Johannes Graf Ballestrem
Ulrike Bär
Tina Gausling
Sebastian Hack
Sabine von Oelffen

Künstliche Intelligenz

Rechtsgrundlagen und Strategien in der Praxis

Springer Gabler

Künstliche Intelligenz

Johannes Graf Ballestrem • Ulrike Bär
Tina Gausling • Sebastian Hack
Sabine von Oelffen

Künstliche Intelligenz

Rechtsgrundlagen und Strategien in der Praxis

Springer Gabler

Johannes Graf Ballestrem
Osborne Clarke
Köln, Deutschland

Ulrike Bär
Osborne Clarke
Köln, Deutschland

Tina Gausling
Allen & Overy
München, Deutschland

Sebastian Hack
Osborne Clarke
Köln, Deutschland

Sabine von Oelffen
Osborne Clarke
Köln, Deutschland

ISBN 978-3-658-30505-5 ISBN 978-3-658-30506-2 (eBook)
https://doi.org/10.1007/978-3-658-30506-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Springer Gabler ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Danksagung

Unser besonderer Dank gebührt den nachfolgend genannten, wissenschaftlichen Mitarbeitern der Kanzlei Osborne Clarke, die durch Ihren persönlichen Einsatz maßgeblich zum Gelingen dieses Buches beigetragen haben:

Bosko Vetter
Daniel Pesch
Julius Gäntgen
Lucas Mayr
Samantha Wowrzyk
Victoria Brücken
Viktoria Krasovski

Inhaltsverzeichnis

Über die Autoren

Dr. Johannes Graf Ballestrem, LL.M. Dr. Johannes Graf Ballestrem studierte Rechtswissenschaften in Bonn, Paris und Lausanne. Seit 2010 ist er als Rechtsanwalt im gewerblichen Rechtsschutz tätig und Partner der Kanzlei Osborne Clarke seit 2019.

Dr. Johannes Graf Ballestrem berät nationale und internationale Konzerne sowie mittelständische Unternehmen in Fragen des geistigen Eigentums, insbesondere des Patentrechts und der weiteren technischen Schutzrechte, sowie des Gesetzes gegen den unlauteren Wettbewerb (UWG). Neben der Vertretung in gerichtlichen und außergerichtlichen Auseinandersetzungen umfasst seine Tätigkeit auch die Verhandlung und Erstellung von Verträgen.

Darüber hinaus hat er Erfahrung bei der Beratung zu Rechtsfragen der Digitalisierung. Er berät regelmäßig zum urheber- und patentrechtlichen Schutz von Daten und Datenbanken sowie zu Zugangsrechten zu Daten.

Dr. Ulrike Bär Dr. Ulrike Bär, LL.M. Tax, Fachanwältin für Steuerrecht, Dipl.-Finanzwirtin (FH) studierte Rechtswissenschaften in Bonn und London. Sie berät seit 2003 als Rechtsanwältin im nationalen und internationalen Steuerrecht und ist Senior Counsel in der Praxisgruppe Steuerrecht bei Osborne Clarke.

Sie ist spezialisiert auf die steueroptimierte Strukturierung von Unternehmen, Transaktionen und Investitionen, insbesondere im grenzüberschreitenden Bereich. Weitere Schwerpunkte sind die Begleitung von streitigen Auseinandersetzungen sowie Betriebsprüfungen und die Beratung zu Fragen der Tax Compliance.

Dr. Ulrike Bär publiziert regelmäßig zu steuerlichen Themen und referiert zu steuerlichen Fragen, insbesondere aus den Bereichen IP/IT. Sie ist Mitglied des Steuerberaterverbandes und Delegierte der Steuerkommission der International Chamber of Commerce (ICC).

Dr. Tina Gausling Dr. Tina Gausling, LL.M. (Columbia University) ist Fachanwältin für Informationstechnologierecht und zertifizierte Datenschutzexpertin (CIPP/E) bei Allen & Overy LLP in München. Sie berät nationale und internationale Unternehmen umfassend im Datenschutz-, IT- und E-Commerce-Recht, u. a. in globalen Compliance-Projekten, M&A-Transaktionen und bei der Verhandlung komplexer IT- und Datenschutzverträge. Darüber hinaus vertritt Tina Gausling ihre Mandanten in datenschutzbehördlichen und gerichtlichen Verfahren. Ein besonderer Fokus ihrer Beratungspraxis liegt auf grenzüberschreitenden Fragestellungen mit Bezug zu aktuellen technologischen Entwicklungen, insbesondere in den Bereichen Online-Marketing und AdTech, IoT und Künstliche Intelligenz. Dr. Gausling wirkt als Mitglied des European Advisory Board der IAPP (International Association of Privacy Professionals) intensiv an der rechtlichen Weiterentwicklung dieser Themen mit. Sie publiziert regelmäßig in Fachzeitschriften und internationalen Journals und tritt als Sprecherin auf fachspezifischen Konferenzen und in (Inhouse-)Seminaren auf, u. a. als Referentin der C.H. Beck Akademie.

Dr. Sebastian Hack, LL.M. Dr. Sebastian Hack studierte Rechtswissenschaft in Köln (Dr. jur.), Pittsburgh, New York und London (LL.M.). Sebastian Hack ist Rechtsanwalt und Partner in der Praxisgruppe Kartellrecht bei Osborne Clarke.

Ein Schwerpunkt seiner Beratung liegt im Vertriebskartellrecht, der Compliance-Beratung und auf kartellrechtlichen Fragestellungen in der digitalen Wirtschaft, einschließlich dem Umgang und Zugang mit Daten sowie neuen Geschäfts- und Plattformmodellen. Zudem verteidigt er regelmäßig Unternehmen in kartellbehördlichen Ermittlungsverfahren und vertritt Unternehmen vor Gericht.

Er verfügt über besondere sektorspezifische Erfahrung in den Bereichen Retail und Digital Business.

Dr. Sabine von Oelffen, LL.M. Dr. Sabine von Oelffen studierte Rechtswissenschaft in München (Dr. jur.) und London (LL.M.). Sabine von Oelffen ist Senior Associate in der Praxisgruppe IT bei Osborne Clarke. Sie berät die Mandanten der Kanzlei umfassend in allen IT-rechtlichen Fragestellungen, insbesondere bei der Ausgestaltung und Verhandlung von klassischen IT-Projektverträgen. Ein Tätigkeitsschwerpunkt liegt hierbei in den Bereichen Informationstechnologie, Outsourcing und Beratung bei SAP-Projekten. Weitere Tätigkeitsfelder von Dr. Sabine von Oelffen sind die Beratung von Unternehmen bei der Erstellung von Standardverträgen (Einkauf, Lizenz, Hardware, Software, Consultingverträge), bei Lizenzthemen (insbesondere im Hinblick auf den Einsatz künstlicher Intelligenz) sowie hinsichtlich des Fremdpersonaleinsatzes bei IT-Projekten mit besonderem Schwerpunkt auf agilen Projekten.

Zudem ist Dr. Sabine von Oelffen Gastdozentin an der WHU – Otto Beisheim School of Management in Vallendar und an der Universität zu Köln (Vorlesung und Tutorium „German Civil Law“). Dr. Sabine von Oelffen hält regelmäßig Vorträge und verfasst Publikationen zu aktuellen Themen des IT-Vertragsrechts.

Grundlagen: Rechtliche Einordnung der Thematik Künstliche Intelligenz/ Maschinelles Lernen

1

Johannes Graf Ballestrem, Ulrike Bär, Tina Gausling, Sebastian Hack und Sabine von Oelffen

Zusammenfassung

Künstliche Intelligenz (KI oder **Artificial Intelligence, AI)** bezeichnet Systeme, die intelligentes Verhalten zeigen, indem sie ihre Umgebung analysieren und – mit einem gewissen Grad an Autonomie – Maßnahmen ergreifen, um bestimmte Ziele zu erreichen. Einsteigend wird in diesem Kapitel ein Überblick über die Einsatzfelder von KI, dort entstehende Problemfelder und den bereits existierenden rechtlichen Rahmen sowie die Bezugspunkte zu den jeweiligen Rechtsgebieten und dort zu findende Lösungsansätze gegeben.

1.1 Begrifflichkeiten und technische Grundlagen

Künstliche Intelligenz (**KI** oder **Artificial Intelligence**, **AI**) bezeichnet „Systeme, die intelligentes Verhalten zeigen, indem sie ihre Umgebung analysieren und – mit einem gewissen Grad an Autonomie – Maßnahmen ergreifen, um bestimmte Ziele zu erreichen. KI-basierte Systeme können rein softwarebasiert sein, in der virtuellen Welt agieren (z. B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme) oder in Hardwaregeräte eingebettet sein (z. B. fortgeschrittene Roboter, autonome Fahrzeuge, Drohnen oder Internet of Things-Anwendungen)“ (Hochrangige Expertengruppe für

J. G. Ballestrem · U. Bär · S. Hack · S. von Oelffen (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: johannes.ballestrem@osborneclarke.com; ulrike.baer@osborneclarke.com; sebastian.hack@osborneclarke.com; sabine.vonoelffen@osborneclarke.com

T. Gausling
Allen & Overy, München, Deutschland
E-Mail: tina.gausling@allenovery.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_1

künstliche Intelligenz 2019, S. 1). KI-Systeme versuchen die kognitiven Fähigkeiten des Menschen durch Algorithmen nachzubilden. Algorithmen sind – einfach gesprochen – mathematische Handlungsanweisungen (Steuerungsbefehle), die dafür sorgen, dass ein Daten-Input in einen Daten-Output transformiert wird (Plattform Industrie 4.0 2019, S. 3).

1.2 Einsatzfelder von KI in Unternehmen

Die Einsatzfelder von KI in Unternehmen sind vielfältig. Zu unterscheiden ist zunächst zwischen der Nutzung von KI für innerbetriebliche Zwecke des Unternehmens **(1)**, dem Angebot von KI-basierten Leistungen und Produkten an den Kunden **(2)** sowie der Auswertung und Kommerzialisierung der mittels KI gesammelten Daten **(3)**.

(1) Klassische Einsatzfelder von KI für innerbetriebliche Zwecke sind beispielsweise der unter dem Begriff **Smart Factories** bekannte Einsatz von KI-basierten Produktionsabläufen oder die Verwendung von KI-basierten Lösungen für die Kommunikation innerhalb des Unternehmens. Denkbar ist beispielsweise der Einsatz eines Chatbots, welcher Reisebuchungen der Mitarbeiter verarbeitet oder Anfragen an den IT-Support beantwortet.
(2) An Kunden gerichtete Angebote KI-basierter Leistungen und Produkte sind bereits heute vielfältig und werden aller Voraussicht nach in den nächsten Jahren exponentiell ansteigen. Kundenzielgruppe dieser Angebote sind Unternehmen wie Verbraucher gleichermaßen. Bedeutende Anwendungsfelder des Einsatzes von KI als Tool für die Erbringung von Leistungen im geschäftlichen Verkehr zwischen Unternehmen (**B2B-Bereich**) umfassen **Predictive Maintenance,**[1] **Predictive Analytics,**[2] intelligente Warenlager, visuelle KI zum Auffinden von Fehlern und Schäden sowie KI-basierte Plattformlösungen für die Abwicklung von Geschäftsprozessen jeglicher Art. Die Palette KI-basierter Produkte im B2B-Bereich reicht von smarten Produktionsmaschinen bis hin zu KI-basierten Nutzfahrzeugen, welche z. B. in der Landwirtschaft zum Einsatz kommen und kontinuierlich Daten sammeln, auswerten und bei den folgenden Arbeitsschritten berücksichtigen. Das Angebot von KI-basierten Leistungen gegenüber Verbrauchern ist insbesondere im Bereich der Kommunikation ausgeprägt und umfasst u. a. digitale Assistenten, Chatbots und sog. **Companion Roboter** (oder **Co-Bots**), die Menschen Gesellschaft leisten. Neben KI-basierten Leistungen erhalten Verbraucher bereits heute ein großes Angebot KI-basierter Produkte, das von (teil-) autonom fahrenden Autos bis hin zu smarten Haushaltsgeräten reicht. Eine weitere Besonderheit von KI-basierten Leistungen und Produkten besteht darin, dass diese auch untereinander, d. h. nicht nur mit ihren Nutzern interagieren (**Internet of Things**).

[1] Predictive Maintenance ist die vorausschauende Instandhaltung von Industriellen Gegenständen. Dazu werden im Vorfeld instandhaltungsrelevante Daten erhoben und eine Prognose für den Wartungsbedarf erstellt (Faber et al. 2018, S. 300).

[2] Im Rahmen der Predictive Analytics werden Datenbestände durchsucht, um Vorhersagen für zukünftige Entwicklungen (z. B. Trends an Märkten) zu machen. Dabei können riesige Datenbestände durchsucht und präzise Aussagen getroffen werden (Erichsen 2018, S. 130).

(3) Mit dem Einsatz und Angebot KI-basierter Leistungen und Produkte geht die kontinuierliche Sammlung großer Mengen von Daten sowohl durch die Anbieter der KI-Lösung als auch durch die Nutzer derselben einher. Zunächst sind Daten essenziell für das „Training" und die kontinuierliche Verbesserung der KI-Lösung. Bei Neueinführung einer KI-Lösung kann sich hier freilich das praktische Problem stellen, über welche Bezugsquelle die für das „Training" der KI-Lösung erforderlichen Daten beschafft werden können. Die während des Einsatzes der KI-Lösung generierten Daten sind häufig nicht nur für die Anbieter und die Nutzer der KI-Lösung, sondern auch für Dritte, die beispielsweise Komplementärprodukte anbieten, von hohem wirtschaftlichem Wert. Dies gilt insbesondere dann, wenn Anbieter von KI-Lösungen durch den Einsatz derselben in unterschiedlichsten Anwenderunternehmen Zugang zu großen Mengen von Daten erhalten und diese auswerten können. Die mittels KI-Lösungen gewonnenen und ausgewerteten Daten sind dann vielfach selbst (gesonderter) Gegenstand von Handelsgeschäften zwischen Unternehmen. Sie sind ein zentraler Faktor für die Optimierung von Produktentwicklung und Vertrieb und ermöglichen es ggf. sogar, komplett neue Märkte zu erschließen.

1.3 Besondere rechtliche Herausforderungen beim Einsatz von KI

Die Generierung und der Einsatz von „KI" stellen ein Geschäftsfeld dar, das im Vergleich zu sonstigen digitalen Lösungen besonders vielfältige rechtliche Herausforderungen mit sich bringt. Eine dieser Herausforderungen besteht darin, für die Ermöglichung des Einsatzes von KI auf rechtlicher Ebene Lösungen für bisher noch nicht (final) entschiedene ethisch-moralische Fragestellungen zu finden, etwa im Bereich des autonomen Fahrens.[3] Hier bedarf es einer Untersuchung dahingehend, inwieweit möglicherweise bereits bestehende gesetzliche Vorgaben ausreichend sind, um neue Fragestellungen hinreichend rechtlich beantworten zu können.

Eine zentrale Frage betrifft die Frage nach der Haftung für KI-Systeme. Trifft den Hersteller der KI-Software eine besondere Verantwortung für Schäden, die infolge des Einsatzes der Software eintreten? Lässt sich KI mit den klassischen Mustern des **Produkthaftungsgesetzes** (**ProdHaftG**) erfassen? Bestehen Pflichten zur Kontrolle der KI-Lösung? Wie lassen sich die Verantwortungsbereiche zwischen Hardwarehersteller, Nutzer und KI abgrenzen? Die Brisanz dieser grundlegenden Fragestellungen lässt sich auch verdeutlichen am Beispiel eines Chatbots, der von den Nutzern gezielt mit rechtswidrigen Inhalten konfrontiert wird und dann selbst rechtswidrige Äußerungen von sich gibt. Trifft das den Chatbot betreibende Unternehmen eine Pflicht zur Kontrolle der „Äußerungen" des Chatbots? Muss das Unternehmen ggf. Maßnahmen zur Abstellung der rechtswidrigen Äußerungen ergreifen, z. B. durch Abstellung des Chatbots?

Neben der Debatte um ein eigenes rechtliches Haftungsregime, auch im Hinblick auf mögliche rechtliche Vertragsgestaltungen bedarf es der Beleuchtung weiterer Aspekte, etwa des Einsatzes von KI unter Einhaltung datenschutzrechtlicher Anforderungen.

[3] Siehe hierzu die Ausführungen im Bericht der Ethik-Kommission (2017).

Die Automatisierung intelligenten Verhaltens bringt daneben auch neue Fragestellungen im Patent-, Urheber-, Wettbewerbs- und Kartellrecht mit sich, etwa im Hinblick darauf, wie durch KI generierte Innovationen geschützt werden und wem beispielsweise Patent- und Urheberrechte an den generierten Inhalten zustehen. Das vorliegende Buch nimmt überdies auch das Steuerrecht in Bezug, das ebenfalls im Rahmen der Kommerzialisierung von KI Beachtung finden muss.

1.4 Rechtlicher Rahmen für den Einsatz von KI in Unternehmen

Da bisher für KI kein spezieller Rechtsrahmen existiert, richtet sich der rechtliche Rahmen des Einsatzes von KI nach den allgemeingültigen gesetzlichen Regelungen. Je nach Einsatzbereich und Zielgruppe der KI-Lösung können Aspekte des Zivilrechts, des Öffentlichen Rechts und sogar des Strafrechts berührt sein. Angebot und Einsatz einer KI-Lösung erfordern daher bereits in der Entwicklungsphase eine umfassende rechtliche Betrachtung, um zwingende rechtliche Vorgaben zum frühestmöglichen Zeitpunkt berücksichtigen zu können und spätere (unter Umständen teure) Anpassungen der technischen Lösung zu vermeiden.

Auch wenn Generierung und Einsatz des jeweiligen KI-Programms immer einer individuellen rechtlichen Würdigung bedürfen, so gibt es doch typische Fallkonstellationen, die nachfolgend rechtlich eingeordnet und überblicksartig angerissen werden sollen.

1.4.1 Datenschutzrecht

Der Einsatz von KI-gesteuerten Mechanismen erfordert zunächst die Verarbeitung großer Datenmengen, die naturgemäß im datenschutzrechtlichen Kontext Fragen aufwerfen. Daten bilden den Grundstein für Entwicklung, Betrieb und Nutzung von KI-Lösungen. **Daten** lassen sich als maschinenlesbare, codierte Informationen beschreiben (Zech 2015, S. 138). Während die Inhalte der Daten die semantische Ebene widerspiegeln, konstituiert die syntaktische Ebene die Daten als solche (Zech 2015, S. 138). Auf der semantischen Ebene enthalten Daten Angaben, (Zahlen-)Werte oder formulierbare Befunde, die durch Messung, Beobachtung u. a. gewonnen wurden. Daten machen letztlich den wirtschaftlichen Wert der KI-Lösung aus. Der besondere Wert von Daten ergibt sich dabei regelmäßig nicht aus den Daten als solchen, sondern aus ihren Inhalten, also dem sinnlich wahrnehmbaren Ergebnis, wenn die Daten bestimmungsgemäß ausgeführt werden (Zech 2015, S. 142). Die Beachtung der für die Generierung, Verarbeitung und Speicherung von Daten geltenden Gesetze ist daher von herausragender Bedeutung für den Einsatz von KI. Vor diesem Hintergrund besteht eine besondere rechtliche Herausforderung darin, die Besonderheiten der bisher nicht gesetzlich regulierten KI-Mechanismen mit den Anforderungen der **Datenschutz-Grundverordnung** (**DS-GVO**) in Einklang zu bringen.

1.4.1.1 Personenbezogene Daten

Häufig fallen Betrieb und Nutzung von KI-Lösungen in den Anwendungsbereich der DS-GVO. Die Anforderungen der DS-GVO sind gemäß Art. 2 Abs. 1 DS-GVO immer – aber auch nur -– dann zu beachten, wenn personenbezogene Daten generiert, verarbeitet und/oder gespeichert werden. Gem. Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Identifiziert ist eine Person, wenn sie durch die jeweiligen Daten unmittelbar bestimmt werden kann. Der sachliche Anwendungsbereich der DS-GVO ist daher eröffnet, wenn eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten oder eine nichtautomatisierte Verarbeitung personenbezogener Daten vorliegt, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Da die DS-GVO strenge und umfangreiche Anforderungen in Bezug auf die Verarbeitung personenbezogener Daten stellt, ist es empfehlenswert, bereits bei der Planung und Entwicklung der KI-Lösung zu evaluieren, ob die KI-Lösung DS-GVO-konform umgesetzt und betrieben werden kann.

1.4.1.2 Schnittstelle zum Arbeitsrecht

Auch am Arbeitsplatz beziehungsweise im Rahmen der Begründung eines Arbeitsverhältnisses gewinnen KI-Lösungen an Bedeutung. Gleichzeitig erfordert dies auch die Betrachtung von Konstellationen zwischen Datenschutz- und Arbeitsrecht. Werden etwa Bewerbungsverfahren unter Verwendung von KI-Lösungen durchgeführt oder Arbeitsverhältnisse anhand KI-gestützter Entscheidungsprozesse begründet bzw. beendet, ist neben der spezialgesetzlichen Regelung zum Beschäftigtendatenschutz in § 26 BDSG auch Art. 22 DS-GVO[4] zu berücksichtigen, der die rechtlichen Anforderungen an automatisierte Entscheidungen statuiert.

1.4.1.3 Maschinengenerierte Daten

Werden mittels der KI-Lösung Daten generiert, gespeichert und/oder verarbeitet, die keine personenbezogenen Daten im Sinne der DS-GVO sind (**Maschinengenerierte Daten**), so ist auch der Anwendungsbereich der DS-GVO nicht eröffnet. Speziell auf Maschinengenerierte Daten zugeschnittene, gesetzliche Regelungen existieren derzeit nicht. Eine für die Kommerzialisierung Maschinengenerierter Daten zentrale Frage ist daher, ob und in welchem Umfang Rechte an Maschinengenerierten Daten durch vertragliche Vereinbarung der Parteien eingeräumt werden können. Zudem sind auch ohne vertragliche Gestaltungen beim Umgang mit Maschinengenerierten Daten einschlägige Regelungsbereiche zu beachten, beispielsweise das Geheimnisschutzgesetz oder das Computerstrafrecht.

[4] Diese Normen regeln die Anforderungen an eine zulässige Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses bzw. das grundsätzliche Verbot einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung im Einzelfall.

1.4.1.4 Weitere Aspekte des Öffentlichen Rechts

Je nach Art und Einsatzzweck kann eine KI-Lösung auch weitere Bereiche des öffentlichen Rechts tangieren. So kann etwa die KI-Lösung selbst oder das Programm, in dem sie verkörpert ist, eine Gefahr für die öffentliche Sicherheit darstellen. In einer derartigen Situation können sowohl das Herstellerunternehmen als auch die Anwender der KI-Lösung als Zustandsstörer Adressaten ordnungsbehördlicher Maßnahmen werden. Denkbar wäre eine Verantwortlichkeit als Zustandsstörer[5] beispielsweise im Falle eines falsch programmierten autonomen Fahrsystems, welches durch die Falschprogrammierung Verkehrsregeln missachtet. Eine andere Fallkonstellation, in der Berührungspunkte zum öffentlichen Recht bestehen, ist der Einsatz einer KI-Lösung in Bereichen, in denen es zu grundrechtsrelevanten Handlungen kommt.[6] So kann es beim Einsatz automatisierter Bewerbungsverfahren oder bei der Kreditvergabe und den diesbezüglich bestehenden Konditionen zu Diskriminierungen im Sinne von Art. 3 GG kommen (Härtel 2019, S. 56). Auch wenn dies im Rahmen der Privatwirtschaft geschieht, kann die mittelbare Drittwirkung der Grundrechte einen Verwender von KI-Lösungen verpflichten.

1.4.2 Urheberrecht

Neben datenschutzrechtlichen Problemstellungen werfen Entwicklung, Betrieb und Nutzung von KI-Lösungen daneben auch vielfältige urheberrechtliche Fragen auf. Je nach Einzelfall kann (beispielsweise beim Text- und Data Mining) bereits die Datenerhebung auf urheberrechtliche Grenzen stoßen. Anbieter von KI stellen sich wiederum die Frage, ob und inwieweit ihre KI-Lösung bzw. die durch diese generierten Daten urheberrechtlichen Schutz genießen. An der KI-Lösung selbst können Urheber- und Erfinderrechte bestehen. Werden Daten so systematisiert, dass eine Datenbank im Sinne des **Urheberrechtsgesetzes** (**UrhG**) entsteht, so kann diese ebenfalls urheberrechtlichen Schutz genießen. Bevor die KI-Lösung bzw. durch diese generierte Daten kommerzialisiert werden, sollten daher Bestehen und ggfs. Umfang entsprechender Schutzrechte geprüft wer-

[5] „Zustandsstörer ist derjenige, der die Beeinträchtigung zwar nicht verursacht hat, durch dessen maßgeblichen Willen der beeinträchtigte Zustand aber aufrechterhalten wird. Voraussetzung dafür ist das der Inanspruchgenommene […] die Möglichkeit zu deren Beseitigung hat. Darüber hinaus muss ihm die Beeinträchtigung zurechenbar sein.“ (BGH 18. Dezember 2015, NJW 2016, S. 863 (865)).

[6] Je nach Einsatzgebiet der KI und Konstellation des Sachverhalts können Entscheidungen der KI-Lösung für die betroffene Person einen Eingriff in die Grundrechte darstellen, so dass sie im Rahmen der Entscheidungsfindung berücksichtigt werden müssen. Dies gilt einerseits für den Einsatz von KI-Lösungen im Rahmen öffentlich-rechtlicher Tätigkeiten als auch im Privatrecht. Letzteres ist in Situationen anzunehmen, in denen zwischen den Parteien eine ungleiche Machtverteilung besteht und die Entscheidung im erheblichen Umfang über die Teilhabe am gesellschaftlichen Leben entscheidet (Werner 2019, S. 1045).

den. Daneben empfiehlt sich eine Prüfung dahingehend, ob möglicherweise Dritte Rechte an der KI-Lösung und/oder den hierdurch generierten Daten geltend machen könnten.

Möchte ein Anbieter die KI-Lösung Anwenderunternehmen am Markt zur Verfügung stellen, stellen sich zudem mannigfaltige Fragen des Softwarelizenzrechts. Zentrale Bedeutung in der Praxis kommt hierbei der Wahl der passenden Lizenzmetrik zu.

1.4.3 Lauterkeitsrecht

Das durch das **Gesetz gegen unlauteren Wettbewerb** (**UWG**) kodifizierte Lauterkeitsrecht hat ebenfalls erhebliche Bedeutung für Betrieb und Nutzung von KI-Lösungen. So sind bei der Datenerhebung mittels KI als mögliche Grenzen sowohl der in § 4 Nr. 3 UWG normierte, lauterkeitsrechtliche Nachahmungsschutz als auch der Schutz vor wettbewerbswidriger Behinderung zu beachten. Auf der anderen Seite können Betreiber oder Nutzer einer KI-Lösung im Einzelfall auch einen lauterkeitsrechtlichen Anspruch auf Zugang zu bestimmten Daten geltend machen.

1.4.4 Kartellrecht

Kartellrechtliche Fragestellungen ergeben sich in Bezug auf KI-Lösungen insbesondere dann, wenn sich der Inhaber bestimmter (maschinengenerierter) Daten weigert, einem Unternehmen Zugang zu bestimmten Daten einzuräumen. Kartellrechtlich interessant ist zudem die (algorithmische) Festsetzung von unterschiedlichen Preisen für einzelne Personen oder Personengruppen. Ganz allgemein gibt es bei der algorithmischen Preissetzung einige kartellrechtliche Stolpersteine, die es zu meiden gilt. Von zentraler Bedeutung ist auch die Frage, wer für einen kartellrechtswidrigen Algorithmus verantwortlich ist. In Frage kommen hier z. B. der Programmierer, der Verkäufer und der Verwender des Algorithmus.

1.4.5 Haftungsrechtliche Fragestellungen

Wird die KI-Lösung auf dem Markt anderen Anwendern zur Verfügung gestellt, stellt sich unweigerlich die Frage, wer für Fehler der KI-Lösung oder für durch diese verursachte Schäden haftet. Wenn die in einen Kühlschrank eingebettete Software versagt und das Gerät deshalb Feuer fängt, liegt die Anwendbarkeit der Produkthaftung auf der Hand. Soll sich daran etwas ändern, wenn der Nutzer des Kühlschranks nach dessen Erwerb eine Software, zum Beispiel ein Update des Kühlschrankherstellers, aus dem Internet herunterlädt und aufspielt? Spielt die Intelligenz der Software eine Rolle? Von zentraler Bedeutung sind insoweit die Produkt- und Produzentenhaftung. Das Produkthaftungsrecht gilt jedoch für bewegliche Sachen. Ob KI-Systeme, die aus Computer-Algorithmen und damit aus

Software bestehen, bewegliche Sachen in diesem Sinne sind, ist in der Rechtswissenschaft stark umstritten. Einschlägige gerichtliche Entscheidungen gibt es bislang nicht. Gleichwohl geben wir Ihnen einen Überblick über die nach derzeitigem Stand anzuwendenden Regelungen und einen Ausblick auf die in der Entwicklung befindliche Gesetzgebung.

1.4.6 Vertragsrechtliche Fragestellungen

Schließen Unternehmen einen Vertrag über den Einsatz einer KI-Lösung, so sollten die besonderen Charakteristika von KI-Lösungen wie deren autonomes Handeln oder das „Black-Box"-Phänomen in den Verträgen entsprechenden Niederschlag finden. Kann beispielsweise aufgrund des „Black-Box"-Phänomens keine Garantie dafür übernommen werden, dass der Einsatz der KI-Lösung zu einem bestimmten Erfolg führt, so sollte dieses Verständnis der Parteien in einer vertraglichen Regelung festgehalten werden. Eine hiervon zu unterscheidende Frage, die in der juristischen Literatur heftig diskutiert wird, ist die Frage, ob und inwieweit KI-Lösungen selbst Verträge abschließen können sollten.

