwalt
Florian.Jaekel-Gottmann@bblaw.com
Tel.: +49 69 756095-585

Lennart Kriebel
Rechtsanwalt
Lennart.Kriebel@bblaw.com
Tel.: +49 69 756095-477