1.4.7 Strafrecht

KI-Lösungen sind neben den genannten Aspekten des Zivil- und Öffentlichen Rechts auch in strafrechtlicher Hinsicht relevant. Da wir im Folgenden den Einsatz von KI aus der wirtschaftsrechtlichen Perspektive beleuchten, sollen mögliche strafrechtliche Problemfelder an dieser Stelle nur überblicksartig angerissen werden. Stehen KI-Lösungen in Zusammenhang mit Unfällen oder sonstigen Situationen, in denen Rechtsgüter verletzt werden, wird häufig nach einem strafrechtlich Verantwortlichen gesucht. Nach aktueller Gesetzeslage kann eine strafrechtliche Verantwortlichkeit nur natürliche Personen treffen. Die KI-Lösung selbst kann hingegen nicht strafrechtlich belangt werden. Gegen das Herstellerunternehmen oder das die KI-Lösung verwendende Unternehmen können keine Strafen, sondern lediglich Geldbußen im Rahmen des § 30 des **Gesetzes über Ordnungswidrigkeiten** (**OWiG**) verhängt werden. In Betracht kommt jedoch eine strafrechtliche Verantwortlichkeit der Mitarbeiter dieser Unternehmen. Beispielsweise können Personen, die bei der Herstellung der KI-Lösung mitgewirkt haben, im Falle von fahrlässigen Konstruktions-, Fabrikations- oder Instruktionsfehlern sowie bei Verletzung einer Produktbeobachtungs- oder Rückrufpflicht strafrechtlich zur Verantwortung gezogen werden (Schuster 2019, S. 6 (8)). Zudem können sich die Anwender der KI-Lösung strafbar machen. Eine strafrechtliche Verantwortlichkeit ist beispielsweise in Fällen denkbar, in denen die KI-Lösung den Verwender bei der Wahrung seiner eigenen Sorgfaltspflichten unterstützt. Vertraut der Nutzer blind auf die Funktionstüchtigkeit der KI-Lösung, kann er bei Fehlentscheidungen von strafrechtlicher Relevanz entsprechend verurteilt werden. Eine derartige Verantwortlichkeit besteht jedoch nur insoweit, als der Verwender auf die Entscheidung der KI-Lösung Einfluss nehmen kann. Dies ist im Bereich der voll automatisierten Ent-

scheidungsfindung nicht mehr der Fall. Dann scheidet eine strafrechtliche Verantwortlichkeit des Benutzers aus (Böhringer 2019, S. 15). Bei einer Unterscheidung der in Bezug auf KI-Lösungen denkbaren Straftaten nach der Verschuldensform dürfte die Mehrzahl der Fälle Fahrlässigkeitstaten, wie die fahrlässige Körperverletzung und die fahrlässige Tötung ausmachen (Schuster 2019, S. 7; Böhringer 2019, S. 14). Doch auch Vorsatztaten sind bei dem Einsatz von KI-Lösungen denkbar. Diese könnten vor allem im Bereich der Entscheidungsfindung in Dilemma-Situationen, wie etwa beim automatisierten Fahren, wenn KI-basiert die Entscheidung getroffen wird, ob bei einer unvermeidbaren Kollision ein junger Mensch oder mehrere alte Menschen getroffen werden[7] relevant werden.

1.4.8 Steuerrecht

KI-Lösungen sind auch steuerrechtlich relevant. Steuerpflichtige, die KI-Lösungen zur Datenbeschaffung und -verarbeitung einsetzen oder dem KI-System zu Grunde liegende Daten bzw. die KI selbst betriebswirtschaftlich nutzbar machen, schaffen wirtschaftliche Werte. So können beispielsweise große unstrukturierte Datenmengen (**Big Data**) vielseitig verwertet werden und führen wie auch eine Veräußerung oder Lizenzierung von KI-Software zur Steigerung der wirtschaftlichen Leistungsfähigkeit. Eine solche Steigerung schöpft der Staat grundsätzlich durch Einkommen-, Körperschaft- und Gewerbesteuer ab. In diesem Kontext stellt sich bezogen auf Daten und KI-Lösungen aus steuerbilanzieller Sicht die Frage, ob es sich um immaterielle Wirtschaftsgüter handelt und ob diese zu aktivieren sind, oder einem Aktivierungsverbot unterliegen, so dass der damit verbundene Aufwand sofort als Betriebsausgabe abzugsfähig ist. Werden KI-Lösungen über Grenzen hinweg überlassen, können sich Quellensteuereinbehaltungspflichten ergeben, die, wenn sie nicht ordnungsgemäß erfüllt werden, zur steuerlichen Haftung führen können. Ein wichtiger steuerrechtlicher Bereich bei der gemeinsamen Entwicklung und Nutzung von KI-Lösungen im Konzern sind zudem Verrechnungspreise, d. h. die Verpflichtung zur fremdüblichen Ausgestaltung der zugrunde liegenden vertraglichen Beziehungen, einschließlich der Vergütung für die Beiträge und Leistungen der Beteiligten. Schließlich sind auch die umsatzsteuerlichen Implikationen von zentraler Bedeutung.

Eine erste Ausgangsbasis für die Ermittlung des jeweils zu beachtenden, rechtlichen Rahmens bilden folgende Fragen

- Welcher Einsatzbereich besteht für die KI-Lösung?
- Was ist die Zielgruppe der KI-basierten Leistungen und Produkte? Richtet sich das Angebot nur an Unternehmen oder auch an Verbraucher?

[7] Siehe hierzu die Ausführungen im Bericht der Ethik-Kommission (2017, S. 16).

- Werden durch die KI-Lösung personenbezogene oder (nur) maschinengenerierte Daten verarbeitet?
- Hat das Unternehmen, welches die KI-Lösung einsetzen möchte, berechtigten Zugang zu den für Betrieb und/oder Nutzung der KI-Lösung benötigten Daten oder müssen für die Beschaffung der Daten zusätzliche Verträge geschlossen werden?
- Haben dritte Parteien ebenfalls de facto Zugriff auf die durch die KI-Lösung generierten Daten?
- Wird eine (weitere) Kommerzialisierung der mittels der KI-Lösung generierten Daten angestrebt?
- Gelten für die KI-Lösung besondere regulatorische Anforderungen (z. B. wegen Einsatzes der KI-Lösung im Straßenverkehr oder im Finanzsektor)?

Literatur

Böhringer J (2019) Strafrechtliche Verantwortlichkeit für autonome Systeme. RAW 2019:13–17

Erichsen J (2018) Predictive Analytics – Künftiger Arbeitsschwerpunkt des Controllings oder Treiber für den Jobverlust? BC 2018:129–131

Ethik-Kommission zum automatisierten und vernetzten Fahren des Bundesministeriums für Verkehr und digitale Infrastruktur (2017) Bericht der Ethik-Kommission zum automatisierten und vernetzten Fahren des Bundesministeriums für Verkehr und digitale Infrastruktur vom 20.06.2017. https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.html. Zugegriffen am 09.11.2019

Faber T, Griga M, Groß J (2018) Predictive Maintenance- Hürden und Chancen zur Sinnvollen Nutzung von Maschinendaten. DS 2018:299–302

Härtel I (2019) Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren. LKV 2019:49–60

Hochrangige Expertengruppe für Künstliche Intelligenz, Eingesetzt von der Europäischen Kommission (2019) A definition of AI: main capabilities and disciplines, 08.04.2019. https://ec.europa.eu/futurium/en/ai-alliance-consultation. Zugegriffen am 14.04.2020

Plattform Industrie 4.0 (2019) Künstliche Intelligenz und Recht im Kontext von Industrie 4.0, herausgegeben vom Bundesministerium für Wirtschaft und Energie, April 2019. https://www.plattform-40.de/PI40/Redaktion/DE/Downloads/Publikation/kuenstliche-intelligenz-und-recht.pdf?__blob=publicationFile&v=4. Zugegriffen am 14.04.2020

Schuster FP (2019) Strafrechtliche Verantwortlichkeit der Hersteller beim automatisierten Fahren. DAR 2019:6–11

Werner W (2019) Schutz durch das Grundgesetz im Zeitalter der Digitalisierung. NJOZ 2019:1041–1046

Zech H (2015) Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“. CR 2015:137–146

KI und DS-GVO im Spannungsverhältnis

2

Tina Gausling

Zusammenfassung

Sowohl für die Generierung als auch den Einsatz von Künstlicher Intelligenz besteht bisher kein spezialgesetzlicher Rechtsrahmen, auch nicht in datenschutzrechtlicher Hinsicht. Den meisten KI-Programmen ist jedoch gemein, dass sie auf Basis personenbezogener Trainingsdaten geschaffen werden und somit den strengen Anforderungen der Datenschutzgrundverordnung unterfallen. Die Qualität der KI-Generierung hängt nach derzeitigem Stand wesentlich vom Umfang der verfügbaren Trainingsdaten ab. Zudem ist zu Beginn der Entwicklungsphase nicht immer klar, zu welchen anderen als den ursprünglich intendierten Zwecken die KI möglicherweise in Zukunft genutzt werden kann. Damit steht die KI-Entwicklung in diametralem Gegensatz zu den Kernprinzipien der DS-GVO, u. a. der Datenminimierung und Zweckbindung. Der nachfolgende Beitrag soll Verantwortlichen Schnittstellen zur DS-GVO und Lösungswege aufzeigen, mit denen KI-Projekte und datenschutzrechtliche Vorgaben bestmöglich in Einklang gebracht werden können.

Nachdem die Umsetzung der Datenschutzgrundverordnung (**DS-GVO**) im Vorfeld zu deren Anwendbarkeit seit dem 25. Mai 2018 die datenschutzrechtliche Debatte und Praxis zahlreicher Unternehmen dominiert hat und auch gegenwärtig insbesondere in Anbetracht durch die Datenschutzbehörden vermehrt verhängter Bußgelder weiter prägt, richtet sich der Fokus des datenschutzrechtlichen Diskurses zunehmend auf eine Schnittstelle, die von Marktforschern für die nächsten Jahre als Megatrend (Panetta 2019) identifiziert wurde: die **Künstliche Intelligenz** (**KI**, **Artificial Intelligence**, **AI**).

T. Gausling (✉)
Allen & Overy, München,, Deutschland
E-Mail: tina.gausling@allenovery.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_2

2.1 Künstliche Intelligenz als technologischer Trend

Der vom US-Marktforschungsinstitut Gartner erstellte „Gartner Hype Cycle for Emerging Technologies 2019" beleuchtet die neuen Technologien, die in den nächsten fünf bis zehn Jahren erhebliche Auswirkungen auf Wirtschaft, Gesellschaft und Menschen haben werden. Der Hype Cycle verläuft dabei in insgesamt fünf Phasen. Am Anfang steht ein beachtliches öffentliches Interesse an der neuen Technologie (**Phase 1**), die zu überzogenen (**Phase 2**) und schließlich enttäuschten Erwartungen (**Phase 3**) führt, bevor die Vorteile der Technologie erkannt (**Phase 4**) und kontinuierlich weiterentwickelt werden (**Phase 5**).

Aus 2000 Technologien in 29 Kategorien identifizierte Gartner insgesamt fünf Megatrends. Neben den Bereichen „Sensoren und Mobilität", „‚Ausbau' des Menschen", „Postklassisches Computing und Kommunikationslösungen (‚Comms')" sowie „Digitale Ökosysteme" handelt es sich dabei um „Fortgeschrittene KI und Analytics". Die Relevanz dieser Technologien wird zwangsläufig zu neuen juristischen Fragestellungen führen, auf die praxisorientierte Antworten gefunden werden müssen.

Trotz dieses Umstands existieren bisher keine konkreten Gesetzesvorhaben, die spezifische Regelungen zur Generierung und zum Einsatz künstlicher Intelligenz beinhalten. Auch zwischenzeitlich erschienene Orientierungshilfen etwa der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (**Datenschutzkonferenz**, **DSK**) beschränken sich auf die Wiedergabe der in der DS-GVO enthaltenen Grundprinzipien (DSK 2019b) bzw. legen die DS-GVO-Anforderungen an die KI-Entwicklung unverhältnismäßig restriktiv aus (DSK 2019c). Sie lassen dabei außer Acht, was für den Verantwortlichen in einem KI-Projekt faktisch überhaupt darstellbar ist.

Eine rein formalistische Auslegung der DS-GVO – die selbst an keiner Stelle konkreten Bezug auf Entwicklungen im Bereich künstlicher Intelligenz nimmt – wird jedoch unweigerlich den Fortschritt der KI-Entwicklung im europäischen Raum hemmen. Es bedarf daher einer praxisorientierten Interpretation der datenschutzrechtlichen Anforderungen, um die Interessen von Unternehmen und auch von Kunden, Konsumenten und Patienten am Einsatz von KI-Programmen mit den Interessen der von der DS-GVO erfassten Betroffenen in einen angemessenen Ausgleich zu bringen.

Der nachfolgende Abschnitt soll daher dem Rechtsanwender praxisorientierte Guidance bieten, um im rechtlichen Graubereich der Schnittstelle von KI und Datenschutz so agieren zu können, dass datenschutzrechtlichen Anforderungen hinreichend Rechnung getragen wird, ohne diese zu Lasten des technologischen Fortschritts unverhältnismäßig eng auszulegen.

2.2 Arten Künstlicher Intelligenz

Grundsätzlich lässt sich zwischen der **schwachen KI** (**Artificial Narrow Intelligence**, **ANI**, **weak AI**), der **starken KI** (**Artificial General Intelligence**, **AGI**) und der sog. **Superintelligenz** unterscheiden.

Schwache KI hat die Lösung spezifischer Anwendungsprobleme zum Gegenstand und *unterstützt* die Entscheidungsfindung in *einem* bestimmten Bereich (vgl. hierzu und im Folgenden Gandhi und Ehl 2017, S. 28). Alltägliche Beispiele sind etwa Sprach- und Gesichtserkennungssysteme.

Starke KI-Systeme existieren bisher noch nicht, werden allerdings für die Mitte dieses Jahrhunderts prognostiziert (Gandhi und Ehl 2017, S. 28). Dabei handelt es sich um Systeme, die den intellektuellen Fähigkeiten des Menschen entsprechen bzw. übertreffen und ihr erworbenes Wissen in vielfältigen Kombinationen zur Anwendung bringen können (Gandhi und Ehl 2017, S. 28).

Der von dem Philosophen *Nick Bostrom* geprägte Begriff der **Superintelligenz** (**Artificial Superintelligence**, **ASI**) bezeichnet schließlich „einen Intellekt, der viel klüger ist als die besten menschlichen Gehirne in praktisch allen Bereichen, einschließlich wissenschaftlicher Kreativität, allgemeiner Lebensweisheit und sozialer Fähigkeiten“[1] (Bostrom 1998). Es handelt sich dabei um eine um ein Vielfaches potenzierte menschliche Intelligenz, deren Auswirkungen heute noch nicht antizipiert werden können und die für die zweite Hälfte dieses Jahrhunderts erwartet wird (Gandhi und Ehl 2017, S. 29).

Derzeit sind sämtliche KI-Anwendungen noch im Bereich der schwachen KI angesiedelt. Es ist daher davon auszugehen, dass auch in den nächsten Jahren vorwiegend die Implementierung schwacher KI-Features im Vordergrund stehen wird. Die nachfolgenden Bezugnahmen auf KI beschränken sich daher auf schwache KI-Systeme. Entsprechend soll sich auch die Beleuchtung der Schnittstelle zum Datenschutzrecht auf diesen Anwendungsbereich beschränken und die damit korrelierenden rechtlichen To Dos beleuchten.

2.3 Daten als Grundlage für Schaffung und Einsatz von KI

Die Zugriffsmöglichkeit auf einen umfassenden Datenbestand stellt einen wesentlichen Faktor für die Optimierung von Produktentwicklung, Vertrieb und der Erschließung neuer Märkte dar. Naturgemäß setzt auch eine erfolgreiche KI-Generierung einen möglichst großen Datenpool voraus, d. h. je größer die vorhandene Datengrundlage ist, desto bessere Ergebnisse erzielt i. d. R. auch das geschaffene KI-Programm.

Damit steht die Entwicklung von KI-Tools zunächst einmal in Widerspruch zu den die DS-GVO durchdringenden Datenschutzprinzipien, allen voran dem Grundsatz der Datenminimierung. Dieser Umstand erschwert es europäischen Unternehmen, im globalen KI-Wettbewerb mit China und den USA zu bestehen. Dies veranschaulicht auch ein Blick auf die weltweit führenden Plattformanbieter, darunter Apple, Amazon, Microsoft, Face-

[1] „By a ‚superintelligence‘ we mean an intellect that is much smarter than the best human brains in practically every field, including scientific creativity, general wisdom, and social skills.“

book und Alphabet in den USA oder Alibaba, Tencent und Samsung in China, gegenüber europäischen Plattformanbietern, die im Plattform-Index der 15 besten Plattform-Aktien weltweit nicht vorkommen.[2]

2.4 Datenanalyse auf Grundlage von Big Data

Um insbesondere die Schnittstelle von KI-Programmen zu datenschutzrechtlichen Anforderungen zu erfassen, bedarf es eines Verständnisses der grundlegenden Terminologie und einer Abgrenzung entsprechender Begrifflichkeiten. Darüber hinaus sollen im Folgenden die wesentlichen technischen Grundlagen zur KI-Generierung dargestellt werden, um auch insofern Implikationen aus dem Bereich des Datenschutzrechts hinreichend würdigen zu können.

2.4.1 Big Data

Die erfolgreiche KI-Generierung und -Entwicklung erfolgt auf Grundlage von **Big Data**. Dieser Begriff ist durch vier Charakteristika gekennzeichnet: volume, velocity, variety und veracity (Schulz 2018, Art. 6, Rn. 195). Big Data bezeichnet zunächst das Vorliegen einer enormen Datenmenge (**volume**), deren Datentypen und -quellen heterogen sind (**variety**). Eine besondere Herausforderung liegt dabei in der Geschwindigkeit der Datenentstehung und der damit verbundenen Notwendigkeit einer Datenverarbeitung in Echtzeit (**velocity**). Darüber hinaus ist auch die Qualität und Vertrauenswürdigkeit der Datengrundlage sicherzustellen, um in den analysierten Daten enthaltene Verzerrungen zu vermeiden (**veracity**).

2.4.2 Analysemethoden

Der Analyse von Big Data zur Generierung von KI liegen verschiedene Methoden zugrunde. Wesentlich ist dafür der Einsatz von Deep-Learning-Techniken als einem Teilbereich des Machine Learning. Machine Learning wiederum wendet die Prinzipien des Data Mining an, ohne jedoch damit deckungsgleich zu sein (vgl. dazu Abschn. 2.4.2.2).

2.4.2.1 Data Mining

Die Begriffe Big Data und **Data Mining** sind keinesfalls als Synonyme zu verstehen. Vielmehr handelt es ich bei Data Mining um eine Analysemethode zur Identifikation relevanter Zusammenhänge und Erkenntnisse auf Basis eines strukturierten Datenbestandes

[2] Vgl. Schmidt (2018) zur sog. „Unwucht der Plattformökonomie“ im Jahre 2018.

(Brühl 2019, S. 5). Um Muster in den zugrunde liegenden Datensätzen zu erkennen, setzt Data Mining Algorithmen aus der Statistik ein (Luber und Litzel 2016). Die Analyse im Wege des Data Mining geschieht dabei nicht notwendigerweise auf Grundlage von Big Data, sondern ist auch auf Basis eines weniger umfangreichen Datenpools möglich (Luber und Litzel 2016).

2.4.2.2 Machine Learning

Beim **Machine Learning** („**ML**“) handelt es sich um eine der wichtigsten Methoden zur Schaffung von KI, die zunächst das Vorhandensein großer Datenmengen für das Training eines KI-Systems voraussetzt. Auf dieser Basis kann ein Computer mittels selbstlernender Algorithmen Muster und Gesetzmäßigkeiten erkennen (Manhart 2018) und lernt dabei durch Beispiele, eigenständige Lösungen für noch unbekannte Probleme zu finden, ohne dass er zuvor dafür programmiert wurde (Brynjolfsson und McAfee 2019, S. 18 f.).

Es werden demnach im Rahmen des maschinellen Lernens Datenmodelle erzeugt, die zukünftige Szenarien auf Grundlage der vorhandenen Datenbasis prognostizieren können (sog. **Predictive Analytics**) (vgl. Mauerer 2017), d. h. die in vorhandenen Datensätzen enthaltenen Muster auf neue Datensätze anwenden und Vorhersagen treffen.

Beispiel

Erstellung eines Modells zur Vorhersage einer Kündigung durch einen Kunden auf Basis historischer Kündigungsdaten (Mauerer 2017). ◀

Darin liegt der Unterschied zum Data Mining. Bei dieser Methode liegt der Fokus auf der Identifikation von Mustern in einem bestehenden Datenbestand. Gleichwohl erfordert der erfolgreiche Einsatz selbstlernender Algorithmen im Rahmen des Machine Learning oftmals die vorgelagerte Analyse und Aufbereitung von Daten auf Grundlage statistischer Methoden (Fink 2019).

2.4.2.2.1 Deep Learning

Teilbereich des Machine Learning ist das **Deep Learning** (Abb. 2.1). Diesem liegen künstliche neuronale Netze zugrunde, die in Schichten geordnet sind und aus einer Vielzahl von Knotenpunkten (sog. **Neuronen**) bestehen. Zwischen den Knotenpunkten werden

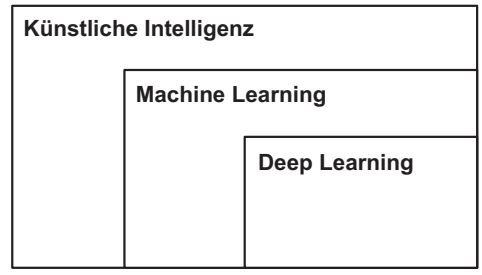

Abb. 2.1 Teilbereiche Künstlicher Intelligenz

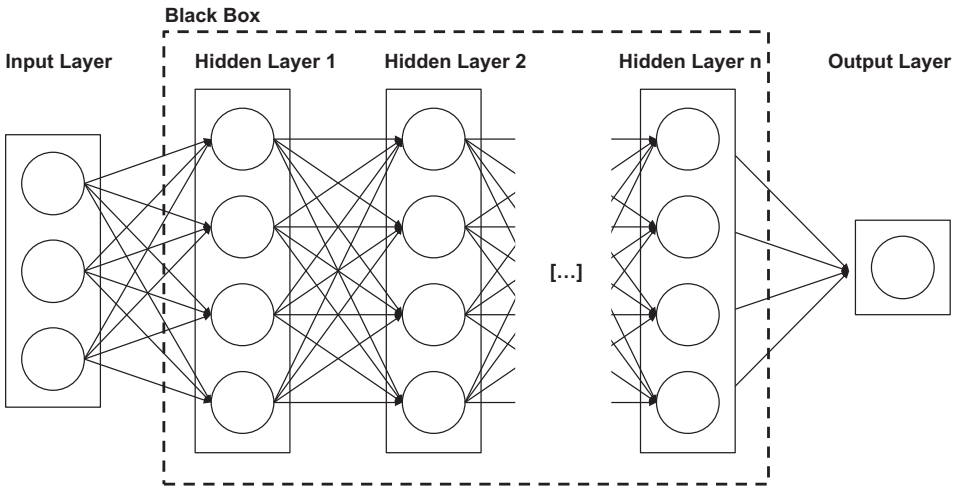

Abb. 2.2 Architektur Neuronaler Netze und Black Box (Gausling 2019a, S. 3, in Anlehnung an Gandhi und Ehl 2017, S. 48)

durch das selbstlernende System Verbindungen aufgebaut oder entfernt bzw. deren Gewichtung angepasst, was die Wahrscheinlichkeit eines korrekten Ergebnisses des dadurch geschaffenen KI-Systems erhöht (Petereit 2016).

2.4.2.2.2 Black Box

Aufgrund der durch das KI-System selbst vorgenommenen Verteilung von Gewichten und Verzerrungen tausender, über zahlreiche Schichten miteinander verbundener, vereinfachter künstlicher neuronaler Netze ist die algorithmische Logik der Entscheidungsfindung im Detail nicht nachvollziehbar und selbst für deren Entwickler nicht erklärbar. Dieser Umstand wird als **Black Box** bezeichnet. Das Black-Box-Phänomen steht dabei zunächst im Widerspruch zu dem in der DS-GVO angelegten Transparenzgrundsatz. Zwar ist es möglich, über die Eingabe von Beispielen und den Vergleich des jeweiligen Ergebnisses (Output) die maßgeblichen Kriterien für die Entscheidung zumindest grob nachzuvollziehen (**Black Box Tinkering** Abschn. 2.12.6.1) – z. B. in Fällen einer Kreditvergabe aufgrund eines Algorithmus. Eine Nachvollziehbarkeit der algorithmischen Entscheidung im Einzelnen ist jedoch (noch) nicht möglich (Abb. 2.2).

2.5 KI-Projekte in Unternehmen

Da KI-Projekte auch in Unternehmen zunehmend an Relevanz gewinnen und entsprechend budgetiert werden, ist es wichtig, die rechtlichen Erfordernisse solcher Projekte frühzeitig in die Planung mit einzubeziehen.

Die wirtschaftlichen Interessen an Entwicklung und Einsatz von KI auf der einen Seite und die Anforderungen des Datenschutzrechts auf der anderen Seite stehen dabei zunächst in einem gewissen Spannungsverhältnis. Die Qualität von KI-Programmen ist eng mit der Menge der verfügbaren Trainingsdaten verknüpft. Die Definition konkreter Einsatzzwecke des KI-Programms ist oftmals jedoch erst zu einem späteren Zeitpunkt möglich. Dies steht auf den ersten Blick im Widerspruch zu den datenschutzrechtlichen Grundsätzen der Zweckbindung und der Datenminimierung. Vor diesem Hintergrund sollte am Anfang von KI-Entwicklung und -Einsatz eine Datenschutzstrategie stehen, die die wesentlichen Kernfragen datenschutzrechtlicher Compliance aufgreift und bei der Verwirklichung des jeweiligen Projektes berücksichtigt. Zielsetzung sollte es dabei sein, das unternehmerische Interesse an der KI-Entwicklung und die Anforderungen der DS-GVO bestmöglich zum Ausgleich zu bringen und dies entsprechend zu dokumentieren. Dies ist vor allem deshalb wichtig, um Bußgelder und spätere kostenintensive Anpassungen der Entwicklung von Vornherein zu vermeiden.

Fragen zur Sicherstellung datenschutzrechtlicher Compliance in KI-Projekten

1. Welche Use Cases sollen durch die Entwicklung des KI-Programms abgedeckt werden?
2. Welche Daten sollen zugrunde gelegt werden?
3. Handelt es sich bei den relevanten Daten um personenbezogene Daten?
4. Wenn ja: Ist eine Anonymisierung der personenbezogenen Daten möglich?
5. Wenn nein: Ist die Nutzung der personenbezogenen Daten datenschutzrechtskonform möglich?
   a. Wer ist datenschutzrechtlich verantwortlich?
   b. Auf welche Rechtsgrundlage kann die Datenverarbeitung im Rahmen der Generierung von KI und des Einsatzes von KI-Programmen gestützt werden?
   c. Muss eine Datenschutzfolgenabschätzung durchgeführt werden?
   d. Welche Informationspflichten müssen erfüllt werden und in welcher Form?
   e. Wie kann auf Betroffenenanfragen reagiert werden?
   f. Was ist im Zusammenhang mit KI-Programmen zu beachten, die Entscheidungen auf automatisierter Basis treffen?

2.6 Personenbezug der Trainingsdaten

Wesentliche Kernfrage (Nr. 3 der Fragen zur Sicherstellung datenschutzrechtlicher Compliance in KI-Projekten) ist zunächst, ob es sich bei den zur Entwicklung des KI-Programms benötigten Trainingsdaten überhaupt um personenbezogene Daten[3] handelt, deren Vorliegen zur Anwendbarkeit der DS-GVO führt. Ist dies nämlich nicht der Fall

[3] Zu steuerrechtlichen Aspekten im Zusammenhang mit personenbezogenen Daten vgl. Abschn. 7.1.1.5 und 7.2.3.

bzw. kann auf den Einsatz solcher personenbezogenen Daten verzichtet werden, bestehen keine datenschutzrechtlichen Bedenken betreffend die Durchführung des KI-Projektes.

2.6.1 Personenbezogene Daten

2.6.1.1 Definition

Gem. Art. 2 Abs. 1 DS-GVO ist die DS-GVO nur dann sachlich anwendbar, wenn eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten oder eine nichtautomatisierte Verarbeitung personenbezogener Daten vorliegt, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Eine Definition personenbezogener Daten enthält Art. 4 Nr. 1 DS-GVO. Erfasst sind danach „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen." Zur Feststellung der Identifizierbarkeit einer Person sollten laut Erwägungsgrund (EG) 26 der DS-GVO „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern." Zur Bestimmung der Wahrscheinlichkeit des Einsatzes solcher Mittel sollten gemäß EG 26 DS-GVO „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."

2.6.1.2 Pseudonymisierte Daten

Bei pseudonymisierten Daten liegen auch weiterhin personenbezogene Daten vor und ist damit auch die DS-GVO anwendbar. Eine Pseudonymisierung liegt gem. Art. 4 Nr. 5 DS-GVO vor, wenn „die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können." Diese zusätzlichen Informationen müssen „gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden" (vgl. dazu auch Bitkom e.V. 2017, S. 132).

2.6.1.3 Trainingsdaten

Handelt es sich bei den im Rahmen des Machine-Learning-Prozesses eingegebenen Daten um personenbezogene Trainingsdaten, ist damit der sachliche Anwendungsbereich der DS-GVO eröffnet. Dies gilt ebenfalls für den Output der solchermaßen eingegebenen und über mehrere Schichten verarbeiteten Daten. Letztlich bedarf die Frage, ob personenbezogene Daten involviert sind, stets einer Analyse des Einzelfalls.[4] Je stärker Big-Data-

[4] Vgl. zum Personenbezug bei Daten von Big-Data-Analysen ausführlich Schefzig (2014, S. 103–118).

Analysen auf die Identifizierung konkreter Muster und die Aussonderung eines Individuums ausgerichtet sind, etwa zum Zwecke der Betrugsprävention im Versicherungs- und Gesundheitswesen, desto näher liegt die Anwendbarkeit der DS-GVO (vgl. hierzu und im Folgenden Schulz 2018, Art. 6, Rn. 256–259). Gleiches gilt, wenn im Rahmen der KI-Generierung bestehende Datensätze ausgewertet und neue Informationen hinzugespeichert werden. Umgekehrt sind auch Vorhersagemodelle (*Predictive Analytics*) oder Simulationen denkbar, die entweder bereits während der Ersterhebung oder bei einer zweckändernden Nutzung personenbezogener Daten diese anonymisieren. In diesem Fall ist die DS-GVO entweder nicht anwendbar oder der Anwendungsbereich wird unmittelbar wieder verlassen.

2.6.2 Anonymisierungsmöglichkeiten

Abhängig von der Art des zu generierenden KI-Programms gibt es Möglichkeiten, auf die Nutzung personenbezogener Daten zu verzichten. Dies hat den Vorteil, dass die Einschränkungen der DS-GVO gerade nicht zur Anwendung gelangen. Allein die Pseudonymisierung personenbezogener Daten ist dafür nicht ausreichend, auch wenn diese etwa im Bereich der Interessenabwägung zugunsten des KI-Anbieters wirken kann. Vielmehr bedarf es einer Anonymisierung der relevanten Daten im vorstehend geschilderten Umfang. Unternehmen stehen daher vor der Herausforderung, Verfahren zur Anonymisierung personenbezogener Daten zu finden, ohne dass die Qualität des KI-Programms darunter leidet (vgl. hierzu und im Folgenden Drechsler und Jentsch 2018, S. 2).

Bisher erfolgte eine Veränderung personenbezogener Daten etwa durch Verrauschung oder Vergröberung. Beides wirkt sich allerdings negativ auf die Datenqualität aus. Daher wurden in der Vergangenheit Methoden zur Anonymisierung häufig als impraktikabel angesehen oder waren schlicht zu arbeitsaufwändig (vgl. Drechsler und Jentsch 2018, S. 2). Auch gegenwärtig setzt daher die Entwicklung von KI-Programmen häufig noch auf personenbezogenen Daten auf. Aufgrund der durch steigende Rechnerkapazitäten eröffneten Möglichkeiten des maschinellen Lernens nehmen jedoch Anstrengungen von Unternehmen zu, KI-Programme auf Basis anonymisierter Daten zu entwickeln. Kommen entsprechende technische Ansätze, die die Möglichkeit der Anonymisierung von Trainingsdaten bieten, zum Einsatz, unterfällt die KI-Generierung in solchen Fällen gar nicht erst dem Anwendungsbereich der DS-GVO. Daher sollte bei jeder Entwicklung eines KI-Programms geprüft werden, ob derartige Anonymisierungstechniken aus technischer Sicht sinnvollerweise zum Einsatz kommen und datenschutzrechtliche Hindernisse von vornherein ausgeschlossen werden können.

2.6.2.1 Synthetisierung von Daten

Im Rahmen der Daten-Synthetisierung wird ein Originaldatensatz durch neu generierte Daten ersetzt, die die wesentlichen statischen Merkmale des ursprünglichen Datensatzes enthalten (vgl. Drechsler und Jentsch 2018, S. 2). Die Originaldaten werden dabei durch

einen algorithmischen Prozess in einen synthetischen Datensatz überführt (vgl. Drechsler und Jentsch 2018, S. 5–6). Die künstlich erzeugten Daten (auch **Surrogatdaten** oder **artifizielle Daten**) werden demnach nicht durch eine direkte Erhebung bei den Betroffenen gewonnen, auch wenn für die Herstellung der künstlichen Daten Originaldaten verwendet werden müssen (vgl. Drechsler und Jentsch 2018, S. 5–6).

Unabhängig von der Frage, inwieweit für die Überführung der Originaldaten in Surrogatdaten die DS-GVO einschlägig ist,[5] ließe sich der Zweck der Verarbeitung der Originaldaten – nämlich Datenverarbeitung zwecks Erstellung synthetischer Datensätze – anders als im Rahmen der KI-Entwicklung, deren Einsatz später oft für ursprünglich nicht antizipierte Zwecke in Betracht kommt, eindeutig benennen. Zudem käme eine Rechtfertigung auf Grundlage berechtigter Interessen in Betracht (zu Rechtfertigungsgrundlagen allgemein Abschn. 2.8). Für sämtliche allein auf Basis der synthetischen Daten gewonnenen Erkenntnisse sind dann ohnehin die Vorgaben der DS-GVO nicht mehr maßgeblich, soweit jedenfalls der Originaldatensatz vollständig in einen synthetischen Datensatz überführt worden ist. Insbesondere bedürfen auch spätere Zweckänderungen beim Einsatz der synthetischen Datensätze keiner datenschutzrechtlichen Rechtfertigung mehr.

2.6.2.2 Generative Adversarial Networks

Bei sog. **Generative Adversarial Networks** (**GANs**) handelt es sich um eine Deep-Learning-Methode, im Rahmen derer synthetische Daten produziert werden (Abb. 2.3). Dabei arbeiten zwei konkurrierende neuronale Netze, die mit der gleichen Datensammlung trainiert werden, gegeneinander (vgl. hierzu und im Folgenden Giles 2018a, S. 59). Das erste neuronale Netz (**Generator**) generiert dabei möglichst realistische Outputs, z. B. künstlich erzeugte Fotos oder Handschriften. Das zweite Netz (**Diskriminator**) vergleicht den Output mit echten Trainingsbildern und bestimmt, ob ein Original oder eine Fälschung vorliegt. Dadurch wird der Input für das erste Netz verbessert, das seine Parameter entsprechend anpassen kann. Entsprechend bieten GANs die Möglichkeit der Schaffung künstlicher Szenarien, die echten entsprechen. So können etwa auf Grundlage von im Internet verfügbaren

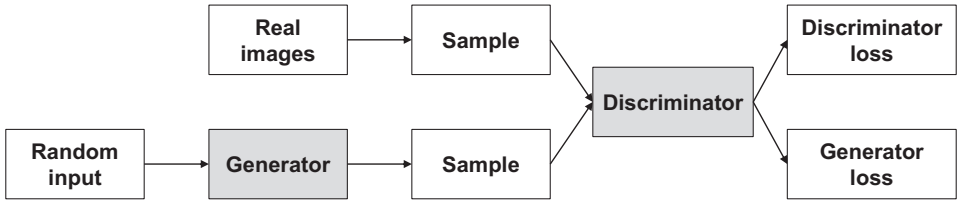

Abb. 2.3 Generative Adversarial Network (Google Developers 2019, developers.google.com/machine-learning/gan/gan_structure)

[5] Zu der Frage, inwieweit eine Anonymisierung personenbezogener Daten einen Verarbeitungsvorgang i.S.d. DS-GVO darstellt vgl. Abschn. 2.7.3.1.2.

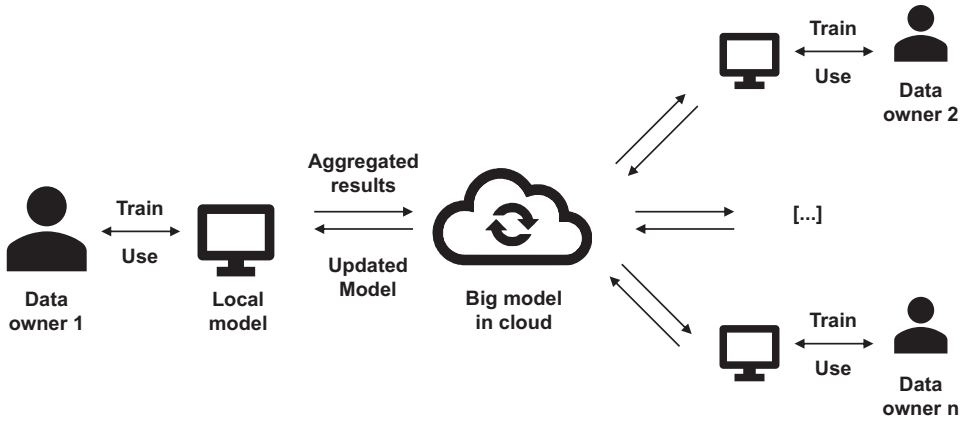

Abb. 2.4 Federated Machine Learning (in Anlehnung an Borzymowski 2019)

Fotos neue, synthetische Bilder erzeugt werden.[6] Auf Basis der solchermaßen generierten anonymisierten Daten ist dann ein weiteres Training außerhalb der strengen Vorschriften der DS-GVO möglich. Gerade im Bereich der medizinischen Forschung bietet das GAN-Verfahren vielfältige Möglichkeiten. Ist im Regelfall für die Verarbeitung von Gesundheitsdaten zwingend eine Einwilligung gem. Art. 9 Abs. 2 lit. a DS-GVO erforderlich, wäre diese im Falle künstlich erzeugter Krankenakten obsolet (Giles 2018b).

2.6.2.3 Federated Machine Learning

Beim sog. **Federated Machine Learning** (Abb. 2.4) handelt es sich um ein ML-Verfahren, bei dem ein Algorithmus über mehrere dezentralisierte Endgeräte trainiert wird, die jeweils auf Grundlage eigener Trainingsdaten trainieren. Die KI-Berechnungen erfolgen also unmittelbar auf dem Endgerät. Die Ergebnisse der solchermaßen trainierten lokalen Modelle werden dann im zweiten Schritt zusammengeführt und aggregiert (Borzymowski 2019). Das dadurch erzeugte globale Modell wird schließlich wieder zu den lokalen Datenquellen zurückgespielt, die auf dieser Basis weiter trainieren (Borzymowski 2019). Es werden somit keine personenbezogenen Daten an das globale Modell übermittelt.

2.7 Datenschutzrechtliche Verantwortlichkeiten

Können Anonymisierungstechniken nicht sinnvoll eingesetzt werden und ist die DS-GVO sowohl sachlich als auch räumlich anwendbar, stellt sich die Frage nach den datenschutzrechtlich verantwortlichen Akteuren. Dies ist insbesondere dann der Fall, wenn mehrere Parteien in die für die Schaffung von KI-Programmen erforderliche Datenverarbeitung

[6] Vgl. hierzu https://www.thispersondoesnotexist.com/ und OpenAI Blog, https://openai.com/blog/generative-models/.

involviert sind. Bei den Beteiligten handelt es sich insbesondere um die einbezogenen Entwickler des Programms, den Dienstleister bzw. Hersteller des KI-Programms sowie das Unternehmen, das dieses KI-Programm auf den Markt bringt. Bei der Frage, in welchem datenschutzrechtlichen Verhältnis diese Akteure zueinanderstehen, ist wiederum eine Betrachtung des jeweiligen Einzelfalls maßgeblich. Sind zwei (oder mehr) Parteien involviert, kommen datenschutzrechtlich grundsätzlich immer die folgenden Szenarien in Betracht: Auftragsverarbeitung, Joint Controllership oder eine jeweils eigenständige Verantwortlichkeit.

2.7.1 Auftragsverarbeitung

Nach der Legaldefinition des Art. 4 Nr. 8 DS-GVO ist unter einem **Auftragsverarbeiter** „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle zu verstehen, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet." Den Auftragsverarbeiter zeichnet dabei seine Weisungsgebundenheit gegenüber dem Verantwortlichen aus.

Bei dem **Verantwortlichen** handelt es sich gem. Art. 4 Abs. 1 Nr. 7 DS-GVO um „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (…)." Der Verantwortliche muss als „Herr der Daten" seine Auftragsverarbeiter sorgfältig auswählen (vgl. Art. 28 Abs. 1 DS-GVO) und ist für die datenschutzrechtliche Zulässigkeit der von ihm beauftragten Datenverarbeitungsvorgänge verantwortlich (Thalhofer und Zdanowiecki 2019, § 19, Rn. 150).

Unabhängig davon, ob das KI-Programm von einem Dritten entwickelt wurde, wird es sich bei dem Unternehmen, das das KI-Programm einsetzt, i. d. R. um den datenschutzrechtlich Verantwortlichen handeln (dazu Abschn. 2.7.3.1). Dies entspricht auch der Art. 24 Abs. 1 DS-GVO zugrunde liegenden Erwägung, die nicht etwa den Hersteller von Verarbeitungstechnologien, sondern allein den Verantwortlichen in die Pflicht nimmt, der diese auswählt und einsetzt und damit auch ursächlich für den Einsatz des jeweiligen Systems und dessen Folgen ist (vgl. Martini 2018, Art. 24, Rn. 18).

2.7.1.1 Weisungsgebundenheit

Ob es sich bei dem Anbieter des KI-Programms, der dieses für ein Unternehmen betreibt, um einen Auftragsverarbeiter oder einen ebenfalls bzw. gemeinsam Verantwortlichen handelt, hängt davon ab, inwieweit eine Weisungsgebundenheit des Anbieters gegenüber dem Verantwortlichen vorliegt. Dies schließt allerdings nicht aus, dass der Verantwortliche dem Auftragsverarbeiter die Entscheidung über technisch-organisatorische Fragen überlässt[7] (DSK 2018a, S. 1). Auch wenn der Auftragsverarbeiter demnach durchaus eigenver-

[7] Noch zur Richtlinie 95/46/EG (DSRL) vgl. Art.-29-Datenschutzgruppe (2010, S. 17–18).

antwortlich Aufgaben wahrnehmen kann, bleibt die Festsetzung der Verarbeitungszwecke und der wesentlichen Elemente der Datenverarbeitungsmittel (z. B. Art der verarbeiteten Daten, Dauer der Datenverarbeitung und die Entscheidung über den Zugang zu den Daten) weiterhin allein dem Verantwortlichen überlassen (Art.-29-Datenschutzgruppe 2010, S. 17–18).

Eine solche Weisungsgebundenheit ist in verschiedenen Fallkonstellationen denkbar. Lässt ein Unternehmen ein KI-System von einem externen Dienstleister entwickeln und greift dieser auf personenbezogene Daten der Endkunden des Auftraggebers zu, mittels derer die KI zu ihrem jeweiligen Zweck trainiert wird, handelt es sich um eine weisungsgebundene Tätigkeit und einen klassischen Fall der Auftragsverarbeitung. Oftmals entwickeln Unternehmen KI-Systeme jedoch angesichts hoher Entwicklungskosten nicht selbst oder geben eine solche Entwicklung in Auftrag, sondern greifen auf bereits bestehende und oftmals Cloud-basierte KI-Lösungen eines externen Dienstleisters zurück („**KI as a Service**"). Auch dies geschieht wiederum im Auftrag des verantwortlichen Unternehmens und stellt damit ebenfalls eine Variante der Auftragsverarbeitung dar.

Beispiel

Relevante KI-Anwendungen stellen etwa Chatbots im Bereich Customer Service, Sprachassistenten oder Textautomation dar. Personenbezogene Daten der Endkunden des Unternehmens werden dabei im Rahmen des konkreten Einsatzes der KI verarbeitet.[8] ◀

Vorteil der Auftragsverarbeitung ist der Umstand, dass es für die Weitergabe der in Rede stehenden personenbezogenen Daten an den Auftragsverarbeiter bzw. der beauftragten Erhebung durch den Auftragsverarbeiter keiner zusätzlichen Rechtsgrundlage gem. Art. 6 ff. DS-GVO bedarf (DSK 2018a, S. 2). Ausreichend ist, dass der Verantwortliche selbst die Datenverarbeitung auf eine Rechtsgrundlage stützen kann.

2.7.1.2 Rechtsfolgen eines Auftragsverarbeitungsverhältnisses

Liegt eine Weisungsgebundenheit im oben beschriebenen Sinne vor, erfordert dies den Abschluss einer **Auftragsverarbeitungsvereinbarung** (**AVV**) gem. Art. 28 Abs. 3 DS-GVO (sog. **1. Stufe der Datenverarbeitung**). Bei Verstößen gegen die in Art. 28 DS-GVO enthaltenen Vorgaben drohen sowohl dem Auftraggeber als auch dem Auftragsverarbeiter gem. Art. 83 Abs. 4 DS-GVO Geldbußen von bis zu EUR 10 Mio. oder – je nachdem, welcher der Beträge höher ist – 2 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens. Erfolgt zudem etwa im Rahmen von Cloud-basierten Lösungen eine Übermittlung personenbezogener Daten von Endkun-

[8] Vgl. zu weiteren in Unternehmen eingesetzten KI-Lösungen Begleitforschung Mittelstand-Digital (2019).

den des Unternehmers in sog. Drittländer (z. B. die USA), bedarf es darüber hinaus entweder eines Angemessenheitsbeschlusses der Europäischen Kommission, dass das Drittland ein angemessenes Schutzniveau bietet (vgl. Art. 45 Abs. 3 DS-GVO), oder „geeigneter Garantien" gem. Art. 46 Abs. 1 DS-GVO, z. B. in Form von Standardvertragsklauseln oder, Binding Corporate Rules (sog. **2. Stufe der Datenverarbeitung**).[9] Werden die an die Übermittlung in Drittländer gestellten Anforderungen nicht erfüllt, droht sogar ein Bußgeld von bis zu EUR 20 Mio. oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens. Auch hier richtet sich das Bußgeld nach dem höheren der beiden Beträge. Zudem drohen gem. Art. 82 Abs. 2 S. 2 Auftragsverarbeitern, wenn sie gegen speziell für sie geltende Pflichten verstoßen (vgl. Art. 28 Abs. 2 bis Abs. 4 DS-GVO), Schadensersatzforderungen von Betroffenen.

2.7.2 Joint Controllership

Wird ein externer Dienstleister eingesetzt, stellt sich immer auch die Frage, ob das das KI-Programm einsetzende Unternehmen und der Dienstleister bzw. Hersteller des KI-Programms möglicherweise **gemeinsame Verantwortliche** i.S.d. Art. 26 DS-GVO sind. Die Abgrenzung stellt den Rechtsanwender in der Praxis oftmals vor Schwierigkeiten, weil auch im Falle der Auftragsverarbeitung dem Auftragversarbeiter ein gewisser Entscheidungsspielraum im Hinblick auf die technisch-organisatorischen Fragen der Verarbeitung zukommen kann (Abschn. 2.7.1.1).

2.7.2.1 Gemeinsame Festlegung der Zwecke und Mittel

Mehrere Verantwortliche können gemeinsam verantwortlich sein, wenn sie gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen (Art. 26 Abs. 1 DS-GVO). Die Schwelle zum Joint Controllership ist nach der Rechtsprechung des EuGH niedrig.[10] Danach ist es ausreichend, wenn die eine Partei der anderen die Verarbeitung ermöglicht und einen faktischen Einfluss auf die Datenverarbeitung nimmt (bei FB Insights durch Parametrierung)[11] und der von der einen Partei verfolgte kommerzielle Zweck eine Gegenleistung für den der anderen Partei gebotenen Vorteil darstellt.[12] Zwar erfolgten die einschlägigen Entscheidungen des EuGH noch zur DSRL, jedoch kommt ihnen für die DS-GVO Indizwirkung zu.

[9] „Zur Datenübermittlung in Drittländer vgl. EuGH 16.07.2020 – Rs. C-311/18 – Schrems II."

[10] Vgl. EuGH 5. Juni 2018 – Rs. C-2010-16 = NJW 2018, 2537 – Fanpages; EuGH 10. Juli 2018 – Rs. C-25/17 = NJW 2019, 285 – Jehovan todistajat; EuGH 29. Juli 2019 – Rs. C-40/17 = NJW 2019, 2755 – Fashion ID.

[11] Vgl. EuGH 5. Juni 2018, NJW 2018, 2537, Rn. 36.

[12] EuGH 29. Juli 2019, NJW 2019, 2755, Rn. 80.

2.7.2.1.1 Gemeinsames Festlegen der Zwecke und Mittel der Verarbeitung

Erste Voraussetzung für das Vorliegen einer gemeinsamen Verantwortlichkeit ist das Merkmal der „Gemeinsamkeit". Bereits in ihrer Stellungnahme zur alten DSRL ging die zwischenzeitlich vom **Europäischen Datenschutzausschuss** (**EDSA**)[13] ersetzte Art.-29-Datenschutzgruppe davon aus, dass der Begriff „gemeinsam" im Sinne von „nicht alleine" zu verstehen sei (Art.-29-Datenschutzgruppe 2010, S. 22). Dieses Verständnis spiegelt auch die Definition des „Verantwortlichen" in Art. 4 Nr. 7 DS-GVO, wonach der Verantwortliche „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" und damit von einer Beteiligung von mehr als einer Person für eine Gemeinsamkeit ausgeht (vgl. Spoerr 2020, Art. 26 DS-GVO Rn. 15).

Das gemeinsame Festlegen erfordert dabei einen bestimmenden tatsächlichen Einfluss der Verantwortlichen, nicht jedoch eine vollständig gleichrangige oder gleichwertige Verantwortlichkeit im Hinblick auf die Entscheidung über die Zwecke und Mittel der Verarbeitung[14] (DSK 2018b, S. 2). Die gemeinsame Verantwortung bezieht sich zudem nur auf die Phase der Datenverarbeitung, für die die Beteiligten gemeinsam über Zwecke und Mittel entschieden haben.[15] Nicht erforderlich ist hingegen eine „umfassende Kontrolle" der Parteien über sämtliche Phasen der Datenverarbeitung (DSK 2018b, S. 2), d. h. die gemeinsame Verantwortlichkeit ist jeweils vorgangsbezogen zu ermitteln. Auch die Möglichkeit des Zugriffs auf die Daten ist nicht erforderlich.[16]

2.7.2.1.2 Festlegung der Zwecke der Verarbeitung

Gemäß der von der Art.-29-Datenschutzgruppe vorgenommenen Definition handelt es sich bei dem festzulegenden „Zweck" um ein „erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet" (Art.-29-Datenschutzgruppe 2010, S. 16), und mithin um das unmittelbare oder mittelbare Ziel der jeweiligen Datenverarbeitung (Specht-Riemenschneider und Schneider 2019, S. 505). Die Parteien müssen mit der Datenverarbeitung entweder einen gemeinsamen oder eigenen Zweck verfolgen (vgl. Spoerr 2020, Art. 26, Rn. 17; Specht-Riemenschneider und Schneider 2019, S. 505). Soweit die Beteiligten unterschiedliche Zwecke verfolgen, ist der erforderliche bestimmende Einfluss auf die Datenverarbeitung dann gegeben, wenn „eine Zweckverfolgung im Rahmen dieser konkreten Datenverarbeitung nicht ohne die andere möglich ist" (DSK 2018b, S. 2). Ähnlich äußert sich der EuGH. Danach können auch eigene wirtschaftliche Zwecke der Beteiligten an den Datenverarbeitungsvorgängen ausreichend sein, wenn der damit jeweils verfolgte „wirtschaftliche Vorteil" die „Gegenleistung für den (der anderen Partei) gebotenen Vorteil" darstellt.[17]

---

[13] Dieser hat die Orientierungshilfen der Art.-29-Datenschutzgruppe in weiten Teilen übernommen.

[14] EuGH 5. Juni 2018, NJW 2018, 2537, Rn. 43.

[15] EuGH 29. Juli 2019, NJW 2019, 2755, Rn. 70.

[16] EuGH 10. Juli 2018, NJW 2019, 285, Rn. 75.

[17] EuGH 29. Juli 2019, NJW 2019, 2755, Rn. 80; vgl. ferner Spoerr (2020, Art. 26, Rn. 17) mit weiteren Hinweisen zu insoweit kritischen Stimmen.

2.7.2.1.3 Entscheidung über die Mittel der Verarbeitung

In seinen Entscheidungen zur gemeinsamen Verantwortlichkeit differenziert der EuGH nicht zwischen der gemeinsamen Festlegung der Zwecke und der gemeinsamen Festlegung der Mittel der Verarbeitung. Um jedoch einzelne Fallkonstellationen – gerade auch im KI-Bereich – ausreichend bewerten zu können, bedarf es der Klärung der Frage, inwieweit es neben einer gemeinsamen Festlegung der Zwecke der Verarbeitung auch einer Festlegung der Mittel der Verarbeitung bedarf.

Die Art.-29-Datenschutzgruppe ging insoweit davon aus, dass eine gemeinsame Kontrolle dann gegeben ist, „wenn verschiedene Parteien im Zusammenhang mit spezifischen Verarbeitungen entweder über den Zweck oder über wesentliche Elemente der Mittel entscheiden, die einen für die Verarbeitung Verantwortlichen kennzeichnen“ (Art.-29-Datenschutzgruppe 2010, S. 23). Danach genügt eine gemeinsame Festlegung entweder der Zwecke **oder** der Mittel der Datenverarbeitung.

Demgegenüber führt die Datenschutzkonferenz in ihrem Kurzpapier zur gemeinsamen Verantwortlichkeit aus, dass „eine Beteiligung der Parteien an der Bestimmung der Zwecke **und** Mittel sehr verschiedene Formen annehmen könne“ (DSK 2018b, S. 2). Damit scheint die DSK von der Notwendigkeit einer gemeinsamen Festlegung sowohl der Zwecke als auch der – „zumindest wesentlichen Elemente der“ – Mittel der Datenverarbeitung auszugehen (DSK 2018b, S. 1; Spoerr 2020, Art. 26, Rn. 17). Gleichzeitig sei von einer solchen gemeinsamen Festlegung jedoch auch dann auszugehen, wenn die „verwendende Stelle (…) im Voraus durch den Anbieter festgelegte Zwecke und Mittel akzeptiere bzw. sich diesen anschließe.“ (DSK 2018b, S. 3). Jedenfalls im Ergebnis genügt dann auch nach Auffassung der DSK eine gemeinsame Festlegung nur der Zwecke der Verarbeitung, wenn sich einer der Beteiligten den bereits vorab vom anderen Beteiligten ausgewählten Mitteln anschließt.

2.7.2.2 Rechtsfolgen einer gemeinsamen Verantwortlichkeit

Liegt eine gemeinsame Verantwortlichkeit vor, ist der Abschluss einer Vereinbarung erforderlich, die den Anforderungen des Art. 26 Abs. 1 DS-GVO entspricht. Nur wenn es sich bei den Parteien um unabhängig voneinander Verantwortliche handelt (Abschn. 2.7.2.3), wäre weder der Abschluss einer AVV noch einer Vereinbarung gem. Art. 26 Abs. 1 DS-GVO erforderlich.

Jeder der gemeinsam Verantwortlichen haftet gem. Art. 82 Abs. 4 i. V. m. Abs. 2 Satz 1 DS-GVO im Falle einer nicht DS-GVO-konformen Datenverarbeitung für den gesamten Schaden, sofern ihm nicht der Nachweis seines fehlenden Verschuldens gelingt (Art. 82 Abs. 3 DS-GVO) (DSK 2018b, S. 4). Fehlt eine Vereinbarung nach Art. 26 DS-GVO trotz Bestehens einer gemeinsamen Verantwortlichkeit, können hierfür Geldbußen nach Art. 83 Abs. 4 lit. a DS-GVO verhängt werden.

2.7.2.3 Datenübermittlung zwischen gemeinsam Verantwortlichen

Art. 26 DS-GVO lässt offen, ob Datenübermittlungen zwischen gemeinsam Verantwortlichen einer gesonderten Rechtsgrundlage nach Art. 6 bzw. Art. 9 DS-GVO bedürfen.

Europaweit abgestimmte Stellungnahmen der Datenschutz-Aufsichtsbehörden zu dieser Frage existieren derzeit (noch) nicht. Die deutschen Aufsichtsbehörden vertreten jedoch in ihrem Papier zur gemeinsamen Verantwortlichkeit (DSK 2018b, S. 1) die Auffassung, dass eine Übermittlung personenbezogener Daten unter gemeinsam Verantwortlichen ein eigener Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DS-GVO sei und als solcher einer Rechtsgrundlage bedürfe.

Zu derselben Sichtweise tendiert auch die Rechtsprechung des Europäischen Gerichtshofs. Nach Auffassung des EuGH trage die Rechtsfigur der gemeinsamen Verantwortlichkeit dazu bei, einen „umfassenderen Schutz der Rechte" Betroffener sicherzustellen.[18] Diese Wertung steht ebenfalls einer „Privilegierung" der Beziehung zwischen zwei Verantwortlichen im Fall der gemeinsamen Verantwortlichkeit entgegen.

2.7.2.4 Unabhängig voneinander Verantwortliche

Liegt im Zusammenhang mit der Verarbeitung personenbezogener Daten zur Herstellung oder für den Einsatz einer KI-Applikation weder ein Auftragsverarbeitungsverhältnis noch die Rechtsfigur der gemeinsamen Verantwortlichkeit vor, handelt es sich um unabhängig voneinander bzw. selbstständige Verantwortliche. Ebenso wie im Falle der gemeinsamen Verantwortlichkeit bedarf es auch hier einer gesonderten Rechtsgrundlage für die Übermittlung personenbezogener Daten zwischen den Beteiligten und haften auch hier die Verantwortlichen gem. Art. 82 Abs. 4 i. V. m. Abs. 2 Satz 1 DS-GVO gemeinsam, wenn sie sich nicht exkulpieren können.

Eine Vereinbarung gemäß Art. 26 Abs. 1 DS-GVO ist nicht erforderlich. Gleichwohl ist zu empfehlen, dass die Parteien freiwillig eine Vereinbarung abschließen. Im Falle rechtlicher Streitigkeiten zwischen den selbstständigen Verantwortlichen schafft diese Klarheit für die Abwicklung des Haftungsausgleichs im Innenverhältnis gem. Art. 82 Abs. 5 DS-GVO (vgl. dazu auch DSK 2018b, S. 4).

2.7.3 Datenschutzrechtliche Rollenverteilung in KI-Projekten

In der Praxis bedarf es auch im Kontext von KI-Projekten insbesondere der Abgrenzung zwischen Auftragsverarbeitungsvereinbarung und gemeinsamer Verantwortlichkeit sowie zwischen der gemeinsamen Verantwortlichkeit und der bloßen Übermittlung zwischen unabhängig voneinander Verantwortlichen. In welchem datenschutzrechtlichen Verhältnis die an der Verarbeitung Beteiligten zueinander stehen und ob ggfs. der Abschluss einer entsprechenden Vereinbarung gesetzlich zwingend ist, hängt letztendlich jedoch vor allem von den genauen Umständen des Einzelfalls ab.[19]

[18] EuGH 5. Juni 2018, NJW 2018, 2537, Rn. 42.

[19] Vgl. dazu auch EuGH 5. Juni 2018, NJW 2018, 2537, Rn. 43.

Die nachfolgende Bewertung erfolgt aufgrund der Annahme, dass es sich bei den gegenständlichen KI-Systemen jeweils um sog. **schwache KI** handelt. Die Benennung eines Verantwortlichen wird jedoch spätestens dann an ihre Grenzen stoßen, wenn die derzeit noch auf der Ebene schwacher KI entwickelten Programme die Grenze zur starken KI überschreiten, die als solche selbst in der Lage ist, über Mittel und Zwecke der Verarbeitung zu entscheiden.

2.7.3.1 Auftragsverarbeitungsverhältnis

Ein klassisches Auftragsverarbeitungsverhältnis liegt im Kontext von KI dann vor, wenn ein Auftraggeber sich eines externen Dienstleisters bedient, um personenbezogene Daten unter Einsatz des vom Dienstleister entwickelten KI-Systems verarbeiten zu lassen. Oftmals handelt es sich dabei um Cloud-basierte Systeme, d. h. der Dienstleister ist entweder selbst ein Cloud-Anbieter oder er bedient sich stattdessen eines weiteren Dienstleisters. Es handelt es sich hier um eine typische weisungsgebundene Tätigkeit, weil der Dienstleister die betroffenen personenbezogenen Daten (z. B. der Arbeitnehmer oder Endkunden des Auftraggebers) nur im Rahmen der vom Auftraggeber gemachten Vorgaben verarbeitet.

Beispiel

Denkbar ist z. B. der Einsatz von Chatbots, der von dessen Anbieter für das Unternehmen betrieben wird. Chatbots erfüllen jedenfalls gegenwärtig noch bestimmte Funktionen, beispielsweise im Bereich des Customer Service. Auch wenn es sich hier nicht um KI im engeren Sinne handelt, d. h. um ein System, das autonom Entscheidungen trifft, sind insbesondere datenschutzrechtliche Aspekte zu beachten. So werden auch im Rahmen des Chats und der Serviceanfragen der Endkunden i. d. R. personenbezogene Daten verarbeitet.

Überdies setzen Online-Shops häufig KI-Dienstleister ein, die das Bonitätsscoring im Rahmen von Bestellprozessen übernehmen. Gleiches gilt für Versicherungen, die Schadensabwicklungsprozesse möglichst effizient durchführen möchten und zu diesem Zwecke die KI externer Anbieter einsetzen. In beiden Fällen verarbeiten die jeweiligen Dienstleister unter Einsatz der von ihnen entwickelten KI weisungsabhängig die Daten der Endkunden des jeweiligen Auftraggebers, sodass es sich hier jeweils um ein Auftragsverarbeitungsverhältnis handelt. ◀

Häufig möchten sich die in Abschn. 2.7.3.1 genannten Auftragsverarbeiter in Verträgen mit dem Auftraggeber das Recht einräumen lassen, die durch ihren KI-Dienst verarbeiteten Daten auf anonymisierter Basis für eigene Zwecke zu nutzen. Grundsätzlich fallen anonymisierte Daten nicht unter die DS-GVO, d. h. es wären dann weder vom Auftraggeber noch vom Dienstleister bestimmte weitergehende datenschutzrechtliche Vorgaben, etwa im Hinblick auf die Notwendigkeit des Vorliegens einer Rechtsgrundlage, zu beachten.

Es stellt sich jedoch die Frage, ob eine Anonymisierung als Verarbeitung i.S.d. DS-GVO zu verstehen ist und daher ein vom Dienstleister vorgenommener Anonymisierungsvorgang als solcher einer datenschutzrechtlichen Rechtfertigungsgrundlage bedarf. In die-

sem Falle wäre der KI-Anbieter selbstständiger Verantwortlicher (vgl. dazu Abschn. 2.7.3), da er den Anonymisierungsvorgang zunächst nur für die Zwecke des Trainings und potenziellen weiteren Kommerzialisierung seiner KI verfolgt.

2.7.3.1.1 Anonymisierung gem. § 3 BDSG a.F.

Nach § 3 Abs. 4 Nr. 2 BDSG a.F. war unter dem Begriff der Verarbeitung „das Speichern, **Verändern**, Übermitteln, Sperren und Löschen personenbezogener Daten" zu verstehen. Der Begriff der Anonymisierung wurde in § 3 Abs. 6 BDSG a.F. explizit definiert. Danach war das Anonymisieren „das **Verändern** personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." Vor diesem Hintergrund lag in der Anonymisierung eine Verarbeitungstätigkeit gem. Art. 3 Abs. 4 Nr. 2 BDSG a.F. Auch die Art.-29-Datenschutzgruppe ging insoweit davon aus, dass es sich bei der Anonymisierung um eine „Weiterverarbeitung personenbezogener Daten handle" und es insofern einer Rechtsgrundlage für diese Verarbeitungstätigkeit bedürfe (Art.-29-Datenschutzgruppe 2014, S. 3).

2.7.3.1.2 Anonymisierung unter der DS-GVO

In der DS-GVO wird der Begriff der Anonymisierung nicht mehr definiert. Auch die Definition des Verarbeitungsbegriffs in Art. 4 Nr. 2 DS-GVO enthält keine konkrete Bezugnahme auf den Begriff der Anonymisierung. In der Literatur wird teilweise impliziert, dass der Verarbeitungsbegriff auch den Akt der Anonymisierung umfasse. So könne neben Löschung und Vernichtung auch eine „vollständige De-identifkation" eine „Verarbeitungsoperation" darstellen (Klabunde 2018, Art. 4 Rn. 23). Geht man mit dieser Auffassung davon aus, dass die Anonymisierung ein eigenständiger Verarbeitungsakt ist, handelt es sich bei dem KI-Anbieter um einen selbstständigen Verantwortlichen gem. DS-GVO und bedarf es für den Anonymisierungsvorgang einer hinreichenden datenschutzrechtlichen Rechtfertigung.

Nach anderer Auffassung sei Voraussetzung für eine Veränderung, unter die nach der alten Rechtslage explizit auch die Anonymisierung gefasst wurde, dass die Daten einen „neuen Informationswert" erhielten (vgl. dazu und im Folgenden Schild 2020, Art. 4, Rn. 45). Dies sei nicht der Fall, wenn die Information nur reduziert, jedoch nicht verändert werde. Dieser Auffassung ist zuzustimmen, weil eine Anonymisierung als solche, die gerade auf die Entfernung des Personenbezugs abzielt, unter der DS-GVO nicht schutzwürdig ist und daher auch keiner gesonderten Rechtsgrundlage bedarf. Insofern handelt der KI-Anbieter an dieser Stelle auch nicht als Verantwortlicher mit der Folge, dass es keiner Rechtfertigung für die Anonymisierung bedarf.

2.7.3.2 Gemeinsame Verantwortlichkeit

Die Grenze von Auftragsverarbeitungsverhältnis zur gemeinsamen Verantwortlichkeit ist jedoch dann überschritten, wenn ein Anbieter die eigene KI mit den zunächst innerhalb der Vorgaben des Auftraggebers verarbeiteten personenbezogenen Daten mit Zustimmung

des Auftraggebers zu eigenen Zwecken weitertrainieren möchte, um zum einen sein KI-System zu optimieren und auf dieser Grundlage auch anderen Kunden ein hochwertigeres KI-Produkt anbieten, zum anderen aber auch für den Auftraggeber bessere Ergebnisse erzielen zu können. In dieser Konstellation liegt zunächst eine gemeinsame Festlegung der Zwecke der Datenverarbeitung vor (vgl. Art. 26 Abs. 1 DS-GVO). Beide Parteien verfolgen hier unterschiedliche Zwecke und der „wirtschaftliche Vorteil" des Auftraggebers, der in verbesserten Ergebnissen des jeweiligen KI-gesteuerten Dienstes liegt, stellt die Gegenleistung für den dem KI-Anbieter gebotenen Vorteil dar, nämlich der Verbesserung seines KI-Produktes. Geht man mit der DSK auch von dem Erfordernis einer gemeinsamen Entscheidung über die Mittel der Verarbeitung aus, steht dies ebenfalls der Annahme einer gemeinsamen Verantwortlichkeit nicht entgegen. Das für die Datenverarbeitung zum Einsatz kommende Mittel stellt vorliegend das KI-System dar, das zwar vom Anbieter selbst ohne Zutun des Auftraggebers entwickelt wurde, dessen Einsatz sich der Auftraggeber jedoch angeschlossen hat (vgl. DSK 2018b, S. 3).

Eine gemeinsame Verantwortlichkeit liegt auch in einer Konstellation vor, in denen Dritte auf das KI-Programm und darin verarbeitete personenbezogene Daten zugreifen können oder in der das Programm mit Daten aus anderen Quellen angereichert wird.

- Im Falle der gemeinsamen Verantwortung muss sichergestellt werden, dass für die weitergehende Datenverarbeitung durch den KI-Anbieter eine geeignete Rechtsgrundlage vorliegt. In der Regel dürfte es jedoch an einer Einwilligung der Betroffenen fehlen, sodass regelmäßig nur eine Rechtfertigung über berechtigte Interessen in Betracht kommt (Abschn. 2.8.3).

2.7.3.3 Unabhängig voneinander Verantwortliche

Ein KI-Anbieter, der seine Dienste einem Unternehmen zur Verfügung stellt und im Rahmen der Erbringung seiner KI-Dienste personenbezogene Daten des Unternehmens verarbeitet, handelt in Bezug auf die für den Auftraggeber verarbeiteten personenbezogenen Daten als Auftragsverarbeiter, bleibt jedoch in Bezug auf die personenbezogenen Daten, auf deren Grundlage seine KI entwickelt wurde, selbstständiger Verantwortlicher. Nur soweit – wie unter Abschn. 2.7.3.2 dargestellt – Auftraggeber und KI-Anbieter übereinkommen, die für den Auftraggeber verarbeiteten Daten zum Vorteil beider Parteien auch für das weitergehende Training und die Optimierung der Anbieter-KI zu verwenden, handelt es sich um gemeinsam Verantwortliche.

2.8 Rechtsgrundlagen für den Einsatz von KI

Zentrale Voraussetzung für die Verarbeitung personenbezogener Daten im Rahmen der Herstellung sowie des Einsatzes einer KI-Applikation ist das Vorliegen einer rechtlichen Grundlage, die in den Datenschutzbestimmungen den Betroffenen entsprechend zu erläutern ist.

In der Praxis sind insbesondere die Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO, die Vertragserfüllung gem. Art. 6 Abs. 1 S. 1 lit. b DS-GVO und überdies die berechtigten Interessen des Verantwortlichen gem. Art. 6 Abs. 1 S. 1 lit. f. DS-GVO relevante Rechtsgrundlagen.

Sind sog. besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) betroffen, ist eine Datenverarbeitung gem. Art. 9 Abs. 1 i. V. m. Abs. 2 lit. a DS-GVO nur auf Grundlage einer Einwilligung oder der in Abs. 2 statuierten Ausnahmen zulässig. Diese unterscheiden sich von den in Art. 6 Abs. 1 DS-GVO genannten. Eine Verarbeitung besonderer Kategorien personenbezogener Daten ist nämlich nicht generell für Vertragszwecke möglich (außer im Falle des Behandlungsvertrages gem. § 22 Abs. 1 Nr. 1 lit. b BDSG). Auch eine Verarbeitung auf Basis berechtigter Interessen, wie diese in Art. 6 Abs. 1 S. 1 lit. f DS-GVO vorgesehen ist, sehen die Ausnahmetatbestände in Art. 9 Abs. 2 DS-GVO nicht vor. Vor diesem Hintergrund stellt die Einwilligung gem. Art. 9 Abs. 2 lit. b DS-GVO die wesentliche Rechtfertigungsgrundlage dar, wenn ein KI-System besondere Kategorien personenbezogener Daten verarbeitet.

2.8.1 Einwilligung

Soweit es um die Generierung von KI als solcher geht, stellt die Einwilligung unter den in Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlagen die für den KI-Anbieter am wenigsten praktikable Lösung dar, weil sie jederzeit widerruflich ist. Dies stellt den KI-Entwickler vor die Frage, inwieweit in diesem Fall nachträglich Daten gem. Art. 17 Abs. 1 lit. b DS-GVO gelöscht werden müssen (Abschn. 2.11.2) bzw. inwieweit dies im Rahmen der Schaffung von KI technisch überhaupt möglich ist (vgl. zur Black Box Abschn. 2.4.2.2.2).

2.8.1.1 Anforderungen an eine wirksame Einwilligung

Den Nachweis einer wirksamen Einwilligung hat gem. Art. 7 Abs. 1 DS-GVO der Verantwortliche zu erbringen, wenn er seine Datenverarbeitung auf eine Einwilligung stützt. Die Einwilligung ist in Art. 4 Nr. 11 DS-GVO legaldefiniert. Danach muss eine wirksame Einwilligung freiwillig, spezifisch, informiert und unmissverständlich erfolgen. Die Art.-29-Datenschutzgruppe verlangt in ihren Guidelines zur Einwilligung (Art.-29-Datenschutzgruppe 2018c, S. 13), die vom EDSA übernommen wurden, dass der Einwilligungstext bestimmte Mindestangaben enthält. Diese umfassen die Identität des Verantwortlichen, den Zweck der Datenverarbeitung, die Kategorien der betroffenen Daten, das Widerrufsrecht, die Verwendung für automatisierte Einzelentscheidungen nach Art. 22 Abs. 2 DS-GVO sowie bei Übermittlungen in Drittländer die damit verbundenen Risiken, wenn ein angemessener Schutz und geeignete Garantien fehlen.

2.8.1.2 Granularität der Einwilligung

Zudem ist es erforderlich, dass die Einwilligung hinreichend granular erfolgt, d. h. zu verschiedenen Verarbeitungsvorgängen eine jeweils gesonderte Einwilligung eingeholt wird

(vgl. EG 43 DS-GVO; Art.-29-Datenschutzgruppe 2018c, S. 11). Sowohl die Spezifizierung als auch die Granularität des Einwilligungstextes lassen sich im Kontext von auf Big-Data-Analysen basierenden KI-Lösungen nur bedingt abbilden (vgl. Gausling 2019a, S. 6). Der Zweck kann in diesen Fällen anfänglich nur generisch beschrieben werden, weil zu diesem Zeitpunkt die am Ende des Trainingsprozesses geschaffenen Möglichkeiten der KI noch nicht hinlänglich prognostizierbar sind und damit korrespondierende Zwecke nicht vollumfänglich antizipiert werden können. Daher sind die üblicherweise an eine Einwilligung zu stellenden Anforderungen im Zusammenhang mit der Schaffung von KI-Applikationen weiter auszulegen, um unternehmerische Interessen hinreichend zu berücksichtigen. Eine überzogen formalistische Interpretation würde an dieser Stelle ansonsten die Entwicklung von KI, die anfängliche Erwartungen übersteigt, unnötig erschweren. Dafür spricht auch, dass weder die DS-GVO noch die Art.-29-Datenschutzgruppe bei der Formulierung von an die Einwilligung zu stellenden Anforderungen die speziellen Erfordernisse von KI adressiert haben.

Auch im Zusammenhang mit dem konkreten Einsatz von KI ist die Einholung einer Einwilligung problematisch, wenn die KI nicht textbasiert arbeitet. Dies gilt insbesondere für den Fall digitaler Sprachassistenten.

Beispiel

Verarbeitet der digitale Sprachassistent besondere Kategorien personenbezogener Daten eines Nutzers, ist dessen Einwilligung gem. Art. 9 Abs. 2 lit. b DS-GVO mangels anderer Alternativen zwingend. Insbesondere sind Vertragszwecke und „berechtigte Interessen“ in Art. 9 Abs. 2 DS-GVO nicht als Ausnahmen vorgesehen. Recherchiert der Nutzer also etwa nach der Diagnose zu seinem individuellen Krankheitsverlauf oder gibt in der Interaktion mit dem Sprachassistenten seine politischen Meinungen preis, wäre streng genommen eine Einwilligung erforderlich. Der Sprachbefehl als solcher, der oft lediglich in der Nennung eines Aktivierungswortes besteht (z. B. „Alexa“ für Amazon Echo), genügt nicht den Anforderungen des EDSA an eine wirksame Einwilligung.

Es ist demnach in diesem Kontext zwingend eine weite Auslegung der Minimalanforderungen geboten, die eine wirksame Einwilligung erfüllen muss. Dies gilt insbesondere vor dem Hintergrund, dass es sich bei digitalen (Sprach-)assistenten um ein weitgehend akzeptiertes Geschäftsmodell handelt, das insbesondere durch Nutzerfreundlichkeit gekennzeichnet ist. Es sind hier zwar durchaus Wege denkbar, eine formal korrekte Einwilligung einzuholen (z. B. durch Anklicken einer Checkbox mit einem wirksamen Einwilligungstext, bevor der Assistent aktiviert werden kann, oder durch das Vorlesen eines Einwilligungstextes, den der Nutzer etwa durch das Aktivierungswort „Ja“ akzeptieren muss. All dies liefe jedoch den Kundenanforderungen an eine zügige Durchführung der gestellten Anfrage zuwider. ◀

2.8.2 Vertragserfüllung

Gem. Art. 6 Abs. 1 S. 1 lit. b DS-GVO ist eine Verarbeitung personenbezogener Daten zulässig, wenn diese für die Erfüllung eines Vertrags, dessen Vertragspartei der Betroffene ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Gelingt es, den Datenverarbeitungsprozess auf diese Zwecke zu stützen, ist dies für den Verantwortlichen die praktikabelste Variante. In dieser Konstellation ist weder eine jederzeit widerrufliche Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO erforderlich noch muss der Datenverarbeitungsvorgang auf „berechtigte Interessen" gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO gestützt werden. Diese setzen voraus, dass „Interessen oder Grundrechte und Grundfreiheiten" der Betroffenen nicht überwiegen, und erfordern daher eine entsprechende Abwägung. Im Regelfall besteht daher unternehmensseitig der Wunsch, die Verarbeitung personenbezogener Daten soweit wie möglich auf Art. 6 Abs. 1 S. 1 lit. b DS-GVO zu stützen. Dies ist im KI-Kontext vor allem dann möglich, wenn das KI-System auf eine bestimmte Funktion ausgerichtet ist, die einen Kommunikationsaustausch im Vorfeld eines Vertragsschlusses oder einen Vertragsschluss selbst zum Gegenstand hat.

Chatbots

Die regelmäßig rein textbasierten Chatbots übernehmen typischerweise bestimmte Funktionen. Wie dargestellt, handelt sich dabei um sog. KI im engeren Sinne, die keine autonomen Entscheidungen trifft und überwiegend im Customer Support und Customer Service eingesetzt wird, um wiederkehrende Fragen von Nutzern zu Produkt- und Dienstleistungsangeboten des Unternehmens automatisiert beantworten zu können und Verträge abzuwickeln.

Unter Berücksichtigung des gegenwärtigen Standes der Technik ist es daher gerechtfertigt, die Kommunikation des Chatbot unter die Erfüllung vertraglicher Zwecke gem. Art. 6 Abs 1 lit. b DS-GVO zu subsumieren, solange mit dem Einsatz des Chatbot tatsächlich nur der Bereich des „Customer Support", d. h. die (schnellere) Abwicklung von Kunden- bzw. Interessentenanfragen, abgedeckt werden soll und keine darüber hinausgehenden Zwecke verfolgt werden. ◀

Klartextanalyse

Wenn darüber hinaus weitere Zwecke ermöglicht werden sollen, z. B. die Analyse des Klartexts zur Verbesserung des Chatbot, kommen insoweit „berechtigte" wirtschaftliche Interessen gem. Art. 6 Abs. 1 lit. f DS-GVO des Unternehmens in Betracht, solange nicht die Interessen der betroffenen Kunden oder Interessenten überwiegen. Im Hinblick darauf, dass die Klartext-Analyse vor allem zur Verbesserung der Customer-Convenience im Rahmen der Chatbot-Nutzung beitragen soll, die gerade auch (potenziellen) Kunden zu Gute kommt, ist hier ein Überwiegen der Betroffeneninteressen nicht ersichtlich.

Dies gilt vor allem deshalb, weil die Nutzung des Chatbot regelmäßig produkt- und dienstleistungsbezogen erfolgen wird und daher kein besonders schützenswertes Interesse auf Nutzerseite erkennbar ist. Solange Datenschutzbehörden noch nichts Gegenteiliges haben verlauten lassen, ist daher eine Interessenabwägung zugunsten des Unternehmens unter Inkaufnahme eines gewissen Risikos, dass Behörden zu einem anderen Ergebnis gelangen, gut begründbar. ◀

Sprachassistenten

Auch die Interaktion zwischen Sprachassistenten und Nutzern lässt sich unter den Tatbestand des Art. 6 Abs. 1 S. 1 lit. b DS-GVO subsumieren, wenn man dafür die vertragsgemäße Bereitstellung des digitalen Assistenten ausreichen lässt. Eine solch extensive Auslegung des Zweckbindungsgrundsatzes erscheint aufgrund der vielfältigen Möglichkeiten von Nutzer-Anfragen bei der Verwendung digitaler Assistenten auch geboten. Diese reichen von bloßen Eingaben zu Recherchezwecken über konkrete Bestellungen beim Anbieter bis hin zur Vermittlung anderer Dienstleister und deren Angebots- und Produktpalette. Andernfalls wäre der Anbieter gezwungen, vor jedem Sprachbefehl die Einwilligung des Nutzers gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO einzuholen, wenn er die Rechtsunsicherheiten vermeiden möchte, die die Verarbeitung auf Grundlage berechtigter Interessen gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO aufgrund der jederzeitigen Widerspruchsmöglichkeit des Nutzers gem. Art. 21 Abs. 1 S. 1 DS-GVO mit sich bringt.

Die Einholung einer Einwilligung ist jedoch weder für den Nutzer noch für den Anbieter praktikabel. Eine solche würde die Durchführung des Sprachbefehls erkennbar verzögern und daher der von Kunden erwarteten Nutzerfreundlichkeit und damit seinem Interesse insgesamt zuwiderlaufen. Eine Verarbeitung auf Grundlage berechtigter Interessen würde angesichts der damit verbundenen Unsicherheiten das Geschäftsmodell der digitalen Assistenten und die Möglichkeit eines datenschutzkonformen Einsatzes ganz generell in Frage stellen, obschon Sprachassistenten bereits Eingang in den Alltag weiter Teile der Bevölkerung gefunden und als Geschäftsmodell etabliert haben. Daher verdient in diesem Fall die gem. Art. 6 Abs. 1 S. 1 lit. b DS-GVO auf Vertragszwecke bzw. vorvertragliche Maßnahmen abstellende Variante den Vorzug. ◀

2.8.3 Berechtigte Interessen

Wenn eine Rechtfertigung über Art. 6 Abs. 1 S. 1 lit. b DS-GVO zu Vertragszwecken nicht in Betracht kommt, erfolgt nach Möglichkeit ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO. Sofern keine besonderen Kategorien personenbezogener Daten involviert sind, kann danach eine Datenverarbeitung auch auf Grundlage „berechtigter Interessen des Verantwortlichen oder eines Dritten (erfolgen), sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (…)." EG 47 DS-GVO stellt insofern auf die „vernünftigen Erwartungen" der betroffenen Nutzer ab.

Zwar besteht gem. Art. 21 Abs. 1 DS-GVO eine Möglichkeit zum Widerspruch durch den Betroffenen, doch ist auch diese Rechtsgrundlage grundsätzlich attraktiver als eine proaktiv einzuholende Nutzereinwilligung, die im Vorfeld der Datenverarbeitung erteilt werden muss.

In Teilen der Literatur (Drewes 2016, S. 725) wird explizit die Auffassung vertreten, dass Big-Data-Analysen, die das Fundament für die KI-Generierung darstellen, auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO zulässigerweise erfolgen können. EG 47 DS-GVO enthält überdies weitere Beispiele für Datenverarbeitungsszenarien, die über „berechtigte Interessen" gerechtfertigt werden können. Zwar beziehen sich diese nicht explizit auf KI, bilden jedoch häufig den Gegenstand von KI-Anwendungen.

2.8.3.1 Betrugsprävention

Gem. 47 EG handelt es sich dabei zunächst um die Datenverarbeitung zum Zwecke der Betrugsprävention. Eine Rechtfertigung gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist demnach jedenfalls dann möglich, wenn die Datenverarbeitung auf das „für die Verhinderung von Betrug unbedingt erforderliche Maß" beschränkt ist.

Beispiel

KI-basierte **Fraud Detection** wird häufig in der Versicherungs- und Banking-Branche eingesetzt, weil sie regelmäßig effizienter in der Aufdeckung von Betrugsversuchen ist als eine manuell durchgeführte Betrugsprävention. Diese kennzeichnet Transaktionen häufig fälschlicherweise als Betrug und führt zu sog. „False Positives", die auf Seiten des betreffenden Unternehmens zusätzlichen Aufwand erzeugen und daher unnötig Ressourcen binden (vgl. Schonschek 2018). ◄

Für die vorgelagerte Entwicklungsphase eines KI-basierten Betrugspräventionstools dürfte es zunächst kaum möglich sein, die Trainingsdaten auf das zwingend erforderliche Maß zu beschränken, weil deren Bedeutung für die Präzision der über das Tool erzielten Ergebnisse zu diesem Zeitpunkt noch nicht zwangsläufig antizipiert werden kann. Auch hier ist daher eine extensive Auslegung insoweit geboten, als sich das Fraud-Detection-System noch in der Entstehung befindet. Im Rahmen des konkreten Einsatzes des Tools kann dann der Verantwortliche der in EG 47 DS-GVO formulierten Beschränkung der Betrugsprävention durch technisch-organisatorische Maßnahmen nachkommen. Werden z. B. pseudonymisierte Datenbestände von Dritten durchsucht und dem Verantwortlichen lediglich Matches mitgeteilt, handelt es sich um ein minimalinvasives Vorgehen, das auch die Interessen Betroffener hinreichend berücksichtigt.

2.8.3.2 Online-Marketing

Daneben stuft EG 47 grundsätzlich auch die Verarbeitung personenbezogener Daten zum Zwecke der **Direktwerbung** als eine Verarbeitung ein, die berechtigten Interessen dient. Ein berechtigtes Interesse kann demnach auch die Verarbeitung personenbezogener Daten zur Ermittlung der geeigneten Zielgruppe(n) für die beabsichtigte Werbemaßnahme sein

(Drewes 2016, S. 725). Nach Teilen der Literatur bedarf es jedoch jeweils einer Betrachtung des Einzelfalls (Schulz 2018 Rn. 90). So seien gerade in den Bereichen des **Cross-Device-Tracking** und **Online Behavioural Targeting**, bei denen es sich um Vorstufen der Direktwerbung handelt (Gausling 2019b, S. 339), u. a. die betroffenen Datenarten, Belästigungspotenzial sowie das Informations- und Widerspruchsmanagement im Rahmen der Abwägung zu berücksichtigen (Schulz 2018, Rn. 90; a. A. Schirmbacher 2016, S. 278, der Maßnahmen wie das Cross-Device-Tracking nicht mehr von den Nutzererwartungen gedeckt sieht).

Dass im Online-Marketing eine Verarbeitung personenbezogener Daten auf Grundlage berechtigter Interessen grundsätzlich möglich ist, entspricht auch der in der „Orientierungshilfe für Anbieter von Telemedien“ (DSK 2019a, S. 16) von den deutschen Datenschutzbehörden dargelegten Rechtsauffassung.[20] Dies erfordere allerdings „substantielle Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Beteiligten“ und müsse „auf den konkreten Einzelfall bezogen sein“. Im Rahmen der Interessenabwägung seien konkrete Kriterien heranzuziehen, u. a. die vernünftige Erwartung der betroffenen Personen sowie deren Interventionsmöglichkeiten, die Verkettung von Daten, beteiligte Akteure, die Dauer der Beobachtung, den Kreis der Betroffenen, Datenkategorien sowie der Umfang der Datenverarbeitung. Die DSK geht dabei jedenfalls dann von einem Überwiegen der Interessen des Betroffenen aus, wenn es sich um Maßnahmen mit einer gewissen Eingriffsintensität handelt, wie etwa „automatisierten Selektionsverfahren zur Erstellung detaillierter Profile, Verhaltensprognosen bzw. Analysen, die zu zusätzlichen Erkenntnissen führen“ (DSK 2018d, S. 5).

- Auch wenn EG 47 der DS-GVO die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung auf Grundlage berechtigter Interessen anerkennt und dann erst recht ein im Vorfeld erfolgendes Tracking des Nutzerverhaltens zulässig sein müsste, ist im Hinblick auf eindeutige Stellungnahmen der Datenschutzbehörden für Tracking eine detaillierte Analyse des Einzelfalls unter Berücksichtigung der von der DSK genannten Kriterien erforderlich. Je eingriffsintensiver demnach das – KI-gestützte – Tracking ausgestaltet ist, desto näher liegt das Erfordernis einer Einwilligung.

2.9 Datenschutzfolgenabschätzung

Auch die Anforderungen der Datenschutzfolgenabschätzung (**DSFA**) sind bereits vor der Implementierung algorithmenbasierter Systeme (Krempl 2018), d. h. noch im Stadium der KI-Generierung zu beachten.

[20] Anders noch DSK in ihrer Positionsbestimmung zur „Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“, die von einem strikten Einwilligungserfordernis für die Erstellung von pseudonymen Nutzungsprofilen zu Werbezwecken ausging.

Nach Art. 35 Abs. 1 DS-GVO muss der Verantwortliche „eine Abschätzung der Folgen" der beabsichtigten Verarbeitungsvorgänge „für den Schutz personenbezogener Daten" dann durchführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat."[21] Im Rahmen der DSFA sind insbesondere Abhilfemaßnahmen zu beleuchten, durch die der Schutz personenbezogener Daten sichergestellt wird (vgl. Art. 35 Abs. 7 lit. d DS-GVO). Dabei handelt es sich um einen mitunter zeitaufwändigen Vorgang, der jedoch in bestimmten Fällen zwingend durchzuführen ist, um ein Bußgeld gem. Art. 83 Abs. 4 lit. a DS-GVO zu vermeiden.

Angezeigt ist eine DSFA gem. Art. 35 Abs. 3 lit. a DS-GVO insbesondere bei „systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen." Entsprechend sieht auch die DSK in ihrer auf Grundlage von Art. 35 Abs. 4 DS-GVO ausgegebenen Muss-Liste die Notwendigkeit einer Datenschutzfolgenabschätzung vor allem in Fällen vor, in denen eine umfangreiche Verarbeitung zwecks Bewertung verhaltensbasierter Daten stattfindet (z. B. Einsatz von **Data-Loss-Prevention-Tools,** um unerwünschtes Verhalten von Mitarbeitern zu erkennen),[22] umfassende Profile erstellt werden (z. B. zum Betrieb von Kontaktportalen[23] oder zur Erfassung des Kaufverhaltens zwecks Kundenbindung)[24] oder eine Bewertung persönlicher Aspekte erfolgt (z. B. Auswertungen von Telefongesprächen durch ein Callcenter zwecks Ermittlung der Stimmungslage).[25]

Eine DSFA ist laut DSK überdies im Falle umfangreicher Algorithmen-basierter Verarbeitungen von personenbezogenen Daten erforderlich, wenn diese aus unterschiedlichen Quellen zusammengeführt werden und (1) entweder rechtserheblichen Entscheidungen oder ähnlich erheblich beeinträchtigenden Maßnahmen zugrunde liegen[26] oder (2) der Entdeckung unbekannte Muster für noch unbekannte Zwecke dienen.[27]

Diese genannten Fallgruppen beschreiben den wesentlichen Kern vieler KI-Anwendungen, die Eingang in Entscheidungsprozesse in Unternehmen gefunden haben, auch wenn sich nicht alle explizit auf Künstliche Intelligenz und dieser zugrunde liegende Algorithmen beziehen. Vor diesem Hintergrund wird der Einsatz künstlicher Intelligenz re-

[21] Ähnlich § 67 Abs. 1 BDSG.

[22] DSK 2018c, Fallgruppe 8.

[23] DSK 2018c, Fallgruppe 9.

[24] DSK 2018c, Fallgruppe 14.

[25] DSK 2018c, Fallgruppen 11 und 13.

[26] DSK 2018c, Fallgruppe 5.

[27] DSK 2018c, Fallgruppe 10.

gelmäßig eine DSFA erfordern. Dabei ist zu beachten, dass eine DSFA ggfs. nicht nur einmal erfolgt, sondern in Abhängigkeit von der Dynamik der Verarbeitungsprozesse möglicherweise einen „fortlaufenden Prozess" darstellt (Art.-29-Datenschutzgruppe 2017, S. 17). Damit gilt insbesondere für die Weiterentwicklung KI-basierter Technologien, dass diese regelmäßig erneut auf den Prüfstand gestellt werden müssen.

2.10 Datenschutzrechtliche Grundprinzipien und korrespondierende Informationspflichten gem. Art. 13, 14 DS-GVO

Werden zur Herstellung oder beim Einsatz der KI im Unternehmen, sei es im Rahmen der Bewerberselektion oder im Bereich des Customer Service, personenbezogene Daten verarbeitet, trifft den Verantwortlichen die Pflicht, dem Betroffenen die Informationen gem. Art. 13 oder Art. 14 DS-GVO bereitzustellen. Welche der beiden Normen einschlägig ist, richtet sich danach, ob die Datenerhebung direkt beim Betroffenen (Art. 13 DS-GVO) oder durch andere Quellen erfolgt (Art. 14 DS-GVO).[28] Die Informationspflichten sind dabei Ausfluss der die DS-GVO durchdringenden datenschutzrechtlichen Grundprinzipien, die ihrerseits in Art. 5 DS-GVO verankert sind und anhand derer die korrespondierenden Informationspflichten im Folgenden dargestellt werden sollen.

Die Grundprinzipien der DS-GVO und die damit korrespondierenden Informationspflichten bilden zunächst einen diametralen Gegensatz zu den Anforderungen an die Schaffung einer qualitativ hochwertigen KI. Wie dargestellt, setzt diese jedenfalls gegenwärtig regelmäßig einen großen Pool personenbezogener Daten voraus, befinden sich doch entsprechende Anonymisierungsmethoden erst in der Entwicklung. In der DS-GVO hingegen sind die strikte Zweckgebundenheit der Verarbeitungstätigkeit (Art. 5 Abs. 1 lit. b DS-GVO) und deren Beschränkung auf das „notwendige Maß" (Art. 5 Abs. 1 lit. c DS-GVO) als zentrale Leitkriterien fest verankert. Solange daher keine konkreten gesetzlichen Leitlinien für die Verarbeitung personenbezogener Daten zur KI-Entwicklung geschaffen worden sind, muss das verantwortliche Unternehmen die gegensätzlichen Anforderungen bestmöglich in Einklang bringen.

2.10.1 Transparenz

Gem. Art. 5 Abs. 1 lit. a DS-GVO müssen die personenbezogenen Daten in einer für den Betroffenen nachvollziehbaren Weise, d. h. transparent, verarbeitet werden.

[28] Da es sich um im Wesentlichen inhaltsgleiche Vorschriften handelt, soll nachfolgend lediglich auf Art. 13 DS-GVO eingegangen werden.

2.10.1.1 Darstellung von Informationen

Dieses Transparenzerfordernis spiegelt sich in Art. 12 DS-GVO wider, wonach der Verantwortliche die in Art. 13 dargestellten und zum Zeitpunkt der Datenerhebung zur Verfügung zu stellenden Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" bereitstellen muss. Eine solche Darstellung ist auch im Bereich KI unproblematisch möglich, solange eine Belehrung textbasiert erfolgen kann.

Beispiel

Betreibt ein Unternehmen einen Chatbot zum Zwecke des Kundenservice, sollten die Datenschutzbestimmungen bereits zu Beginn des Chats z. B. via Link verfügbar gemacht werden. Die Datenschutzbestimmungen wiederum sollten den Einsatz des Chatbot konkret erwähnen. Werden die Chatbot-Funktionen erst nach dem Download einer App bereitgestellt, muss dem Nutzer die Datenschutzerklärung schon vor der Installation der App zur Verfügung gestellt werden (für über den Apple App Store verfügbare iOS-Apps etwa durch Verlinkung auf eine App-spezifische Datenschutzerklärung unter dem Punkt „Datenschutz" in der App-Beschreibung). ◀

Sofern eine Textdarstellung im Rahmen der KI-Anwendung möglich ist, ist angesichts oftmals überfrachteter und daher vom Nutzer regelmäßig nur ausschnittsweise gelesener Datenschutzerklärungen (vgl. Strassemeyer 2020, S. 176) auch eine Darstellung über **Piktogramme** denkbar. Art. 12 Abs. 7 DS-GVO, wonach Informationen gem. Art. 13, 14 DS-GVO „in Kombination mit standardisierten Bildsymbolen bereitgestellt werden können", sieht diese Möglichkeit explizit vor. Die Europäische Kommission, die in Art. 12 Abs. 8 DS-GVO zum Erlass gem. Art. 92 DS-GVO delegierter Rechtsakte zur Bestimmung der durch Bildsymbole darzustellenden Informationen und Standardisierung dieser Bildsymbole ermächtigt wird, hat davon bisher allerdings keinen Gebrauch gemacht. Überdies sieht Art. 12 Abs. 7 DS-GVO auch lediglich eine „Kombination" von schriftlichen bzw. elektronischen Informationen mit „standardisierten Bildsymbolen" vor.

Anders als im Falle von Webseiten oder Apps wird eine klassische Display-Darstellung bei vielen KI-Anwendungen, z. B. Sprachassistenten oder IoT-Geräten, regelmäßig allerdings ohnehin nicht in der KI-Anwendung selbst möglich sein (Conrad 2019, S. 403). Auch eine grundsätzlich begrüßenswerte Darstellung über Bildsymbole hälfe an dieser Stelle nicht weiter. Die Art.-29-Datenschutzgruppe führt in ihrer vom EDSA ebenfalls übernommenen Stellungnahme zur Transparenz (Art.-29-Datenschutzgruppe 2018b, S. 26) Bildsymbole zwar als Möglichkeit zur Informationsbereitstellung auch für „bildschirmlose intelligente Technologie" und IoT-Umgebungen auf, erklärt jedoch nicht, wie dies ohne vorhandenes Display praktisch umsetzbar sein soll. Nach Auffassung der Art.-29-Datenschutzgruppe können jedoch auch „Sprachmeldungen, schriftliche Angaben in papiergestützten Installationsanweisungen und Videos in digitalen Installationsanwei-

sungen“ ein geeignetes Format für die Informationsübermittlung darstellen. Soweit das Unternehmen eine Online-Präsenz unterhält, gilt dies allerdings nur zusätzlich zu einer über die Online-Präsenz einzusehenden Datenschutzerklärung. Wichtig sei dabei, dass „die wichtigsten Informationen[29] stets über die erste für die Kommunikation mit der betroffenen Person verwendete Modalität bereitgestellt“ würden.

- Im Falle von IoT-Geräten oder digitalen Assistenten sollte das verantwortliche Unternehmen seinen Informationspflichten in der zugehörigen Installationsanleitung und ggfs. zusätzlich über seine Online-Präsenz nachkommen. Im Falle von Sprachassistenten kann zusätzlich die Möglichkeit einer Sprachmeldung eingebaut werden, die bei Abruf des Nutzers die relevanten Informationen vorliest.[30]

2.10.1.2 Betroffenenrechte

Auch die sog. Betroffenenrechte gem. Art. 15 ff. DS-GVO sind Ausfluss des in Art. 5 Abs. 1 lit. a DS-GVO verankerten Transparenzgebots. Entsprechende Informationspflichten sind in Art. 13 Abs. 2 lit. b-d enthalten. Während die Darstellung dieser Betroffenenrechte auch im Rahmen von KI-Anwendungen unkompliziert möglich ist, stellt vielmehr die Umsetzung entsprechender Ersuchen das verantwortliche Unternehmen vor Herausforderungen (dazu Abschn. 2.11).

Art. 22 Abs. 1 DS-GVO gehört systematisch ebenfalls zu den Betroffenenrechten. In informatischer Hinsicht verlangt Art. 13 Abs. 2 lit. f DS-GVO für die darin geregelte Entscheidungsfindung einschließlich Profiling „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“[31] (dazu Abschn. 2.12.6).

2.10.2 Rechtmäßigkeit der Datenverarbeitung

Personenbezogene Daten müssen auf rechtmäßige Weise verarbeitet werden (vgl. Art. 5 Abs. 1 lit. a DS-GVO). Dem Betroffenen muss daher gem. Art. 13 Abs. 1 lit. c DS-GVO die Rechtsgrundlage der Datenverarbeitung in der Datenschutzerklärung mitgeteilt werden. Es gilt insofern die Darstellung unter Abschn. 2.8.

---

[29] Dies sind laut Art.-29-Datenschutzgruppe (2018b, S. 24) „die Einzelheiten zu den Verarbeitungszwecken, die Identität des Verantwortlichen und die Existenz der Rechte der betroffenen Person – zusammen mit Informationen über die wichtigsten Auswirkungen der Verarbeitung bzw. Verarbeitungsvorgänge, mit denen die betroffene Person möglicherweise nicht rechnet.“

[30] Auf diese Weise wird dann auch ein Medienbruch vermieden (Conrad DSRITB 2019, S. 403).

[31] Vgl. ferner EG 63 S. 3 DS-GVO.

2.10.3 Empfänger und Übermittlung in Drittländer

Auch die Übermittlung an Dritte bedarf einer hinreichenden Rechtsgrundlage. Entsprechend verpflichtet Art. 13 Abs. 1 lit. e DS-GVO Betroffene auch über Empfänger oder Kategorien von Empfängern der personenbezogenen Daten zu informieren. Gleiches gilt gem. Art. 13 Abs. 1 lit. f DS-GVO für die geplante Übermittlung in ein Drittland. Eine namentliche Benennung des jeweiligen Empfängers ist dabei nicht zwingend. Erforderlich ist lediglich die Darstellung des Tätigkeitsbereichs, Sektors sowie Standorts der Empfänger (DSK 2018a, S. 32 f.). Doch auch diese Angaben sind beim Einsatz von KI nicht immer realisierbar. In diesem Fall ist dann eine weite Auslegung der an die Beschreibung der Empfänger bzw. Kategorien von Empfängern zu stellenden Anforderungen geboten, die sich eng an den Informationen orientiert, deren Darstellung in den Möglichkeiten des Verantwortlichen liegt.

Beispiel

Erhält der digitale Sprachassistent von seinem Nutzer Anweisungen, eine Bestellung aufzugeben bzw. eine Dienstleistung in Auftrag zu geben, ist an dieser Stelle zwar regelmäßig der Sektor (z. B. Dienstleistungssektor) und der Tätigkeitsbereich (z. B. Beratungsleistungen) im Vorhinein antizipierbar und kann daher zumindest in der Regel über die Datenschutzerklärung abgedeckt werden. Doch trifft dies nicht auf die jeweilige Standortangabe des Empfängers zu, hängt diese doch von den konkreten Bedürfnissen des Nutzers ab, die dieser erst in seinem Sprachbefehl artikuliert. Entsprechend kann eine Standortbeschreibung nicht vorab in die Datenschutzerklärung aufgenommen werden. ◀

2.10.4 Zweckbindung

Kernprinzip der DS-GVO ist der in Art. 5 Abs. 1 lit. b DSD-GVO verankerte Zweckbindungsgrundsatz. Danach dürfen personenbezogene Daten nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden“ und nicht „in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“. Entsprechend muss das verantwortliche Unternehmen auch in der Datenschutzerklärung über diesen Zweck gem. Art. 13 Abs. 1 lit. c DS-GVO informieren.

2.10.4.1 Zweckdarstellung

Die Darstellung des Zwecks gestaltet sich im Kontext der Generierung von KI als schwierig. Big-Data-Analysen stellen regelmäßig die Grundlage für KI-Entwicklungen dar. Allerdings zeichnen sie sich dadurch aus, dass ein konkreter Verarbeitungszweck im Hinblick auf die genutzten Trainingsdaten im Vorhinein gerade nicht benannt werden kann, sondern die Auswertungen regelmäßig der Identifikation unbekannter Muster dienen (Bit-

kom e.V 2017, S. 135). Dementsprechend ist eine Detailbeschreibung des verfolgten Zwecks im Einklang mit dem datenschutzrechtlichen Zweckbindungsgrundsatz und den Anforderungen der Art.-29-Datenschutzgruppe an eine granulare Zweckdarstellung (vgl. Art.-29-Datenschutzgruppe 2018c, S. 11) de facto nicht möglich. Wie bereits im Zusammenhang mit der Einwilligung dargestellt (vgl. Abschn. 2.8.1) und gerade in Ermangelung konkreter gesetzlicher Vorgaben an die KI-Entwicklung, müssen die Anforderungen an die Zweckdarstellung daher im Zusammenhang mit KI flexibler ausgelegt werden, d. h. ist eine extensive Auslegung des Zweckbindungsgrundsatzes geboten (Bitkom 2017, S. 135), die sowohl die unternehmerischen Interessen an der KI-Entwicklung und die Interessen Betroffener in Ausgleich bringt. Entsprechend schlagen einige Industrieverbände vor, für Big-Data-Anwendungen in der Forschung den Zweckbindungsgrundsatz aufzuheben (vgl. hierzu Borchers 2018).

Auch beim konkreten Einsatz von KI erscheint eine weite Auslegung des Zweckbindungsgrundsatzes geboten.

Beispiel

Während es etwa beim Einsatz von Chatbots aufgrund deren eingeschränkter Funktionalität nach gegenwärtigem Stand der Technik möglich ist, im Rahmen der Datenschutzerklärung auf den Zweck des Customer Service zu verweisen, stellt sich dies im Bereich digitaler Assistenten differenzierter dar. Hier sind vielfältige Sprachbefehle möglich. So können Dienstleistungen in Auftrag gegeben, Produkte geordert, bloße Suchanfragen eingegeben oder geräteübergreifende Vernetzungen ausgelöst werden, die vom Anbieter nicht in ihren Einzelheiten vorhergesehen und entsprechend kategorisiert werden können. Auch hier muss demnach bei der Zweckbeschreibung innerhalb der Datenschutzbestimmungen genügen, wenn auf eine „Datenverarbeitung zur Ausführung der vom Nutzer eingegebenen Sprachbefehle“ verwiesen wird. ◀

2.10.4.2 Zweckänderung

Selbst wenn im Rahmen der KI-Entwicklung ursprünglich ein Zweck konkret definiert wurde, können im Rahmen des ML-Prozesses neue Muster erkannt werden, die eine Änderung des ursprünglichen Zwecks nahelegen. Eine solche Zweckänderung ist gem. Art. 6 Abs. 4 DS-GVO nur unter engen Voraussetzungen möglich.

Die Einholung einer Einwilligung, die Art. 6 Abs. 4 DS-GVO als Basis für eine Zweckänderung anerkennt, wird in der Regel nicht praktikabel sein, weil personenbezogene Daten als Trainingsgrundlage für die KI-Entwicklung regelmäßig aus vielfältigen Quellen zusammengeführt werden. Die ebenfalls zulässige Zweckänderung aufgrund einer nationalen oder EU-Rechtsvorschrift, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Absatz 1 DS-GVO genannten Ziele darstellt, wird ebenfalls regelmäßig nicht in Betracht kommen.

Damit wird gem. Art. 6 Abs. 4 DS-GVO eine Zweckänderung in den überwiegenden Fällen in der Praxis nur zulässig sein, wenn der ursprüngliche Zweck der Datenverarbei-

tung mit dem Zweck der Weiterverarbeitung kompatibel, d. h. „logischer nächster Schritt“ ist (Buchner und Petri 2018, Art. 6, Rn. 187). Um dies festzustellen, muss der Verantwortliche ausweislich Art. 6 Abs. 4 DS-GV die folgenden Punkte berücksichtigen: (a) eine Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung, (2) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen, (3) die Art der personenbezogenen Daten, u. a. ob besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 verarbeitet werden, (4) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen sowie (5) dass Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können. Eine Weiterverarbeitung auf Basis von Art. 6 Abs. 4 DS-GVO wird sich also primär daran messen lassen müssen, ob eine Verbindung zwischen ursprünglichem und neuem Zweck hergestellt werden dann.

- Vor der Entwicklung der KI sollten potenzielle Zwecke in den Datenschutzbestimmungen so detailliert wie zu diesem Zeitpunkt möglich beschrieben werden. Es sollten dabei Fallgruppen (sog. „use cases“) gebildet werden, anhand derer es später leichter fällt, die ursprünglich antizipierten Zwecke mit den schließlich konkreten Zwecken der Weiterverarbeitung in Verbindung zu bringen.

Um den Besonderheiten KI-basierter Dienste gerecht zu werden, sollte Art. 6 Abs. 4 DS-GVO daher als eine Art „Öffnungsklausel für ‚verwandte‘ Zwecke der Weiterverarbeitung“ im Bereich Künstlicher Intelligenz verstanden werden (in diese Richtung argumentierend Wilmer 2018, Rn. 39).

2.10.5 Datenminimierung und Speicherbegrenzung

Art. 5 Abs. 1 lit. c DS-GVO enthält den Grundsatz der Datenminimierung. Danach muss die Datenverarbeitung „auf das für die Datenverarbeitung notwendige Maß beschränkt sein.“ Art. 5 Abs. 1 lit. e DS-GVO setzt das Erfordernis der Datenminimierung in zeitlicher Hinsicht über das Prinzip der Speicherbegrenzung fort. Danach müssen personenbezogene Daten „in einer Form gespeichert werden, die eine Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die (Verarbeitungszwecke) erforderlich ist.“

Sofern keine gesetzlichen Aufbewahrungsfristen den Verantwortlichen zu einer weitergehenden Speicherung verpflichten (z. B. gem. § 147 Abs. 1 AO oder § 257 Abs. 1 HGB) oder die für eine Zweckänderung gem. Art. 6 Abs. 4 DS-GVO erforderlichen Voraussetzungen vorliegen, müssen die betroffenen Daten danach grundsätzlich gelöscht werden. Entsprechend müssen Betroffene gem. Art. 13 Abs. 2 lit. a DS-GVO über die geplante Speicherdauer oder jedenfalls die Kriterien für deren Festlegung informiert werden. Ano-

nymisierungstechniken auch im Zusammenhang mit der Schaffung von KI befinden sich derzeit in der Entwicklung. Dabei handelt es sich insbesondere um die oben dargestellten Verfahren zur Synthetisierung von Daten oder Herstellung künstlicher Szenarien im Rahmen von GANs, die als Trainingsgrundlage für die weitere KI-Entwicklung dienen können.

2.11 Betroffenenrechte

Ein Unternehmen muss im Zusammenhang mit den von ihm betriebenen KI-Systemen ein Management vorhalten, das Betroffenen die Möglichkeit zur Wahrnehmung ihrer Rechte gem. Art. 15 ff. DS-GVO ermöglicht. In der Praxis sind vor allem der Auskunftsanspruch gem. Art. 15 sowie der Anspruch auf Löschung gem. Art. 17 DS-GVO relevant.

2.11.1 Auskunftsanspruch

Macht der Betroffene seinen Auskunftsanspruch geltend, muss der Verantwortliche diesen gem. Art. 15 Abs. 1 DS-GVO über die von ihm verarbeiteten Daten sowie die wesentlichen der auch gem. Art. 13 DS-GVO mitzuteilenden Informationen unterrichten, d. h. u. a. Verarbeitungszwecke, Empfänger und Speicherdauer. Damit spiegelt der Auskunftsanspruch die Informationen, über die ein Unternehmen den Nutzer bereits vorab in seinen Datenschutzbestimmungen informieren muss. Auch hier gilt daher die Notwendigkeit eines flexiblen Verständnisses der Reichweite von Informationspflichten, um unternehmerische Interessen an der KI-Generierung auf Basis umfangreicher Datenpools mit dem datenschutzrechtlichen Transparenzprinzip in Einklang zu bringen. Dies gilt insbesondere auch für Auskünfte über „aussagekräftige Informationen über die involvierte Logik“ im Falle automatisierter Entscheidungsfindungen (Art. 15 Abs. 1 lit. h DS-GVO) (Abschn. 2.12).

2.11.2 Recht auf Löschung

Art. 17 Abs. 1 DS-GVO enthält die Fälle, in denen Betroffene die Löschung der von ihnen verarbeiteten Daten verlangen können. Dies betrifft etwa den Widerruf der Einwilligung durch den Betroffenen (Art. 17 Abs. 1 lit. b DS-GVO), den Widerspruch gegen die Verarbeitung auf Grundlage berechtigter Interessen (Art. 17 Abs. 1 lit. c DS-GVO) oder das Entfallen der Notwendigkeit der Datenverarbeitung für den ursprünglichen Zweck (Art. 17 Abs. 1 lit. a DS-GVO).

Es stellt sich die Frage, wie in diesem Kontext mit dem Umstand umzugehen ist, dass durch selbstlernende Algorithmen weiterverarbeitete personenbezogene Daten nicht mit Wirkung für die Zukunft gelöscht werden können, sondern der daraus resultierende Erkenntnisgewinn auf Grund des Black-Box-Prinzips irreversibel zum Gegenstand des Al-

gorithmus geworden ist. Eine Löschung, wie Art. 17 DS-GVO sie vorsieht, kann somit nicht erfolgen. Mit Blick darauf, dass die DS-GVO KI-Technologien an keiner Stelle explizit erwähnt und deren Besonderheiten dort keinen Niederschlag gefunden haben, bedarf es daher einer restriktiven Auslegung der Rechtsfolge des Art. 17 Abs. 1 DS-GO dahingehend, dass eine Löschung nur im Rahmen des faktisch Machbaren erfolgen kann.

Somit kann für den Fall, dass die weitere Datenverarbeitung nicht mehr notwendig ist oder ein Widerruf bzw. Widerspruch erfolgt, die in Art. 17 Abs. 1 DS-GVO vorgesehene Rechtsfolge der Löschung nur dahingehend verstanden werden, dass im Rahmen der KI-Entwicklung eine weitere Nutzung der auf den Betroffenen zurückzuführenden Trainingsdaten für die Zukunft nicht gestattet ist, die weitere Entwicklung der darauf basierenden Algorithmen jedoch möglich bleibt.[32] Eine solche Auslegung ist auch interessengerecht, da Unternehmen ansonsten das Risiko für in der DS-GVO manifestierte Versäumnisse im Hinblick auf neue Technologien tragen müssten und der Fortschritt in der KI-Entwicklung unnötig behindert würde.

2.12 Automatisierte Entscheidungen gem. Art. 22 DS-GVO

Automatisierte Entscheidungsprozesse (**Algorithmic Decision Making**, **ADM-Verfahren**) stellen für Unternehmen eine Möglichkeit dar, um standardisierte Prozesse effizient zu gestalten (z. B. im Rahmen von Recruiting-Prozessen). Automatisierte Entscheidungen oder Profiling durch KI-Systeme sind jedoch gem. Art. 22 Abs. 1 DS-GVO in der Regel unzulässig, wenn die betroffene Person dadurch einer Entscheidung unterworfen wird, die „ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt". Eine finale Entscheidung soll danach grundsätzlich nicht durch das KI-System ausgegeben werden, sondern immer unter dem Vorbehalt einer menschlichen Intervention stehen.

2.12.1 Ausnahmen vom Verbot

Ausnahmen gelten lediglich insoweit, als die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist (Art. 22 Abs. 2 lit. a DS-GVO), mit ausdrücklicher Einwilligung des Betroffenen erfolgt (Art. 22 Abs. 2 lit. c DS-GVO) oder die in § 37 Abs. 1 BSDG genannten Fällen betrifft (z. B. wenn die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht und dem Begehren der betroffenen Person stattgegeben wurde, vgl. § 37 Abs. 1 Nr. 1 BDSG).

[32] Vgl. zu diesem Themenkomplex auch Conrad (2019, S. 401), wonach jedoch eine solche Auslegung „nicht zur endlosen Datenverarbeitung führen und damit dieses Betroffenenrecht aushöhlen" dürfe.

2.12.2 Menschliche Intervention und „Computer says no"-Problem

Hat ein automatisiertes Entscheidungssystem entweder rechtliche Wirkung oder beeinträchtigt es den Betroffenen in ähnlich erheblicher Weise (dazu Abschn. 2.12.5), muss gem. Art. 22 Abs. 1 DS-GVO in jedem Fall eine menschliche Handlung dazwischentreten. Laut Art.-29-Datenschutzgruppe muss der Verantwortliche sicherstellen, dass die Entscheidung „einer echten Aufsicht unterliegt" und der Entscheidungsträger „zur Änderung derselben befugt und befähigt ist" (Art.-29-Datenschutzgruppe, S. 22). Die Einbeziehung einer Person darf also nicht nur Symbolcharakter haben (Art.-29-Datenschutzgruppe, S. 22). Art. 22 DS-GVO liegt die Vorstellung zugrunde, dass es sich bei dem Menschen um eine diskriminierungsfreie Instanz handelt, die die Ergebnisse der KI entsprechend korrigieren kann. Es bleibt die Frage, ob der menschliche Entscheider nicht regelmäßig ohnehin dem vom KI-System ausgegebenen Ergebnis folgen wird und damit den eigentlichen Zweck der Vorschrift konterkariert („**Computer says no**"-Problem, vgl. dazu Zimmer 2019).

2.12.3 Diskriminierung durch Algorithmen und Trainingsgrundlage

Ratio des Art. 22 Abs. 1 DS-GVO ist es, Menschen nicht zum bloßen Objekt künstlicher Intelligenz zu machen, wie es auch die DSK fordert (DSK 2019a, S. 3). Betroffene haben demnach „auch beim Einsatz von KI-Systemen den Anspruch auf das Eingreifen einer Person (**Intervenierbarkeit**), auf die Darlegung ihres Standpunktes und die Anfechtung einer Entscheidung."

Hintergrund dieser Erwägungen ist die Frage, inwieweit diskriminierungsfreies Design von KI derzeit überhaupt möglich ist bzw. in welchem Ausmaß Algorithmen Diskriminierungspotenzial innewohnt. Ein besonderes Augenmerk ist auf die Auswahl der richtigen „Trainingsdaten" zu legen, mit denen die KI trainiert wird. Dies zeigen zahlreiche Fälle aus der Praxis. Diese zeigen, dass die Gründe für eine Diskriminierung entweder in den Daten selbst (vgl. Beispiel zur Recruiting-Software), im Fehlen relevanter Daten, Weglassen sensibler Informationen oder einem dynamischen Weiterlernen (vgl. Chatbot-Beispiel) liegen (vgl. insgesamt dazu Zweig 2019, S. 212 ff.).

Fälle aus der Praxis

1. Chatbots

Ein prominentes Beispiel ist das selbstlernende Chatprogramm Tay, das mittels regulärer Chatverläufe trainiert wurde, die andere mit ihm führten, und auf dieser Basis anstößige und beleidigende Tweets absetzte. Daraufhin wurde es von seinen Entwicklern vom Netz genommen wurde (vgl. dazu Graff 2016). Zwar waren in diesem Fall die Konsequenzen für die Betroffenen nicht entscheidungserheblich. Jedoch mangelt es nicht an Beispielen, in denen automatisierte Entscheidungen durchaus rechtserhebliche Wirkung entfalteten. ◄

2. Recruiting-Software

In einem weiteren bekannten Fall wurde eine Software zur Auswahl von Bewerbern mit Daten trainiert, die auf erfolgreichen Bewerbungen der letzten zehn Jahre basierten. In der Mehrzahl handelte es sich dabei um Bewerbungen männlicher Personen. Obwohl das Trainingsmodell das Geschlecht der Bewerber nicht als Input bekam, fand es Eigenschaften, die mit dem Geschlecht zusammenhingen. Infolgedessen führte die Erwähnung einer Mitgliedschaft im „Frauen-Schach-Club" oder von Frauen-Colleges zu einer negativen Bewertung durch das KI-System.

Im Ergebnis zog die KI den Schluss, dass männliche Bewerber gegenüber weiblichen Kandidatinnen zu bevorzugen seien, und traf eine entsprechende Auswahl. Dieses Beispiel veranschaulicht, welche Auswirkungen die einmal zugrunde gelegte Trainingsbasis haben kann. Überdies zeigt es, dass eine Diskriminierung durch Algorithmen sogar dann möglich ist, wenn eine Kenntnis von der jeweiligen Gruppe, zu der ein Datensatz gehört, nicht besteht (Honey und Stieler 2020, S. 34). ◄

3. Spracherkennungssoftware

Zur Erteilung bestimmter Arbeitsvisa werden in Australien Antragsteller mittels eines Computer-basierten Tests auf ihre Englischkenntnisse getestet. Eine gebürtige Irin erhielt dabei nicht den erforderlichen Score für den mündlichen Teil der Prüfung, dessen Bewertung auf Basis einer Spracherkennungssoftware erfolgte, und infolgedessen auch kein entsprechendes Visum.[33] Hier liegt nahe, dass auf Grundlage einer Spracherkennungssoftware getestet wurde, die jedenfalls nicht mit irischer Aussprache trainiert wurde (Zweig 2019, S. 214). Wird die KI daher nicht mit den Eigenschaften bestimmter Personengruppen trainiert, werden diese von der KI nicht mitgelernt (Zweig 2019, S. 215). ◄

2.12.4 Automatisierte Entscheidungsfindung

Zwar ist Art. 22 Abs. 1 DS-GVO als Betroffenenrecht formuliert, doch handelt es sich dabei um eine Verbotsnorm, die von Unternehmen einzuhalten ist (Arning 2018, Kap. 6, Rn. 345). Gegenstand der Vorschrift ist die automatisierte Entscheidungsfindung i.S.d. Art. 22 Abs. 1 DS-GVO. Diese setzt voraus, dass ein computertechnisches System eine Entscheidung trifft, ohne dass eine relevante menschliche Einflussnahme dazwischentritt (Martini 2018, Art. 22, Rn. 11). Art. 22 Abs. 1 DS-GVO umfasst demnach exklusiv solche Fälle, in denen der automatisierte Verarbeitungsprozess und die Entscheidung deckungsgleich sind (Martini 2018, Art. 22, Rn. 11).

[33] Vgl. dazu den Artikel „Irish-born native English speaker left in visa limbo after low score in voice recognition test" (2017). https://www.abc.net.au/news/2017-08-09/voice-recognition-computer-native-english-speaker-visa-limbo/8789076. Zugegriffen am 25.04.2020.

2.12.5 Rechtliche Wirkung oder ähnlich erhebliche Beeinträchtigung

Die Entscheidung muss rechtliche Wirkung gegenüber dem Betroffenen entfalten oder diesen in ähnlicher Weise erheblich beeinträchtigen (vgl. Art. 22 Abs. 1 DS-GVO). In der DS-GVO finden sich dazu keine näheren Konkretisierungen. Jedoch nimmt die Art.-29-Datenschutzgruppe in ihren Guidelines zu automatisierten Entscheidungen und Profiling, denen sich der EDSA angeschlossen hat, dazu Stellung (vgl. hierzu und im Folgenden Art.-29-Datenschutzgruppe 2018a, S. 23-24).

Demnach liegt eine rechtliche Wirkung vor, wenn die Entscheidung die Rechte einer Person, deren rechtlichen Status oder Rechte aus einem Vertrag betrifft (z. B. in Form der Kündigung eines Vertrages). Eine ähnlich erhebliche Beeinträchtigung liegt gem. Art.-29-Datenschutzgruppe vor, wenn die Entscheidung erhebliche Auswirkungen auf Umstände, das Verhalten oder die Entscheidungen der betroffenen Person hat, sie langfristig oder permanent beeinträchtigt oder zu deren Ausschluss bzw. Diskriminierung führt. Es lasse sich jedoch „schwer genau definieren, was als erheblich genug einzustufen ist, damit die Grenze erreicht wird".

Letztlich obliegt die Entscheidung, ob bei Fehlen der rechtlichen Wirkung der Entscheidung der Anwendungsbereich des Art. 22 DS-GVO aufgrund einer erheblichen Beeinträchtigung in ähnlicher Weise dennoch eröffnet ist, damit einmal mehr dem Rechtsanwender selbst. Lediglich beispielhaft nennt die Art.-29-Datenschutzgruppe mögliche einschlägige Falle (z. B. Entscheidungen über die Kreditwürdigkeit einer Person, den Zugang zu Gesundheitsdienstleistungen und Arbeitsplätzen oder Hochschulzulassungen). Praktisch relevant dürfte derzeit primär der – oben bereits dargestellte – Einsatz von Bewerbersoftware sein.

- Dies betrifft auch die Datenverarbeitungsvorgänge, die letztlich zur Identifikation des Kunden und eine individualisierte Ansprache des Kunden führen. Ob eine erhebliche Beeinträchtigung durch Profiling-Maßnahmen im Bereich des Online-Advertising stattfindet, hängt laut Art.-29-Datenschutzgruppe vom Grad der Profilbildung ab. Eine erhebliche Beeinträchtigung liege demnach im Bereich des Cross-Device-Tracking nahe.

2.12.6 Algorithmen und Darstellung der eingesetzten Logik

Art. 13 Abs. 2 lit. f DS-GVO und Art. 14 Abs. 2 lit. g DS-GVO verlangen für automatisierte Entscheidungsprozesse gem. Art. 22 Abs. 1 DS-GVO „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person". Entsprechend stellt es für Unternehmen eine besondere Herausforderung dar, ihre entsprechende Informationspflicht zu erfüllen und gleichzeitig ihre Geschäftsgeheimnisse zu waren.

2.12.6.1 Keine detaillierte Offenlegung des Algorithmus möglich

Auch hier kommt wieder das Black-Box-Phänomen zum Tragen. Da es selbst Programmierern nicht möglich ist, die Logik der Algorithmen im Detail zu entschlüsseln, können die gesetzlichen Anforderungen auch an dieser Stelle nur so weit reichen, wie der Verantwortliche diesen realistisch nachkommen kann. Zumindest in gewissen Grenzen eröffnet dabei das Verfahren des **Black Box Tinkering** die Möglichkeit, im Wege der Eingabe von Beispielsfällen und des Vergleichs der daraufhin ausgegebenen Entscheidungen, Rückschlüsse auf die dafür ausschlaggebenden Kriterien zu ziehen (Wagner 2018; Gigerenzer et al. 2018).

2.12.6.2 Darstellung der Grundannahmen der zugrunde liegenden Logik ausreichend

Die Informationspflicht gem. Art. 13 Abs. 1 lit. h DS-GVO kann infolgedessen nur dahingehend verstanden werden, dass die Darstellung der Grundannahmen der algorithmischen Logik ausreichend ist, der Algorithmus als konkrete Berechnungsformel folglich nicht offengelegt werden muss (Hennemann 2018, Art. 13, Rn. 31; a. A. wohl Roßnagel et al. 2015, S. 458). Dieses Verständnis folgt den Annahmen der Art.-29-Datenschutzgruppe. Diese verweist in ihren Guidelines auf „die Zunahme und Komplexität des maschinellen Lernens“ (vgl. hierzu und im Folgenden Art.-29-Datenschutzgruppe 2018a, S. 27–28), die das Verständnis für die „Funktionsweise einer automatisierten Entscheidungsfindung oder Profiling“ erschwerten. Eine „ausführliche Erläuterung der verwendeten Algorithmen oder (…) die Offenlegung des gesamten Algorithmus“ sei nicht angezeigt. Vielmehr halten die europäischen Datenschutzbehörden in ihrer Stellungnahme Verantwortliche dazu an, „einfache Möglichkeiten“ zu finden, um Betroffene über die zugrunde liegenden Überlegungen der Entscheidungsfindung zu unterrichten. Dies umfasse Informationen über die bei der Entscheidungsfindung berücksichtigten Merkmale, deren Quelle und Relevanz.

Eine solche Auslegung ist interessengerecht, weil der Betroffene über die wesentlichen Entscheidungsgrundlagen informiert wird, gleichzeitig Betriebs- und Geschäftsgeheimnisse aber nicht offengelegt werden.[34] Dies entspricht auch der Ratio von EG 63 S. 5 DS-GVO. Danach soll der Auskunftsanspruch, im Rahmen dessen ebenfalls über die involvierte Logik zu unterrichten ist, Geschäftsgeheimnisse nicht beeinträchtigen (Hennemann, Art. 13, Rn. 31). Für den Anspruch gem. Art. 22 Abs. 1 DS-GVO kann daher nichts anderes gelten. Insofern kann hier die nach Art. 13 Abs. 2 lit. f bestehende Informationspflicht sowohl mit den Spezifika von KI als auch dem Interesse des Unternehmens am Schutz von Geschäftsgeheimnissen in Einklang gebracht werden.[35]

---

[34] Vgl. Kugelmann 2016, S. 568; im Ergebnis auch Franck 2018, Art. 13, Rn. 26; i. E. entspricht dies der Entscheidung des BGH vom 28. Januar 2014 – VI ZR 156/13 = NJW 2014, S. 1236 zum Umfang des Auskunftsanspruchs gegen die Schufa, in der eine Verpflichtung zur Offenbarung der Score-Formel abgelehnt wurde.

[35] Bäcker, Art. 13 Rn. 54, der sich für eine Lösung des Spannungsverhältnisses im Hinblick auf die involvierte Logik auf der einen und dem Interesse am Schutz von Geschäftsgeheimnissen auf der anderen Seite über Art. 23 ausspricht; ähnlich Frank, Art. 13 Rn. 26.

2.13 Fazit

Spezifische KI-Regularien, die die KI-Entwicklung und deren Einsatz betreffen, existieren bisher nicht. Auch die DS-GVO enthält keine spezifischen Vorschriften. Es bleibt daher dem Rechtsanwender überlassen, die Schnittstellen zum Datenschutzrecht zu identifizieren.

Fundament eines KI-Projektes sollte dabei eine Datenschutzstrategie sein, die die KI-spezifischen datenschutzrechtlichen Fragestellungen aufzeigt und entsprechende Handlungspflichten daraus ableitet. Dazu gehören im Wesentlichen die Schaffung vertraglicher Grundlagen mit Auftragsverarbeitern und gemeinsam Verantwortlichen, die Durchführung einer Datenschutzfolgenabschätzung, die Bereitstellung der gesetzlich erforderlichen Informationen in den entsprechenden Datenschutzbestimmungen sowie die Sicherstellung eines Betroffenenmanagements, d. h. den Umgang mit Betroffenenanfragen. Dabei sind die in Art. 5 DS-GVO manifestierten datenschutzrechtlichen Kernprinzipien zu beachten. Im Bereich von KI-Projekten ist an dieser Stelle eine Auslegung der DS-GVO geboten, die die unternehmerischen Interessen an der Optimierung interner und externer Prozesse bestmöglich mit den Interessen der Betroffenen in Einklang bringt. Dies erfordert ggfs. eine extensive Auslegung der DS-GVO, etwa im Hinblick auf den Grad der Konkretisierung der erforderlichen Informationen in den Datenschutzbestimmungen. In jedem Fall können sich datenschutzrechtliche Verpflichtungen des Verantwortlichen nur im Rahmen des faktisch Machbaren und unter Berücksichtigung von KI-Spezifika bewegen. Es gilt daher, eine zu restriktive Auslegung entlang des Wortlauts der DS-GVO zu vermeiden, um den Fortschritt im Bereich der KI-Entwicklung nicht in unverhältnismäßigen Umfang zu beeinträchtigen.

Literatur

Arning M (2018) In: Moos F, Schefzig J, Arning M (Hrsg) Die neue Datenschutzgrundverordnung. De Gruyter, Berlin/Boston, S 2018

Art.-29-Datenschutzgruppe (2010) WP 169, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, angenommen am 16. Februar 2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf. Zugegriffen am 26.04.2020

Art.-29-Datenschutzgruppe (2014) WP 216, Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10.04.2014

Art.-29-Datenschutzgruppe (2017) WP 248 rev.01, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, zuletzt überarbeitet und angenommen am 4. Oktober 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Zugegriffen am 26.04.2020

Art.-29-Datenschutzgruppe (2018a) WP251rev.01, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, zuletzt überarbeitet

und angenommen am 6. Februar 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Zugegriffen am 26.04.2020

Art.-29-Datenschutzgruppe (2018b) WP 260 rev.01, Leitlinien für Transparenz gemäß der Verordnung 2016/679, zuletzt überarbeitet und angenommen am 10.04.2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Zugegriffen am 26.04.2020

Art.-29-Datenschutzgruppe (2018c) WP 259 rev.01, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, zuletzt überarbeitet und angenommen am 11.04.2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227. Zugegriffen am 26.04.2020

Bäcker M, Petri T (2018) In: Kühling J, Buchner B (Hrsg) Datenschutz-Grundverordnung/BDSG Kommentar, 2. Aufl. C.H. Beck, München

Begleitforschung Mittelstand-Digital (2019) Künstliche Intelligenz im Mittelstand. https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/kuenstliche-intelligenz-im-mittelstand.pdf?__blob=publicationFile&v=5. Zugegriffen am 26.04.2020

Bitkom e.V. (Hrsg) (2017) Entscheidungsunterstützung mit Künstlicher Intelligenz. https://www.bitkom.org/noindex/Publikationen/2017/Sonstiges/KI-Positionspapier/171012-KI-Gipfelpapier-online.pdf. Zugegriffen am 26.04.2020

Borchers D (2018) eHealth: Unternehmen fordern weniger Datensparsamkeit. https://www.heise.de/newsticker/meldung/eHealth-Unternehmen-fordern-weniger-Datensparsamkeit-4091321.html. Zugegriffen am 26.04.2020

Borzymowski M (2019) Föderales Lernen. https://theblue.ai/blog-de/federated-learning-foederales-lernen/. Zugegriffen am 26.04.2020

Bostrom N (1998) How Long Before Superintelligence?. https://nickbostrom.com/superintelligence.html. Zugegriffen am 30.01.2020

Brühl V (2019) WP Big Data, Data Mining, Machine Learning und Predictive Analytics: Ein konzeptioneller Überblick, CFS Working Paper Series, No. 617. https://www.econstor.eu/bitstream/10419/191736/1/1047269953.pdf. Zugegriffen am 26.04.2020

Brynjolfsson E, McAfee A (2019) Von Managern und Maschinen. Har Bus manag 2019(3):16–23

Buchner B, Petri T (2018) In: Kühling J, Buchner B (Hrsg) Datenschutz-Grundverordnung/BDSG Kommentar, 2. Aufl. C.H. Beck, München

Conrad C (2019) DS-GVO 2.0 – Effizienter(er) Schutz durch KI? In: Taeger J (Hrsg) Die Macht der Daten und der Algorithmen – Regulierung von IT, IoT und KI. Informatik und Recht, Edewecht, S 391–407

Drechsler J, Jentsch N (2018) Synthetische Daten, Innovationspotential und gesellschaftliche Herausforderungen, Mai 2018. https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf. Zugegriffen am 26.04.2020

Drewes S (2016) Dialogmarketing nach der DS-GVO ohne Einwilligung des Betroffenen. CR 2016:721–729

DSK (2018a) Kurzpapier Nr. 13, Auftragsverarbeitung nach Art. 28 DS-GVO, Stand: 16.01.2018. https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf. Zugegriffen am 26.04.2020

DSK (2018b) Kurzpapier Nr. 16, Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO, Stand: 19.03.2018. https://www.lda.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf. Zugegriffen am 26.04.2020

DSK (2018c) Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018. https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf. Zugegriffen am 26.04.2020

DSK (2018d) Orientierungshilfe zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO), November 2018. https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf. Zugegriffen am 26.04.2020

DSK (2019a) Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019. https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf. Zugegriffen am 26.04.2020

DSK (2019b) Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – Hambacher Erklärung zur Künstlichen Intelligenz, Hambacher Schloss, 3. April 2019. https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf. Zugegriffen am 26.04.2020

DSK (2019c) Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, Stand: 06.11.2019. https://www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf. Zugegriffen am 26.04.2020

Fink L (2019). https://www.micromata.de/blog/data-science/machine-learning-interview-laura-fink/. Zugegriffen am 26.04.2020

Franck L (2018) In: Gola P (Hrsg) DS-GVO, Kommentar. C.H. Beck, München

Gandhi S, Ehl C (2017) AI&U – Translating Artificial Intelligence into Business

Gausling T (2019a) Künstliche Intelligenz im Anwendungsbereich der DS-GVO. PinG 2019:1–10

Gausling T (2019b) Künstliche Intelligenz im digitalen Marketing – Datenschutzrechtliche Bewertung KI-gestützter Kommunikations-Tools und Profiling-Maßnahmen. ZD 2019:335–341

Gigerenzer G, Müller K, Wagner G (2018) Wie man Licht in die Black Box wirft. http://www.faz.net/aktuell/feuilsleton/debatten/wie-man-algorithmen-transparent-machen-kann-15652267.html?premium#void. Zugegriffen am 26.04.2020

Giles M (2018a) Duell der KIs. Technol Rev 2018(5):58–60

Giles M (2018b) Duell der KIs. https://m.heise.de/tr/artikel/Duell-der-KIs-4133903.html?seite=all. Zugegriffen am 26.04.2020

Google Developers (2019) Overview of GAN Structure. developers.google.com/machine-learning/gan/gan_structure. Zugegriffen am 15.06.2019

Graff B (2016) Rassistischer Chat-Roboter: Mit falschen Werten bombardiert. https://www.sueddeutsche.de/digital/microsoft-programm-tay-rassistischer-chat-roboter-mit-falschen-werten-bombardiert-1.2928421. Zugegriffen am 26.04.2019

Hennemann M (2018) In: Paal B, Pauly D (Hrsg) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl. C.H. Beck, München, S 2018

Honey C, Stieler W (2020) Die große KI-Kulisse. Technol Rev 2020(3):28–35

Klabunde A (2018) In: Ehmann E, Selmayr M (Hrsg) DS-GVO, Kommentar, 2. Aufl. C.H. Beck, München

Krempl S (2018) DS-GVO und KI: Unverträglichkeiten im Datenschutz. https://www.heise.de/newsticker/meldung/DSGVO-und-KI-Unvertraeglichkeiten-beim-Datenschutz-4049785.html. Zugegriffen am 26.04.2020

Kugelmann D (2016) Datenfinanzierte Internetangebote. DuD 2016:566–570

Luber S, Litzel S (2016) Was ist Data Mining. https://www.bigdata-insider.de/was-ist-data-mining-a-593421/. Zugegriffen am 26.04.2020

Manhart K (2018) Was Sie über Maschinelles Lernen wissen müssen. https://www.computerwoche.de/a/was-¬sie-ueber-maschinelles-lernen-wissen-muessen,3329560. Zugegriffen am 26.04.2020

Martini M (2018) In: Paal B, Pauly D (Hrsg) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl. C.H. Beck, München

Mauerer J (2017) Was ist was bei Predictive Analytics? https://www.computerwoche.de/a/was-ist-was-bei-predictive-analytics,3098583,3. Zugegriffen am 26.04.2020

Panetta K (2019) 5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019. https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/. Zugegriffen am 26.04.2020

Petereit D (2016) Was ist eigentlich der Unterschied zwischen AI, Machine Learning, Deep Learning und Natural Language Processing? https://t3n.de/news/ai-machine-learning-nlp-deep-learning-776907/. Zugegriffen am 26.04.2020

Roßnagel A, Nebel M, Richter P (2015) Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO. ZD 2015:455–460

Schefzig J (2014) Big Data = Personal Data? Der Personenbezug von Daten bei Big-Data-Analysen. In: Taeger J (Hrsg) Big Data & Co – Neue Herausforderungen für das Informationsrecht. Oldenburger Verlag für Wirtschaft, Informatik und Recht, Edewecht, S 103–118

Schild H (2020) In: Wolff H, Brink S (Hrsg) BeckOK Datenschutzrecht, 31. Edition, Stand: 01.02.2020. C.H. Beck, München

Schirmbacher M (2016) Onlinemarketing nach der DS-GVO – Ein Annäherungsversuch. ITRB 2016:274–280

Schmidt H (2018) https://www.netzoekonom.de/2018/06/24/wert-der-plattform-oekonomie-steigt-im-ersten-halbjahr-um-1-billion-dollar/. Zugegriffen am 26.04.2020

Schonschek O (2018) Künstliche Intelligenz und Fraud Detection – KI-Dienste helfen bei der Betrugserkennung. https://www.computerwoche.de/a/ki-dienste-helfen-bei-der-betrugserkennung,3545722. Zugegriffen am 26.04.2020

Schulz S (2018) In: Gola P (Hrsg) DS-GVO, Kommentar. C.H. Beck, München

Specht-Riemenschneider L, Schneider R (2019) Die gemeinsame Verantwortlichkeit im Datenschutzrecht – Rechtsfragen des Art. 26 DS-GVO am Beispiel „Facebook-Fanpages“. MMR 2019:503–509

Spoerr W (2020) In: Wolff H, Brink S (Hrsg) BeckOK Datenschutzrecht, 31. Aufl. Stand: 01.02.2020. C.H. Beck, München

Strassemeyer L (2020) Die Transparenzvorgaben der DS-GVO für algorithmische Verarbeitungen – Nachvollziehbarkeit durch innovative Lösungen – Gamification, Ablaufdiagramme und Bildsymbole. K&R 2020:176–183

Thalhofer T, Zdanowiecki K (2019) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, 3. Aufl. C.H. Beck, München

Wagner G (2018) Schlagwort „Open Source“: Algorithmen können und müssen anhand von Beispielfällen transparent gemacht werden. DIW Wochenbericht Nr. 26/2018

Wilmer T (2018) In: Jandt S, Steidle R (Hrsg) Datenschutz im Internet, 1. Aufl. Nomos Verlagsgesellschaft, Baden-Baden

Zimmer D (2019) Die Bändigung der Algorithmen. https://www.faz.net/aktuell/wirtschaft/digitec/regulierungsbedarf-die-baendigung-der-algorithmen-16508743.html?premium. Zugegriffen am 26.04.2020

Zweig K (2019) Ein Algorithmus kennt kein Taktgefühl – Wo künstliche Intelligenz sich irrt, warum uns das betrifft und was wir dagegen tun können, 3. Aufl. Wilhelm Heyne, München

Rechtliche Grenzen der Datenerhebung

3

Johannes Graf Ballestrem

Zusammenfassung

Einschränkungen der Datenerhebung können sich aus dem Lauterkeitsrecht oder dem Urhebergesetz ergeben. So kann beispielsweise KI-gestütztes Data Mining Urheberrechte oder Datenbankschutzrechte Dritter tangieren. Neben der Einordnung der auszulesenden Daten und Datenbanken im Hinblick auf das Urheberrecht und das Datenbankschutzrecht sui generis kommt es auch auf die genaue technische Umsetzung der Datenerhebung und -nutzung an, da sich in tatsächlicher Hinsicht ähnelnde Handlungen in rechtlicher Hinsicht gänzlich unterschiedlich beurteilt werden. Außerdem können aus der Datenerhebung resultierende Vorteile in Wettbewerbsverhältnissen wiederum zu rechtlich relevanten Nachteilen für denjenigen führen, dessen Daten ausgelesen und zu fremden Zwecken verwendet werden. Zusätzlich kann es sich bei den erhobenen Daten um Geschäftsgeheimnisse handeln, die rechtlichen Schutz über das Geschäftsgeheimnisgesetz genießen.

3.1 Urheberrechtliche Grenzen der Datenerhebung

Neben vertraglichen Verboten[1] ergeben sich auch aus dem Urhebergesetz Einschränkungen bei der Datenerhebung und -nutzung. So kann beispielsweise KI-gestütztes Data Mining Urheberrechte oder Datenbankschutzrechte Dritter tangieren. Zum einen können die erhobe-

[1] EuGH 15. Januar 2015, MMR 2015, 189 – Vertragliche Einschränkungen der Nutzung einer schutzlosen Datenbank.

J. G. Ballestrem (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: johannes.ballestrem@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_3

nen Daten unter Umständen selbstständig geschützte Werke im Sinne des Urhebergesetzes sein. Zum anderen können sie dem Inhalt einer geschützten Datenbank entstammen. In diesem Fall sind sie nur in begrenztem Umfang zulässigerweise nutzbar. Ähnliches gilt bei der Verwendung vermeintlich im Internet frei zugänglicher KI-Trainingsdaten. Im Regelfall wird die KI stets nur einen Bruchteil verfügbarer Daten aus geschützten Datenbanken nutzen. Entscheidend ist gleichwohl die rechtliche Einordnung der auszulesenden Daten und Datenbanken im Hinblick auf das Urheberrecht (§ 2 Abs. 1 und 2 UrhG) und das Datenbankschutzrecht sui generis (§ 87a ff. UrhG). Daneben kommt es auf die genaue technische Umsetzung der Datenerhebung und -nutzung an, da in tatsächlicher Hinsicht ähnliche Handlungen in rechtlicher Hinsicht gänzlich unterschiedlich beurteilt werden. Stets unzulässig ist jedenfalls das Umgehen technischer Schutzmaßnahmen, die offensichtlich dem Schutz urheberrechtlich oder datenbankschutzrechtlich geschützter Inhalte dienen (§ 95a UrhG).

3.1.1 Urheberrechte

Das Urheberrecht schützt die Urheber kreativer Arbeitsergebnisse vor der Fremdverwertung und öffentlichen Wiedergabe ihrer Werke, wodurch auch die Erhebung und Nutzung entsprechend geschützter Daten Einschränkungen unterliegen kann. Der urheberrechtliche Schutz knüpft an eine persönliche geistige Schöpfung an, also an ein Arbeitsergebnis, das hinreichend kreativ ist und von einer natürlichen Person stammt. Insofern können einzelne Daten nur urheberrechtlich geschützt sein, wenn sie auf einer kreativen Leistung des Urhebers beruhen. Beispiele sind literarische oder künstlerische Werke (§ 2 Abs. 1 UrhG). Die Schutzschwelle wird schon bei recht geringer Individualität erreicht. Daten als solche sind jedoch regelmäßig nicht geschützt. Auch nicht geschützt ist die bloße hinter dem Datum verborgene Idee oder Information (Informationsfreiheit). Ebenso wenig umfasst sind maschinengenerierte Daten, da diese in aller Regel keine geistige Schöpfung einer natürlichen Person, sondern das Ergebnis automatisierter Verfahren darstellen. Gerade diese Kategorie der „Maschinendaten" ist derzeit aber europaweit rechtlich stark umstritten.

▶ **Praxistipp** Auch Erzeugnisse, die sich im Ergebnis wie Werke präsentieren, sind dann keine eigenpersönlichen Schöpfungen, wenn sie ein Algorithmus erzeugt, ohne dabei Raum für kreative menschliche Gestaltung zu lassen.[2] Die KI selbst kann insoweit nicht Urheber sein. Urheber bleibt stets der Mensch. Nur der Mensch kann sich nach derzeitiger Rechtslage auf Urheberrechte berufen. Dabei kann er allerdings bei Schaffung des Werkes KI verwenden, solange bei ihm selbst noch ein eigener kreativer Anteil verbleibt.

Urheberrechtlich geschützte Daten dürfen ohne Zustimmung des Rechteinhabers schon nicht vervielfältigt, so insbesondere nicht abgespeichert werden (§ 16 UrhG). Das Abspei-

[2] KG Berlin 12. Dezember 2019, 2 U 12/16 Kart, juris Rn. 57 ff.; Loewenheim 2017, § 2 UrhG, Rn. 38–39.

chern findet bei vielen Nutzungsarten aber im Hintergrund jedenfalls als Vorbereitungs- oder Begleitmaßnahme statt. Auch das Abspeichern entsprechender Daten im Zuge der Datenerhebung greift in etwaige Urheberrechte ein. Die bloße Bildschirmanzeige ist hingegen zulässig, auch wenn technisch notwendige Vervielfältigungen durch Bildschirm und Grafikkarte erfolgen. Solche vorübergehenden, nur flüchtig und begleitend erfolgenden Vervielfältigungen sind privilegiert, sofern sie im Ergebnis einer rechtmäßigen Nutzung (bspw. der nicht öffentlichen Bildschirmanzeige) dienen (§ 44a UrhG).

Einschränkungen ergeben sich auch für die spätere Nutzung erhobener Daten. Die öffentliche Wiedergabe geschützter Inhalte ist von der Zustimmung des Rechteinhabers abhängig (§ 15 Abs. 2 UrhG). Insofern ist das Ins-Netz-Stellen von geschützten Inhalten unzulässig. Ein bloßes Verlinken öffentlich zugänglicher Inhalte ist hingegen regelmäßig ohne Zustimmung erlaubt.[3]

Daneben können auch Datenbanken vom Urheberrechtsschutz umfasst sein, wenn ihre Struktur (Auswahl und Anordnung der Elemente) hinreichend kreativ ist (§ 4 Abs. 1 UrhG). Schutzgegenstand ist dann aber nicht der Inhalt der Datenbank in Form der enthaltenen einzelnen Daten, sondern allein die kreative Struktur der Datenbank.[4] Dies ist allerdings eher selten der Fall. Ein Beispiel aus der Rechtsprechung ist etwa die kreative Zusammenstellung von Gedichten oder Kochrezepten. Nicht in diese Kategorie fallen hingegen insbesondere Verkaufsplattformen wie mobile.de, ebay.de, etc. Hier erfolgt die Datensammlung und geordnete Darstellung elektronisch und ohne messbaren kreativen Anteil des Datenbankinhabers. Solche „normalen" Datensammlungen können unter besonderen Bedingungen aber gleichwohl geschützt sein. Dazu nachfolgend unter Abschn. 3.2

Teile einer geschützten Datenbank dürfen ohne Zustimmung nur verwendet werden, wenn sie die kreative Strukturleistung nicht erkennen lassen. Die Übernahme einzelner von der Strukturleistung losgelöster Elemente ist nicht vom Schutzumfang umfasst. Die Entscheidung über die Verwendung urheberrechtlich relevanter Bestandteile der Datenbank obliegt hingegen dem Urheber.

▶ **Praxistipp** An dieser Stelle ergeben sich für den Nutzer von KI kaum Besonderheiten. Die KI selbst kann derzeit weder selbstständig Urheberrechte schaffen noch Rechte Dritter verletzen. Hinter der KI steht immer ein Mensch, der diese einsetzt und im Zweifel für die Folgen haftet. Nutzt ein KI-System also in großem Maße unberechtigterweise Daten, ist derjenige für die Rechtsverletzung verantwortlich, dem ein Verursachungsbeitrag nachgewiesen werden kann. Dies kann der Nutzer der KI sein, aber auch der Hersteller. Bereits beim Programmieren und Training der KI sollte daher darauf geachtet werden Sicherungsmechanismen zu implementieren, die eine unberechtigte Verwendung vom urheberrechtlich geschütztem Content verhindern. Die KI muss im Idealfall also auch „rechtlich" trainiert werden.

[3] EuGH 13. Februar 2014, GRUR 2014, 360.

[4] LG Köln 15. Juni 2005, MMR 2006, 52.

3.1.2 Datenbankschutzrechte

Mit jedem Tag wächst das Informationsangebot im Internet. Big-Data Analysen verknüpfen öffentlich verfügbare mit privaten Datensätzen. KI leistet auf dieser Grundlage einen Mehrwert, der weit über menschliche Auswertungsmöglichkeiten hinausgehen kann. Nicht zuletzt um eine zunehmend mögliche uferlose Nutzung von frei zugänglichen Datensammlungen zu verhindern hat der EU Gesetzgeber bereits in den 1990er-Jahren das Datenbankschutzrecht eingeführt. Das als „Datenbankschutz sui generis" bezeichnete Leistungsschutzrecht gemäß §§ 87a ff. UrhG wurde mit der EU-Datenbankrichtlinie in deutsches Recht umgesetzt. Von dem Leistungsschutzrecht umfasst sind ausschließlich Ergebnisse der Investitionen, die zur Beschaffung, Prüfung und Darstellung der Daten in Form einer Datenbank notwendig waren. Letztlich hat der Datenbankschutz für den Bereich der KI und für die Nutzung maschinengenerierter Daten daher weniger Bedeutung als oft angenommen. Investitionen die der Erzeugung der einzelnen Daten einer Datenbank dienen, sind nämlich nicht berücksichtigungsfähig.[5] Ebenso wie das Urheberrecht, schützt auch das Datenbankrecht sui generis daher die in der Datenbank enthaltenen Informationen und Daten als solche nicht.[6] Ebenso schutzlos sind sogenannte Spin-Off Datenbanken, die im Zuge anderer Leistungen nebenher entstehen und damit keiner gesonderten Investitionen bedürfen.[7] Die Abgrenzung ist im Einzelfall aber schwierig. Entsprechend umstritten ist die Grenze zwischen schutzfähiger Datenbank einerseits und ungeschützten, lediglich erzeugten und abgespeicherten Daten, andererseits.

Anders als bei gemäß § 2 UrhG geschützten Werken (auch Datenbankwerken) und nach § 72 ff. UrhG geschützten Lichtbildern ist für den sui generis Schutz des Datenbankherstellers unerheblich, auf welchem Weg die Datenbank erstellt wird. Werke dürfen nicht rein maschinell ohne Raum für menschliche Gestaltung erzeugt sein. Lichtbilder müssen in einem Verfahren hergestellt werden, das sich technisch wie eine Fotografie darstellt.[8] Dagegen sind Datenbanken gemäß § 87a ff. UrhG auch dann schutzfähig, wenn sie ausschließlich von Software erstellt worden sind. Es kommt allein auf die wesentliche Investition an. Bei Nutzung einer KI Lösung wird also sehr wohl die Investition in die KI zu berücksichtigen sein – nicht anders als etwa Lohnkosten für eine vergleichbare menschliche Tätigkeit zur Zusammenstellung und Pflege der Datenbank.

Liegt eine geschützte Datenbank vor, so ist die Verwertung oder öffentliche Wiedergabe der gesamten Datenbank oder wesentlicher Teile unzulässig. Dabei hält der BGH 10 % des Gesamtumfangs in quantitativer Hinsicht für unwesentlich.[9] Auf europäischer Ebene steht eine abschließende Rechtsprechung aber noch aus. In qualitativer Hinsicht ist

[5] EuGH 9. November 2004, GRUR 2005, 244.

[6] Siehe dazu Erwägungsgrund 46 der EU-Datenbankrichtlinie.

[7] EuGH 9. November 2004, GRUR int. 2005, 244.

[8] KG Berlin 12. Dezember 2019, 2 U 12/16 Kart, juris Rn. 74 f.

[9] BGH 1. Dezember 2010, GRUR 2011, 724.

der Umfang der getätigten Investitionen entscheidend. Der Verwertung wesentlicher Teile steht die wiederholte und systematische Verwertung kleinerer Teile der Datenbank gleich, sofern die Nutzung über den normalen Gebrauch einer Datenbank hinausgeht oder die Interessen des Rechteinhabers unzumutbar beeinträchtigt. Insofern ist auch eine Umgehung durch die Verwendung kleinerer Teile ausgeschlossen, wenn hierdurch schlussendlich insgesamt ein wesentlicher Teil der Datenbank verwendet wird. Zulässig bleibt allerdings die normale Auswertung einer Datenbank (sog. **Konsultation**), die durchaus wiederholt und systematisch erfolgen kann. Insofern ist auch die automatische Datenbankabfrage unter Zuhilfenahme von Algorithmen zulässig, wie sie beispielsweise durch Suchmaschinen erfolgt. Dies gilt somit auch für KI-Lösungen. Zulässig ist auch das Verlinken der aufgefundenen Inhalte, jedenfalls soweit dadurch nicht die Umgehung der Startseite ermöglicht wird. Daneben ist auch die Übermittlung kleiner, unwesentlicher Bestandteile einer Datenbank an anfragende Nutzer zulässig.[10] Unzulässig kann die Nutzung der Datenbank hingegen sein, um ein Konkurrenzprodukt zu schaffen oder das Geschäftsmodell des Rechteinhabers erheblich zu behindern, beispielsweise durch Minderung von Werbeeinnahmen oder durch Erschwerung des Abschlusses von Lizenzverträgen.

▶ **Praxistipp** Datenbankschutz und KI Anwendungen werden in der Praxis selten in Konflikt stehen, denn die Nutzung einzelner Daten ist grundsätzlich nicht verboten. Vorsichtig sollten Sie allerdings bei Verwendung von erheblichen Anteilen aus Datenbanken sein, auch wenn die Datenbanken von ihrem Inhaber frei ins Netz gestellt wurden. In diesem Fall sollten auch etwaige Nutzungsbedingungen beachtet werden. Eine Umgehung technischer Maßnahmen (beispielsweise CAPTCHAS), die darauf ausgerichtet sind KI-gestützte Massenabfragen zu verhindern, kann ebenfalls rechtliche Probleme bringen. Die Abgrenzung ist keineswegs trivial und sollte stets mit Rechtsberatung erfolgen. Bei unzulässigen Handlungen drohen Ihnen als Nutzer der KI Unterlassungs-, Beseitigungs- und Schadensersatzansprüche.

3.1.3 Text und Data Mining

Eine gängige Vorgehensweise im Rahmen der Datenerhebung stellt das Data Mining dar.[11] Selbstverständlich ist gerade dies zugleich ein interessanter Anwendungsfall für KI-Lösungen. Im Zuge des Data Mining werden aber häufig, zum Zwecke der Vorbereitung des eigentlichen Auslesens, Kopien der auszulesenden Datenbanken angefertigt. Insofern wird durch die Vorbereitungsmaßnahmen regelmäßig in bestehende Urheber- oder Datenbankschutzrechte eingegriffen, sofern auf die Anfertigung von Kopien eines wesentlichen Teils der Datenbanken nicht verzichtet werden kann.

[10] BGH 17. Juli 2003, GRUR 2003, 958.

[11] Zum Data Mining im Steuerrecht vgl. Kap. 7, Abschn. 7.1.1 sowie Kap. 7, Abschn. 7.1.1.4.

Das deutsche Gesetz kennt im Bereich des Text und Data Mining eine Ausnahme, die allerdings ausschließlich für wissenschaftliche Forschungszwecke anwendbar ist (§ 60d UrhG). Die wirtschaftliche Nutzung solcher Data Mining Systeme ist hingegen bislang nicht privilegiert. Versuche, die bloß nebensächliche bzw. vorbereitende Vervielfältigung nicht unter den Begriff der Vervielfältigung im Sinne des Urheberrechts zu subsumieren oder unter die privilegierende Vorschrift des § 44a UrhG zu fassen, scheitern (Spindler 2016, S. 1112). Damit bedarf auch die Vervielfältigung zum Zwecke des Data Mining prinzipiell der Zustimmung des Rechteinhabers.

Der EU-Gesetzgeber hat die Notwendigkeit einer Sonderregelung erkannt und in Artikel 4 der EU-Richtlinie 2019/790 eine Privilegierung entsprechender Vorbereitungsmaßnahmen aufgegriffen. Auch diese Erleichterung findet ihre Grenzen allerdings dort, wo Zugangsbarrieren umgangen werden müssen oder Nutzungsvorbehalte der entsprechenden Verwendung entgegenstehen. Eine Aufbewahrung der Kopien ist zudem zeitlich auf das notwendige Maß begrenzt. Es ist anzunehmen, dass die Schutzrechtsinhaber die Möglichkeit nutzen werden, ihre Inhalte Nutzungsvorbehalten zu unterwerfen, wodurch die Privilegierung weitgehend wertlos sein dürfte. Die Richtlinie gilt in den Mitgliedstaaten zudem nicht unmittelbar, sondern muss von dem deutschen Gesetzgeber umgesetzt werden. Die Umsetzungsfrist endet Anfang Juni 2021.

3.2 Wettbewerbsrechtliche Grenzen der Datenerhebung

Sowohl die Datenerhebung als auch die Nutzung erhobener Daten kann lauterkeitsrechtlich Bedeutung erlangen. Das UWG schützt in § 4 UWG die Mitbewerber vor einer Beeinträchtigung ihrer wettbewerblichen Entfaltungsmöglichkeiten, die über normale Beeinträchtigungen im Wettbewerbsverhältnis hinausgehen. Neben dem Schutz vor unzulässigen Nachahmungen (§ 4 Nr. 3 UWG), bietet der Auffangtatbestand des § 4 Nr. 4 UWG Möglichkeiten, gegen das (automatisierte) Auslesen von Daten vorzugehen.

Zusätzlich kann es sich bei den erhobenen Daten um Geschäftsgeheimnisse handeln, die rechtlichen Schutz über das Geschäftsgeheimnisgesetz erlangen. Die Einordnung der Daten als Geschäftsgeheimnis hat Auswirkungen auf die Zulässigkeit der Erlangung und Nutzung der Daten.

3.2.1 Lauterkeitsrecht

Aus der Datenerhebung resultierende Vorteile führen in Wettbewerbsverhältnissen wiederum zu Nachteilen für denjenigen, dessen Daten ausgelesen und zu fremden Zwecken verwendet werden. Das Erzeugen und Aufbereiten von Daten wird regelmäßig höhere Aufwendungen abverlangen als das Auslesen der bereits vorliegenden Daten. Insbesondere technische Verfahren zur automatisierten Datenerhebung, wie Webcrawling und Screen-Scraping, ermöglichen das schnelle und unkomplizierte Auslesen von Inhalten vor

allem im Internet. Durch die Übernahme „fremder" Daten in Suchmaschinen, Vergleichsportale oder durch Wiedergabe im eigenen Namen, wird die Amortisierung der Investitionen des Mitbewerbers stark erschwert. Die Nutzung ausgelesener Daten zu eigenen Zwecken führt regelmäßig zu verringerten Besucherzahlen auf der Webseite des Mitbewerbers und/oder beeinträchtigt die Konkurrenzfähigkeit des betroffenen Marktteilnehmers, der deutlich höhere Investitionen aufwenden musste. Dennoch ist die (automatisierte) Datenerhebung nicht per se unzulässig. Das Lauterkeitsrecht beschränkt jedoch die Erhebung von Daten und deren spätere Verwendung in bestimmten Sachverhaltskonstellationen. In der Rechtsprechung haben sich einige relevante Fallgruppen entwickelt.

▶ **Praxistipp** Generell steht der Einsatz von KI an dieser Stelle unter den gleichen Vorbehalten wie menschliche Verhaltensweisen und der Einsatz bestimmter Software allgemein. KI-Lösungen führen allerdings in gesteigertem Maße dazu, dass der Mensch seine Kontrolle abgibt. Insoweit treffen ihn besondere Pflichten trotzdem für ausreichende wettbewerbliche Compliance Sorge zu tragen. Der Einsatz der KI-Lösung entbindet daher insbesondere nicht davon, sich im Wettbewerb weiterhin fair zu verhalten. Die Geschäftsführung muss daher auch KI-Lösungen regelmäßig darauf kontrollieren lassen, ob unter Umständen Wettbewerbsverstöße drohen oder sogar abzustellen sind. Erwartungsgemäß werden Gerichte ähnliche Maßstäbe anwenden, wie sie bereits für die Compliance Überwachung und Belehrung der Mitarbeiter im eigenen Unternehmen gelten.

3.2.1.1 Nachahmungsschutz

Das Lauterkeitsrecht schützt Wettbewerber vor unzulässigen Nachahmungen ihrer Leistungen, § 4 Nr. 3 UWG. Hierdurch wird die Datenerhebung als solche noch nicht beschränkt. Die Nutzung der erhobenen Daten zum Zwecke der Entwicklung eines Konkurrenzprodukts unterliegt Grenzen. Unter Umständen kann das Anbieten eines nachahmenden Konkurrenzproduktes unzulässig sein. Der KI-Lösung, die etwa zum Produktdesign eingesetzt wird, sollte daher nicht blind vertraut werden. Vielmehr muss der Nutzer sicherstellen, dass das Endprodukt tatsächlich zulässig vertrieben werden darf, insbesondere keine (unzulässige) Nachahmung eines Wettbewerbers darstellt.

Der ergänzende Leistungsschutz setzt aber zunächst eine wettbewerbliche Eigenart der nachgeahmten Leistung voraus. Unter dem Begriff der wettbewerblichen Eigenart verstehen die Gerichte eine Leistung, deren konkrete Ausgestaltung oder bestimmte Merkmale geeignet sind, die angesprochenen Verkehrskreise auf die betriebliche Herkunft oder Besonderheiten hinzuweisen.[12] Insofern ist der Wettbewerber nicht vor einer Anlehnung an jegliche Leistungen geschützt. Vielmehr muss es sich um prägnante Leistungsmerkmale

[12] BGH 2. Dezember 2015, GRUR 2016, 730.

handeln. Daneben muss ein besonderer Unlauterkeitstatbestand vorliegen, der vorliegt wenn die Leistung zu stark an die fremde Leistung erinnert (Herkunftstäuschung) oder die Wertschätzung der nachgeahmten Leistung ausnutzt oder beeinträchtigt, aber insbesondere auch wenn die zur Nachahmung erforderlichen Informationen unredlich erlangt wurden. In diesem Zusammenhang kommt es in erster Linie maßgeblich auf die rechtliche Beurteilung des Sachverhalts nach dem Geschäftsgeheimnisgesetz an Daneben kann sich die Unredlichkeit aus Straftaten ergeben, wie einem Diebstahl von Unterlagen oder Kenntniserlangung durch Betrug. Die Rechtsprechung hält auch das Erschleichen oder missbräuchliche Ausnutzen eines Vertrauensverhältnisses (Vertrauensbruch) für tatbestandsmäßig.[13] Das Erarbeiten der Kenntnisse durch Reverse Engineering ist hingegen, entsprechend der Wertungen des Geschäftsgeheimnisgesetzes, zulässig.

3.2.1.2 Schleichbezug

Der Mitbewerberschutz umfasst daneben die gezielte Behinderung (§ 4 Nr. 4 UWG), worunter unter anderem die Fallgruppe des Schleichbezugs subsumiert wird. Eine solche Behinderung kann sich aus dem Hinwegsetzen über ein selektives Vertriebssystem ergeben. Das Erschleichen von Daten, die eigentlich ausschließlich über ein solches selektives System erworben werden können, stellt unter Umständen einen unzulässigen Schleichbezug dar. Dabei genügt ein Verstoß gegen die AGB des Wettbewerbers jedoch noch nicht. Erst die Umgehung technischer Schutzvorkehrungen unter Einsatz technischer Verfahren begründet die Unlauterkeit eines Schleichbezugs durch das Auslesen von Daten. Bei entsprechenden technischen Vorkehrungen ist daher von einer Datenerhebung Abstand zu nehmen. Die KI muss also auch in der Lage sein, derartige Sicherungsvorkehrungen zu erkennen und zu beachten.

3.2.1.3 Betriebsstörung

Der Vorgang der Datenerhebung kann technisch auf unterschiedlichste Weise durchgeführt werden, so beispielsweise mittels des sogenannten Screen-Scraping. Vereinzelt können solche Vorgänge auch Auswirkungen auf den Betrieb haben, dessen Daten ausgelesen werden. Der Einsatz technischer Mittel kann in Einzelfällen die Funktionsfähigkeit der Systeme beeinträchtigen und zu Verzögerungen oder weiteren technischen Problemen führen, die sich nachteilig auf den Betrieb auswirken. Der Einsatz entsprechend wirkender technischer Mittel ist nach § 4 Nr. 4 UWG unzulässig (Jänich 2020, § 4 Nr. 4 UWG Rn. 78). In der Praxis dürfte es aber meist schwer fallen eine spürbare Beeinträchtigung sowie die Kausalität solcher Handlungen für etwaige Störungen darzulegen und zu beweisen. Keine unzulässige Betriebsstörung stellt der Betrieb eines Systems dar, das durch Anzeigen fremder (schutzloser) Inhalte mittelbar zu einer Minderung der Webseiten-Aufrufe Dritter führt.[14]

[13] BGH 2. Oktober 2008, GRUR 2009, 416; BGH 7. November 2002, GRUR 2003, 356.

[14] BGH 22. Juni 2011, GRUR 2011, 1018.

3.2.2 Geschäftsgeheimnisse

Auch der Schutz von Geschäftsgeheimnissen kann der Datenerhebung entgegenstehen. So ist sowohl die unbefugte Erlangung als auch die unerlaubte Nutzung bzw. Offenlegung von Geschäftsgeheimnissen verboten. Dabei ist jedoch nicht jede geheime Information rechtlich geschützt. Das die EU-Geheimnisschutzrichtlinie umsetzende Geschäftsgeheimnisgesetz umfasst nunmehr Informationen, die geheim sind und aus diesem Grund einen wirtschaftlichen Wert haben. Zudem sind neben einem berechtigen Interesse auch angemessene Geheimhaltungsmaßnahmen erforderlich, um den Geheimnisschutz zu erlangen. Dabei bereitet die Auslegung des Merkmals der angemessenen Geheimhaltungsmaßnahmen in der Praxis Schwierigkeiten und führt zu Rechtsunsicherheiten für die Inhaber der Geheimnisse. Andererseits senkt dieses Erfordernis die Haftungsrisiken der Nutzer, die den Geheimnischarakter einer Information an entsprechenden Maßnahmen erkennen können. Solche Maßnahmen können insbesondere Kennzeichnungen, vertragliche Geheimhaltungsvereinbarungen aber auch technische Maßnahmen sein. Der Umfang notwendiger Maßnahmen ist vom Einzelfall abhängig.

Aus dem Geheimnisschutzgesetz und besonders den rechtlichen Unsicherheiten hinsichtlich der Schutzvoraussetzungen ergeben sich wesentliche Einschränkungen für die Datenerhebung. Bei Vorliegen vertraglicher Beschränkungen oder technischer Schutzmaßnahmen sollte eine Datenerhebung nicht ohne weitere Prüfung vorgenommen werden, da nicht ausgeschlossen werden kann, dass es sich bei entsprechenden Daten um geschützte Geschäftsgeheimnisse handelt.

Unter die erlaubten Handlungen fällt aber das Reverse Engineering (§ 3 Abs. 1 Nr. 2 GeschGehG). Geschäftsgeheimnisse dürfen durch Erforschung eines öffentlich verfügbaren oder rechtmäßig im Besitz befindlichen Produkts erlangt werden und vorbehaltlich anderer rechtlicher Grenzen genutzt werden.

► **Praxistipp** Da ein Reverse Engineering öffentlich verfügbarer Produkte zulässig ist ergeben sich durch Nutzung von KI neue Möglichkeiten an zuvor verborgene Geheimnisse zu gelangen. Da die Rechtsprechung die Bewertung als Geschäftsgeheimnis unter anderem davon abhängig macht wie schwer oder leicht dieses aus einem Produkt für jedermann zu ermitteln ist, stellt sich in Zukunft vermehrt die Frage nach der Möglichkeit derartige Geheimnisse überhaupt noch zu schützen. Ein Weg sind vertraglich zulässige Beschränkungen des Reverse Engineerings. Aber Vorsicht: Derartige Beschränkungen sind praktisch wirkungslos, sobald jedermann das Produkt auch ohne Beschränkungen erwerben kann oder anderweitig legalen Zugang zu dem Produkt hat. Dann werden vertragliche Beschränkungen unwirksam.

Literatur

Jänich VM (2020) In: Heermann P, Schlingloff J (Hrsg) Münchener Kommentar zum Lauterkeitsrecht, Bd 1, 3. Aufl. § 4 Nr. 4 UWG C.H. Beck, München

Loewenheim U (2017) In: Loewenheim U, Leistner M, Ohly A (Hrsg) Schricker/Loewenheim Urheberrecht Kommentar, 5. Aufl. § 2 UrhG. C.H. Beck, München

Spindler G (2016) Text und Data Mining – urheber- und datenschutzrechtliche Fragen. GRUR 2016:1112–1120

Zugangsansprüche zu Daten

4

Johannes Graf Ballestrem und Sebastian Hack

Zusammenfassung

In diesem Kapitel wird in die urheber- und kartellrechtlichen Diskussionen rund um Zugangsrechte zu fremden Datensätzen eingeführt. Bereits heute bestehen Möglichkeiten derartige Zugangsansprüche durchzusetzen. Die Bedingungen für Datenzugangsansprüche werden jedoch voraussichtlich in der Zukunft für Zugangspetenten aufgrund anstehender Gesetzesänderungen und sektorspezifischen Regeln noch günstiger.

4.1 Einleitung

Daten sind in der digitalen Ökonomie ein wertvolles Gut und häufig ein ganz wesentlicher Input für den Erfolg und die Funktionsfähigkeit von KI. Aus diesem Grund stellt sich häufig die Frage, inwieweit Dritte einen Anspruch auf den Zugang und die Nutzung von fremden Datensätzen haben können. Dabei wird die Diskussion häufig unter zwei rechtlichen Blickwinkeln geführt: dem Kartellrecht und dem Urheberrecht. Das nachfolgende Kapitel gibt einen Überblick über die rechtlichen Rahmenbedingungen unter denen ein solcher Anspruch bestehen kann.

4.2 Kartellrecht

Das Kartellrecht dient dem Erhalt des funktionierenden Wettbewerbs. Dort wo Maßnahmen versuchen diesen auszuschalten oder zu beschädigen, greift das Kartellrecht regelnd ein. Dies gilt auch dort, wo Unternehmen sich auch über legitime Mittel eine monopolistische

J. G. Ballestrem · S. Hack (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: johannes.ballestrem@osborneclarke.com; sebastian.hack@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_4

Position aufgebaut haben. Diese Unternehmen unterliegen besonderen kartellrechtlichen Pflichten, um den bereits reduzierten Wettbewerb im selben Markt zu schützen und zu verhindern, dass der Monopolist seine Marktmacht in wettbewerbsfremder Weise einsetzt, um sich auch in anderen Märkten einen Vorteil zu verschaffen. Aus diesem Grund gibt es die kartellrechtlichen Marktmissbrauchsregeln. Nach diesen kann die Verweigerung eines Monopolisten Waren zu liefern, eine Dienstleistung zu erbringen oder eben Zugang zu einer Einrichtung zu gewähren, missbräuchlich sein, wenn hierdurch der Wettbewerb in nicht sachgerechtfertigter Weise beschränkt wird. Inwieweit gilt dies aber auch für den Zugang zu Daten?

4.2.1 Zugangsverweigerung als Missbrauch einer marktbeherrschenden Stellung

Ein Anspruch auf Zugang zu Daten kann sich unter engen Voraussetzungen aus den kartellrechtlichen Missbrauchstatbeständen des europäischen (Art. 102 AEUV) und deutschen (§ 19 GWB) Kartellrechts in Verbindung mit §§ 33 GWB ergeben. Dabei folgen die kartellrechtlichen Missbrauchstatbestände stark vereinfacht einem prüfungstechnischen Zwei-Schritt: zunächst muss ein Unternehmen über ein solches Maß an Marktmacht verfügen, dass es marktbeherrschend im kartellrechtlichen Sinne ist, und zweitens muss es muss diese Marktmacht auch in nicht-sachgerechtfertigter Weise missbraucht haben. Geschädigte von eines solchen Missbrauchs haben dann einen Unterlassensanspruch (in Deutschland nach § 33 GWB), der sich in einen aktiven Zugangsanspruch umwandelt, wenn die einzige Form des Unterlassens des Verstoßes die Lieferung bzw. die Zugangsgewährung darstellt.

Im Einzelnen:

4.2.1.1 Marktbeherrschung

Wann vermitteln Daten eine marktbeherrschende Stellung und stellen für Dritte ein solch unverzichtbares Gut dar, dass der Inhaber verpflichtet werden kann sie mit Dritten zu teilen? Die kartellrechtliche Diskussion um Zwangslizenzen in Bezug auf den Zugang zu Daten wird in der Regel im Zusammenhang mit der sog. „**Essential Facilities-Doktrin**“ geführt.

Dabei wurden die Grundsätze der Essential Facilities-Doktrin im US-amerikanischen Kartellrecht für Sachverhaltskonstellationen entwickelt bei denen ein Unternehmen den Zugang zu unverzichtbaren Inputfaktoren für Anbieter auf nachgelagerten Märkten verweigerte. Dabei ging es in den ursprünglichen Fällen um physische Infrastruktureinrichtungen wie Hafenanlagen, Eisenbahn- und Stromnetze. Der Inhaber der jeweiligen Infrastruktureinrichtung konnte die Existenz, den Umfang und die Konditionen auf der nachgelagerten Marktstufe nach eigenem Ermessen kontrollieren. Aufgrund der damit verbundenen wettbewerbsschädigenden Auswirkungen schuf die Rechtsprechung das Verbot der wettbewerbsbeschränkenden Zugangsverweigerung zu Infrastrukturmonopolen (essential facilities). Aus dem Verbot der Zugangsverweigerung wurde in praktischer Konsequenz ein Geschäftsabschlusszwang.

In der europäischen Entscheidungspraxis wurde dieser Grundsatz auf gewerbliche Schutzrechte ausgeweitet (EuGH, Urt. v. 29.04.2004, C-418/01, NJW 2004, 2725 (Ls.) – IMS Health; EuGH, Urt. v. 26.11.1998, C-7/97, NJW 1999, 2259 – Bronner; EuGH, Urt. v. 06.04.1995, C-241/91 P und C-242/91 P, GRUR Int. 1995, 490 – Magill; EuG, Urt. v. 17.09.2007, T-201/04, WuW 2007, 1169 – Microsoft). Demnach kann ein Zwangslizenz-Anspruch bestehen, wenn ein tatsächlicher oder potenzieller Markt für ein Produkt oder eine Leistung besteht, die Einrichtung für diesen Markt unersetzbar ist sowie nicht mit angemessenen Mitteln reproduzierbar ist und die Zugangsverweigerung effektiven Wettbewerb verhindert.

Während es in der ursprünglichen Entscheidungspraxis zur Essential Facility Doktrin um natürliche Monopole ging, stellen die gewerblichen Schutzrechte, wie sie Gegenstand der europäischen Kartellrechtspraxis waren, rechtliche Monopole dar. Diese rechtlichen Monopole ermöglichen es ihrem Inhaber in der Regel, Unterlassungsansprüche geltend zu machen und durch deren Durchsetzung nicht nur mögliche Verletzer des jeweiligen gewerblichen Schutzrechtes, sondern auch Marktteilnehmer von einem Tätigwerden auf dem Markt auszuschließen (Louven 2018, S. 218).

Inwieweit diese Grundsätze auf Daten übertragbar sind, ist nicht nur Gegenstand anhaltenden rechtlichen Diskurses, sondern hängt auch von Daten ab. Denn bislang sind Daten und Datensätze in der Regel nicht umfassend durch gewerbliche Schutz- oder Eigentumsrechte geschützt, die ein rechtliches Monopol vermitteln könnten (siehe hierzu im Detail Kap. 3). Soweit die Europäische Kommission in ihren Veröffentlichungen zu diesem Thema einzelne Sonderregelungen nennt, hält sie diese jedoch selber für fleckenhaft (Europäische Kommission, COM (2017) 2 final, S. 11; Europäische Kommission, SWD (2017) 2 final, S. 19 ff.).

Aber selbst wenn derzeit Daten noch kein umfassendes rechtliches Monopol vermitteln und ein natürliches Monopol ebenfalls in Bezug auf Daten nicht naheliegt, können Daten gleichwohl zu einem faktischen Monopol führen. Allerdings sind dabei die Besonderheiten von Daten zu beachten, denn diese sind zum Teil nicht exklusiv, d. h. duplizierbar, und zum anderen sind sie in ihrer Nutzbarkeit weder erschöpflich noch rival. Insbesondere bei personenbezogenen Daten kommt es daher bei der Bestimmung von Marktmacht nicht alleine auf die Menge der Daten an, sondern auch auf die Art, Qualität sowie das Alter etc. So kann nicht allein aus dem Umstand, dass ein Marktteilnehmer über eine große Menge an Daten verfügt, der Schluss gezogen werden, er verfügt über Marktmacht auf dem relevanten Markt (Körber 2016 S. 305). So kann abhängig von der Qualität der Daten ein kleiner Datensatz eine höhere wettbewerbliche Bedeutung haben als ein sehr großer. Daten können aber insbesondere dann eine marktbeherrschende Stellung vermitteln, wenn der Zugang zu diesen Daten eine Marktzutrittsschranke darstellt oder Wettbewerber ohne den Zugang in sonstiger Weise erheblich vom Wettbewerb ausgeschlossen werden. Bei personenbezogenen Daten ist dies weniger wahrscheinlich, aber ein besonders großer Datensatz oder Datenpool, i. S. v. Big Data oder Bulk Data, die einen schwer einholbaren Vorsprung im Wettbewerb vermitteln, kann gleichwohl Datenmacht vermitteln (Bundeskartellamt 2016, S. 95 f.).

Nicht-personenbezogene Daten wie herstellerbezogene Daten, die nur durch den Hersteller oder den direkt Berechtigten erstellt werden können, sind hingegen häufig schon wegen rechtlicher oder faktischer Hindernisse nicht duplizierbar. In diesem Fall verfügt das Unternehmen, das die Daten erzeugt oder aus nicht öffentlich zugänglichen Quellen zusammenstellt, über einen exklusiven Zugang zu diesen Daten. Denkbar ist dies z. B. bei fahrzeug- oder maschinenbezogenen Daten eines Herstellers. Diese faktische „Datenherrschaft" kann in Fällen relativer oder überlegener Marktmacht des datenhaltenden Unternehmens sogar noch zusätzlicher Verstärker wirken, wenn also eine besondere Abhängigkeit eines Wettbewerbers von der Einrichtung besteht (Louven 2018, S. 220). Die Rechtsprechung hat eine derartige Abhängigkeit beispielsweise für Ersatzteile und Ersatzteilinformationen bejaht (vgl. BGH, Urt. v. 06.10.2015, KZR 87/13, NZKart 2015, S. 535 – Porsche-Tuning).

Es sind daher zahlreiche Konstellationen denkbar in denen Unternehmen über Datensätze verfügen, von deren Zugang der Wettbewerb auf einer nachgelagerten Stufe abhängt und somit die Datenherrschaft eine der Essential Facilities Doktrin vergleichbare Monopolstellung vermittelt.

4.2.1.2 Missbrauch der marktbeherrschenden Stellung

Die Zugangsverweigerung zum Datenmonopol stellt dann unter den Voraussetzungen der Essential Facilities-Doktrin eine missbräuchliche Ausnutzung der marktbeherrschenden Stellung in Form des Behinderungsmissbrauchs dar. Dabei ist der Begriff der missbräuchlichen Ausnutzung ein objektiver Begriff. Es kommt daher auf die objektive Beeinträchtigung des Wettbewerbs und weniger auf die subjektiven Absichten des Monopolisten an. Danach kann es missbräuchlich sein, wenn die Zugangsverweigerung Wettbewerb auf einem nachgelagerten Markt verhindert, die Daten an sich für den nachgelagerten Markt unersetzlich sind und keine objektive Rechtfertigung für die Zugangsverweigerung besteht. Dementsprechend hat der BGH in der Verweigerung des Zugangs zu einer Diagnose-Software für Kfz sowie der darin verfügbaren Ersatzteilinformationen durch einen Kfz-Hersteller gegenüber einem Tuning-Unternehmen, das einen Softwarezugang zur Wartung und Instandsetzung von Serienfahrzeugen des Kfz-Herstellers nachfragte, eine unbillige Behinderung gesehen (BGH, Urt. v. 06.10.2015, KZR 87/13, NZKart 2015, S. 535, S. 541 – Porsche-Tuning).

Allerdings ist bei der Frage des Missbrauchs auch in den Blick zu nehmen, ob die Maßnahme des Monopolisten objektiv gerechtfertigt ist. Abhängig vom Datenzuschnitt und Aggregationsgrad könnten z. B. datenschutzrechtliche Verbote gegen die Unzulässigkeit einer Zugangsverweigerung sprechen. Zudem sind auch die berechtigten Interessen am Schutz von Betriebs-und Geschäftsgeheimnisse hinreichend zu würdigen und bei der Ausgestaltung der Zugangsgewährung zu berücksichtigen.

► **Praxistipp** Die Durchsetzung kartellrechtlicher Zugangsansprüche ist auch gegenüber Datenmonopolisten möglich. Die Anforderungen an die Durchsetzung sind allerdings hoch. Insbesondere darf der Zugang nicht auf andere

Weise substituierbar sein. Bislang sind zugleich verhältnismäßig wenige Verfahren bekannt mit welchen der Zugang zu Daten erfolgreich erstritten wurde. Mit zunehmender Bedeutung digitaler Lösungen wachsen aber zugleich die Fallzahlen. Sowohl nationale Kartellbehörden als auch die EU befassen sich derzeit intensiv mit der Thematik. Es lohnt sich daher die rechtliche Entwicklung eng zu verfolgen, um mögliche Chancen aber auch Risiken für den eigenen Datenbestand zu erkennen. Ob dieser Datenbestand durch KI-Lösungen verwaltet wird ist dabei weniger entscheidend. Allerdings bieten KI-Lösungen allein durch ihre Effizienz weiteres Potenzial für die Bejahung von Marktmacht bei der Datensammlung.

4.2.2 Regulatorische Ansprüche

Neben einem kartellrechtlichen Anspruch auf Datenzugang gibt es vereinzelt auch spezialgesetzliche Regelungen, die Zugangsansprüche zu bestimmten Daten regeln, um in speziellen Branchen einen Wettbewerb zu ermöglichen oder zu fördern.

Ein Beispiel ist der sogenannte Automotive-Aftermarket. Um Reparatur- und Wartungsdienstleistungen erbringen zu können, sind bestimmte Daten der Fahrzeughersteller elementar. Daher sind die Anbieter von Reparatur- und Wartungsdienstleistungen auf den Zugang zu Fahrzeugdaten zwingend angewiesen. Hierzu zählt beispielsweise die Fahrzeugidentifikationsnummer, die sogenannte VIN. Diese ist in umfangreichen Datenbanken der Fahrzeughersteller mit weiteren notwendigen Daten verknüpft, aus denen sich ergibt, welche Komponenten in einem Fahrzeug verbaut sind. Diese Informationen sind notwendig, um Wartungs- und Reparaturdienstleistungen an dem jeweiligen Fahrzeug vornehmen zu können. Die notwendigen Kenntnisse hat aber allein der Hersteller des Fahrzeugs.

Das faktische Datenmonopol der Fahrzeughersteller führt daher zu wettbewerbsrechtlichen Schwierigkeiten. Die Hersteller können den Zugang zu den Fahrzeugdaten ganz verweigern oder die Konditionen des Zugangs zu Ungunsten der anderen Akteure gestalten und damit einen funktionierenden Wettbewerb auf dem Automotive-Aftermarket verhindern.

Der EU-Gesetzgeber hat diese Problematik erkannt und schon mit der Verordnung Nr. 715/2007 spezialgesetzliche Regelungen für diesen Anwendungsbereich geschaffen. Art. 6 der Verordnung verpflichtet die Fahrzeughersteller zur Gewährung eines uneingeschränkten und standardisierten Zugangs zu Reparatur- und Wartungsinformationen auf leicht und unverzüglich zugängliche Weise über das Internet mithilfe eines standardisierten Formats.

Die Verordnung regelt jedoch nicht ausdrücklich, in welcher Form die Daten bereitzustellen sind. Möglich ist zunächst ein bloßer Lesezugang im Internet: Daneben besteht die Möglichkeit eines Push-Zugriffs. Der Datenlieferant versendet in diesem Fall die für den Empfänger relevanten Daten selber an den Empfänger. Eine weitere Möglichkeit besteht im Pull-Zugriff. Dabei zieht sich der Empfänger, die für ihn relevanten Daten, aktiv über eine Schnittstelle auf sein Endgerät.

Die Fahrzeughersteller ermöglichen in der Praxis jedoch häufig nur einen Lesezugriff im Internet in einer Form, die es den Akteuren auf dem Automotive-Aftermarket nicht ermöglicht, die Daten weiter zu verarbeiten. Hierdurch erleiden die Akteure in tatsächlicher Hinsicht maßgebliche Wettbewerbsnachteile. Aus diesem Grund klagte der Aftermarket auf uneingeschränkten Zugriff auf die Daten in weiterverarbeitbarer Form (EuGH Urt. v. 19. September 2019, C-527/18, GRUR 2019, 1196).

Diese Problematik wurde zwischenzeitlich durch Inkrafttreten der EU-Verordnung Nr. 2018/858 entschärft. Art. 61 der neuen Verordnung sieht nunmehr vor, dass die Angaben in elektronisch verarbeitbaren Datensätzen darzubieten sind. Die ab September 2020 anwendbare Regelung trägt dem Umstand Rechnung, dass auch die genaue Art des Zugangs für einen funktionierenden Wettbewerb von erheblicher Bedeutung ist. Sie gilt insoweit als ein aktuelles Musterbeispiel für regulatorisch gewährten Zugang zu Daten.

4.2.3 Konditionen für einen Zugang

Auch die Bedingungen, zu denen der Zugang zu Daten ermöglicht wird, sind kartellrechtlich relevant. Die Gestaltung der Bedingungen darf im Einzelfall nicht dazu führen, dass die Möglichkeit des Zugangs in der Praxis nicht in Anspruch genommen werden kann. Prohibitive Bedingungen, etwa das Verlangen eines hohen Entgelts für die Zugangsgewährung haben im Ergebnis die gleiche Wirkung wie eine Zugangsverweigerung.

In diesem Zusammenhang können die sogenannten FRAND-Grundsätze eine Orientierungshilfe bieten (EU Commission, free flow of data, COM (2017) 2 final, S. 3). Diese Grundsätze werden bei der Gestaltung und Überprüfung von Bedingungen für die Lizenzierung sogenannter standardessenzieller Patente angewandt. Dabei handelt es sich um Patente, die zwingend genutzt werden müssen, um einem definierten Standard entsprechen zu können. Solche Standards sind beispielsweise im Telekommunikationssektor verbreitet und fördern technische Entwicklungen. Ein Hauptanwendungsfall sind der UMTS oder LTE Standard. Kein Mobilfunkanbieter wäre sinnvoll in der Lage Mobiltelefone anzubieten, wenn diese nicht dem Standard entsprechen. Auch andere Akteure sind in der Praxis häufig darauf angewiesen, dass ihre Produkte den Standards entsprechen. Aus diesem Grund sind Inhaber standardessenzieller Patente verpflichtet, ihre Schutzrechte an andere Akteure zu lizenzieren. Damit diese Möglichkeiten auch tatsächlich genutzt werden können, müssen die Lizenzierungsbedingungen aber angemessen sein.

Diese Überlegungen sind auch im Rahmen anderer kartellrechtlicher Zugangsansprüche relevant. Aus diesem Grund lassen sich die FRAND-Grundsätze grundsätzlich auch auf die Konditionen übertragen, die bei kartellrechtlichen Zugangsansprüchen zu Daten Anwendung finden.

► **Praxistipp** Die in letzter Zeit vor allem im Patentrecht wichtigen FRAND-Grundsätze lassen sich ohne weiteres auf den Zugang zu Daten übertragen. Im Unterschied zur Benutzung von Patenten besteht die zusätzliche Herausforde-

rung allerdings darin, dass die Nutzung der Daten in der Regel erst aufgenommen werden kann, nachdem der Dateninhaber den Zugang zur Datenquelle auch physisch gewährt. Die FRAND-Grundsätze können daher zwar für die Bemessung etwaiger Nutzungsentgelte herangezogen werden, insbesondere wenn es um Zugriff auf urheberrechtlich oder patentrechtlich geschützte Daten geht. Eine unmittelbare Anwendung des FRAND-Einwandes zur Rechtfertigung der Datennutzung scheidet aus praktischen Gründen aber meist aus, weil der interessierte Nutzer de facto keinen Zugang zu den Daten hat. In diesem Fall muss also zunächst auf Zugangsgewährung geklagt werden.

Die Zugangsbedingungen sind dann **FRAND**, wenn sie „**fair, reasonable and non-discriminatory**" sind. Wie solche angemessenen Bedingungen in der Praxis aussehen, ist einzelfallabhängig. Die Bedingungen sollen wettbewerbsanalog sein und die faktische Monopolposition des Dateninhabers „herausfiltern". Insofern genügt es nicht, dass jedem Akteur die gleichen unangemessenen Bedingungen vorgelegt werden, sodass eine Diskriminierung einzelner Akteure ausgeschlossen ist. Vielmehr ist zu ermitteln, welche Vertragsbedingungen sich bei funktionierendem Wettbewerb durchsetzen würden.

Die FRAND-Grundsätze spielen insbesondere bei der Berechnung der Höhe der Gegenleistung eine entscheidende Rolle; auch der zu zahlende Preis muss wettbewerbsanalog sein. Die Berechnung der angemessenen Höhe kann mithilfe anerkannter ökonomischer Ansätze erfolgen. Hierzu zählen Methoden, wie die Berechnung der Höchstbelastungsgrenze, die Preis-Kosten-Schere, sowie das Vergleichsmarktkonzept.

Die Bedingungen und Preise des Datenzugangs können dabei im Einzelfall durchaus variieren, sofern sie einzelne Akteure nicht diskriminieren, sondern auf die unterschiedlichen Gegebenheiten Rücksicht nehmen. Auch ist anerkannt, dass der Verpflichtete einen gewissen Spielraum bei der Gestaltung der Konditionen hat, da eine Vielzahl verschiedener Gestaltungen den FRAND-Grundsätzen entsprechen kann. In der Rechtsprechung haben sich bislang keine konkreteren Anhaltspunkte dazu herausgebildet, wie eine angemessene Gestaltung des Datenzugangs aussehen könnte. Ein wesentlicher Unterschied zur FRAND-Lizenzierung von Patenten kann sich indessen daraus ergeben, dass Datensammlungen nicht automatisch urheberrechtlich geschützt sind (siehe hierzu im Detail Kap. 3). Die Frage nach dem angemessenen Preis wirft daher insbesondere bei automatisch generierten Maschinendaten erhebliche Probleme auf, die keinem Schutzrecht unterliegen, sondern allein der faktischen Datenherrschaft des Maschinennutzers oder des Herstellers. Auf Daten die durch KI-Lösungen generiert werden kann dies entsprechend zutreffen, wenn die Investition in die KI-Lösung allein noch nicht ausreicht um Datenbankschutzrechte zu begründen. Gerade bei Maschinendaten wird sich zudem das Problem der „sole-source"-Datenbanken verstärkt stellen, dass nämlich die Daten nur aus einer Quelle verfügbar sind und das Herstellerrecht daher – entgegen der Intention des Gesetzgebers – faktisch eine Monopolstellung an den Daten selbst vermittelt (Wiebe, GRUR 2017, S. 338).

Bei personenbezogenen Daten kommen Marktmacht und Zugangsansprüche hingegen regelmäßig bereits deshalb nicht infrage, weil sich die Wettbewerber selbst einen eigenen

Datenbestand hierzu zumutbar aufbauen können. Kommt in anderen Fällen eine Zwangslizenz auf Daten in Betracht, stellen sich naturgemäß Folgefragen über die konkrete Ausgestaltung des Datenzugangsverhältnisses. Im Ergebnis geht es hier um die konkreten Bedingungen eines Datenlizenzvertrags. Dabei können dann unter Umständen auch Selbstverpflichtungen der Dateninhaber eine Rolle spielen, insbesondere eine FRAND-Unterwerfung, wie sie die Europäische Kommission in ihrem Paper „Building an European Data Economy" auch für Standardisierungsinitiativen für Zugangsverhältnisse zu Daten diskutiert (Louven Datenmacht und Zugang zu Daten, NZKart 2018, 217, 222; COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy (SWD (2017) 2/1)).

4.2.4 Ausblick und Zusammenfassung

Der Zugang zu Daten ist in der Regel ein wesentlicher Bestandteil für den Geschäftserfolg in der digitalen Ökonomie. Dort wo zudem Netzwerkeffekte eine Rolle spielen (z. B. bei Plattformen) ist das Verhältnis zwischen Datenmenge und Nutzen nicht linear sondern exponentiell, so dass – selbst bei Replizierbarkeit der Daten – der Wettbewerb bestimmte Größenvorteile ab einem bestimmten Punkt nicht mehr aufholen kann und der Markt zu Gunsten eines Marktteilnehmers kippt. Gerade im Bereich IoT sind Daten schon nicht replizierbar und der Zugang hierzu ist zwingend erforderlich, um auf Komplementärmärkten aktiv werden zu können (z. B. für **predicitve maintenance** bei Wartungs- und Reparaturleistungen). Unter dem derzeit geltenden Rechtsrahmen fällt es mitunter nicht leicht einen Anspruch auf Zugang zu Datensätzen eines Dritten erfolgreich durchzusetzen.

Dass die Bedeutung von Daten für die digitale Ökonomie in der KI eine bedeutende Säule ist, haben auch Kartellbehörden und Gesetzgeber verstanden und daher für die anstehende 10. GWB-Novelle einige Änderungsvorschläge in Bezug auf die Bedeutung und den Zugang zu Daten mit aufgenommen:

- Zum einen soll klargestellt und gesetzlich verankert werden, dass der Zugang zu Daten ein Bewertungskriterium für die Marktmacht eines Unternehmens ist;
- Zum anderen und insbesondere soll die Verweigerung des Zugangs zu Daten als ausdrückliche Fallgruppe des Marktmachtmissbrauchs geregelt werden. Damit sollen die zuvor dargestellten derzeit noch hohen Anforderungen der Essential Facilities Doktrin, die ursprünglich nur für physische Zugangsansprüche zu Infrastruktureinrichtungen entwickelt wurde, gesenkt werden. Voraussetzung für diesen neuen Anspruch soll sein, dass der Datenzugang notwendig ist, um auf einem vor- oder nachgelagerten Markt tätig zu sein und dass die Lieferverweigerung den wirksamen Wettbewerb auf diesem Markt auszuschalten droht. Hierdurch soll der Wettbewerb insbesondere auf den nachgelagerten Märkten (wie z. B. den Wartungs- und Reparaturleistungen in Form von predictive maintenance in allen IoT-Bereichen wie bspw. Windenergieanlagen oder Kfz-Sekundärmärkten) zu dem Datensatz-besitzenden Marktbeherrscher sichergestellt werden. Damit gäbe es erstmalig einen gesetzlich geregelten Datenzugangsanspruch.

4.3 Urheberrecht

Die kartellrechtlichen Überlegungen finden auch im Urheberrecht Anwendung. So können Schutzrechtsinhaber entsprechend der Essential Facilities-Doktrin verpflichtet werden, urheberrechtliche Zwangslizenzen zu erteilen. Neben spezialgesetzlichen Regelungen, wie § 42a UrhG für die Herstellung von Tonträgern, können sich solche Zwangslizenzen auch aus den in der Rechtsprechung entwickelten Kriterien ergeben.

Dabei handelt es sich um Sachverhaltskonstellationen, in denen die Nutzung von urheberrechtlich geschützten Werken, vornehmlich Datenbanken und Computerprogrammen, Voraussetzung für den nachgelagerten Markt ist. Datenbanken und Computerprogramme sind oftmals nicht nur Gegenstand des (vorgelagerten) Lizenzierungsmarktes, sondern häufig auch auf nachgelagerten Produktmärkten nachgefragt, die von der Interoperabilität oder Nutzung des urheberrechtlich geschützten Werkes abhängen. Hat der Schutzrechtsinhaber eine große Marktmacht auf dem vorgelagerten Markt, kann er durch Verweigerung einer Lizenzerteilung in bestimmten Fällen einen Wettbewerb auf den nachgelagerten Märkten verhindern.

Ein Beispiel für eine solche Konstellation ist ein Produkt, das mit gängigen Computerprogrammen kompatibel sein muss, um von den potenziellen Kunden genutzt werden zu können. Die Verweigerung einer Lizenzierung des Computerprogramms bzw. die Verweigerung der Offenlegung der Schnittstellen kann unter bestimmten Voraussetzungen in kartellrechtlicher Hinsicht missbräuchlich sein, sofern hierdurch jegliche Konkurrenztätigkeiten auf dem nachgelagerten Markt verhindert werden.

Aus urheberrechtlichen Regelungen ergeben sich in engen Grenzen ebenfalls Zugangsrechte. Insbesondere kann der Inhaber einer urheberrechtlich geschützten Datenbank nicht verbieten, dass Nutzer die Datenbank konsultieren und sich entsprechend informieren, sofern er diese im Internet verfügbar gemacht hat. Anderslautende vertragliche Beschränkungen in den Nutzungsbedingungen der Webseite sind gemäß § 87e UrhG unwirksam. Große Bedeutung im Kontext der KI hat zudem die Analyse von Big Data und damit die Gestattung des data mining umfangreicher Datensätze (siehe hierzu im Detail Kap. 3). Ähnliches gilt für Schnittstelleninformationen zu Computerprogrammen. Auch hier sind Abreden unwirksam, die es dem Wettbewerber verbieten maschinenlesbaren Objektcode (des Objektprogramms) zur Herstellung von Interoperabilität in den für den Menschen lesbaren Quellcode zurückzuübersetzen (§ 69g Abs. 2), beispielsweise um eine KI-Software anzubinden.

► **Praxistipp** Insbesondere bevor Inhalte online zugänglich gemacht werden, sollten Sie sorgfältig prüfen, ob Sie diese tatsächlich dauerhaft zugänglich machen wollen. Gegen die Konsultation der Inhalte durch Dritte bestehen anschließend ebenso wenig Ansprüche, wie gegen die Kopie unwesentlicher Teile der Datenbank (siehe dazu auch Kap. 3.1.2). Nach der Rechtsprechung können dies bis zu ca. 10 % des Inhaltes bei quantitativer oder qualitativer Wertung sein. Bei Zugänglichmachung im Rahmen einer Datenlizenz können vertraglich engere Regelungen getroffen werden. Auch hier sollten Sie aber bedenken, dass gegen die

urheberrechtlichen Grundwertungen verstoßende Regelungen unwirksam sein können. Umgekehrt können Dritte unter Umständen Gleichbehandlung bei der Lizenzerteilung verlangen (kartellrechtliches Diskriminierungsverbot).

Der EuGH hat Kriterien entwickelt, aus denen sich die Missbräuchlichkeit einer Lizenzverweigerung und folglich ein Anspruch auf Erteilung einer Zwangslizenz ergeben können.

Voraussetzung ist, dass die Nutzung des geschützten Werkes unerlässlich ist, um auf dem nachgelagerten Markt ein neues Produkt anbieten zu können. Für dieses neue Produkt muss aber auch eine potenzielle Nachfrage bestehen. Zudem darf es für die Verweigerung einer Lizenzerteilung keine sachliche Rechtfertigung geben. Zuletzt ist auch erforderlich, dass der Wettbewerb auf dem nachgelagerten Markt durch die „Verknüpfung" des vor- und nachgelagerten Marktes ausgeschaltet wird.

Diese Voraussetzungen erfüllt ein potenzieller Anbieter aber nicht, wenn er kein „neues" Produkt anbieten möchte, sondern lediglich bezweckt, als Konkurrent des Schutzrechtsinhabers auf dem nachgelagerten Markt aufzutreten. In einem solchen Fall hat der EuGH (EuGH Rs. C-418/01 – IMS Health) einen Anspruch auf Erteilung einer Zwangslizenz für die Nutzung einer geschützten Datenbank verneint. Zwar hatte sich die streitgegenständliche Datenbankstruktur zu einem gängigen Format entwickelt, auf das die Prozesse der Kunden abgestimmt wurden. Dadurch waren auch potenzielle Konkurrenten von der Einbeziehung der Datenbank abhängig. Dennoch überwogen die Interessen des Schutzrechtsinhabers, da der potenzielle Anbieter keine Verbesserung oder Entwicklung des vorhandenen Produktes anbieten wollte und mit seinem Konkurrenzprodukt daher auch keine potenzielle Nachfrage bedient hätte. Vielmehr konnte der Schutzrechtsinhaber die Nachfrage mit seinem Produkt hinreichend abdecken, sodass kein Bedürfnis für ein unverändertes Konkurrenzprodukt bestand. Das Erfordernis des „neuen Produktes" wird in der Literatur kritisiert, da kleinere Innovationen durch diese Voraussetzung erschwert würden. Dennoch genügt im Grundsatz das Anbieten eines bloßen unveränderten Konkurrenzproduktes nicht, um einen Anspruch auf Erteilung einer Zwangslizenz zu begründen.

Besteht aber ein Anspruch auf Erteilung einer Zwangslizenz, müssen die Bedingungen der Lizenzerteilung angemessen sein. Anhaltspunkte für die Gestaltung angemessener Bedingungen, können die FRAND-Grundsätze bieten.

4.4 Fazit

Die Bedeutung von Daten für die digitale Ökonomie ist fraglos. Für einen funktionierenden Wettbewerb ist daher ein angemessener Zugang der Marktteilnehmer zu den erforderlichen Daten notwendig. Hierbei ist sowohl das Kartellrecht, als auch das Urheberrecht und vereinzelte sektorspezifische Regulierungen behilflich. Denn bereits heute haben Unternehmen die Möglichkeit auf dieser Grundlage Datenzugangsansprüche erfolgreich durchzusetzen. Zugegeben sind die Voraussetzungen hierfür vereinzelt nicht zu vernachlässigen, aber die Bedingungen dürfen in der Zukunft durch anstehende Gesetzesänderungen noch günstiger werden.

Literatur

Bundeskartellamt (2016) Arbeitspapier – Marktmacht von Plattformen und Netzwerken

Europäische Kommission, COM (2017) 2 final – 144/17-Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Aufbau einer europäischen Datenwirtschaft

Europäische Kommission, SWD (2017) 2 final – COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy

Körber T (2016) „Ist Wissen Marktmacht?“ Überlegungen zum Verhältnis von Datenschutz, „Datenmacht“ und Kartellrecht – Teil 1. NZKart 2016:303–310

Louven S (2018) Datenmacht und Zugang zu Daten. NZKart 2018:217–222

Wiebe A (2017) Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken. GRUR 2017:338–345

Eigentum an Daten

5

Sabine von Oelffen

Zusammenfassung

In diesem Kapitel wird die Regelungsalternative „Eigentum an Daten“ näher beleuchtet. Stand heute besteht kein gesetzliches Eigentumsrecht an Daten. Ob eine absolute Eigentumsposition an Daten geschaffen werden sollte, ist Gegenstand politischer und juristischer Diskussion. Da die Wissenschaft einem neuen „Eigentumsrecht“ eher ablehnend begegnet, werden zudem alternative Regelungsvorschläge vorgestellt, die in Reaktion auf die besonderen datenspezifischen Anforderungen entwickelt wurden.

Sowohl im Hinblick auf Maschinengenerierte Daten als auch im Hinblick auf Personenbezogene Daten bzw. gemischte Datensätze aus maschinengenerierten und personenbezogenen Daten stellt sich die Frage, ob gesetzliches Eigentum an Daten (vergleichbar beispielsweise mit gesetzlichem Eigentum an einer Immobilie) bestehen sollte. Ein wie auch immer ausgestaltetes Eigentumsrecht an Datensätzen, die jedenfalls auch Personenbezogene Daten enthalten, müsste dabei in jedem Fall der DS-GVO Vorrang gewähren. Im Folgenden erhalten Sie einen Überblick über die aktuelle Rechtslage und den Diskussionsstand zu diesem Thema.

Aktuell besteht kein Eigentum und auch kein anderweitiges Ausschließlichkeitsrecht an unverkörperten Daten.[1] Personen und Unternehmen, die faktisch Inhaber von Daten-

[1] Zum wirtschaftlichen Eigentum an immateriellen Wirtschaftsgütern wie Software, vgl. Kap. 7, Abschn. 7.1.2.2.

S. Oelffen (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: sabine.vonoelffen@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_5

sätzen sind, haben daher kein absolutes, d. h. gegenüber jedermann wirkendes, Recht, Dritte von dem Zugriff auszuschließen oder die Daten exklusiv zu verwerten. Rechtlicher Hintergrund ist, dass Daten keine körperlichen Gegenstände i.S.d. § 90 **Bürgerliches Gesetzbuch** (**BGB**) und somit nicht eigentumsfähig sind[2] (Mitterer et al. 2017, S. 6). Rechte an Daten bestehen daher lediglich punktuell, z. B. in Form eines Rechts des Datenbankherstellers an einer durch seine Investition erstellten Datenbank i. S. v. §§ 87a ff. UrhG (Mitterer et al. 2017, S. 6). Daten können zudem als „sonstige Gegenstände" i.S.d. § 453 BGB Subjekt schuldrechtlicher Rechtsgeschäfte sein (Ellenberger 2020, § 90 Rn. 2). Wird mit Daten gehandelt, räumt der Datengeber lediglich vertraglich eine faktische Rechtsposition ein. Der Datenbezieher wird aufgrund der fehlenden Möglichkeit der Verschaffung einer absoluten Rechtsposition nicht Eigentümer der Daten (Paal und Hennemann 2017, S. 1698), sondern erlangt lediglich tatsächlichen Zugang zu den Daten.

Aktuell wird auf deutscher[3] und europäischer Ebene diskutiert, ob gesetzliche Rechte an Daten geschaffen werden sollten. So wurde im Kontext des Verordnungsvorschlags und der späteren Umsetzung als Verordnung 2018/1807/EU über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (Kap. 10) ein Datenerzeugerrecht erwogen, welches das bereits bestehende „*de facto*" Eigentumsrecht untermauern und im Sinne eines Abwehrrechts schützen würde (Europäische Kommission 2017, S. 11 und 14; Wiebe 2017, S. 88–89). Die finale Fassung der Verordnung 2018/1807/EU sieht jedoch kein Eigentumsrecht an Daten vor, was auch nicht überrascht, da der Fokus dieser Verordnung nicht auf der Schaffung von Dateneigentum, sondern auf der Gewährleistung des freien Verkehrs von Daten innerhalb der EU liegt. Die noch im Koalitionsvertrag zur aktuellen Legislaturperiode aufgeworfene Frage, ob und wie Eigentum an Daten ausgestaltet werden sollte und könnte (Bundesregierung 2018, S. 129), wird wohl dahingehend beantwortet werden, dass kein „echtes" neues Eigentumsrecht geschaffen wird.

Im juristischen Schrifttum wird die Frage, ob ein gesetzliches Eigentumsrecht an Daten geschaffen werden sollte oder nicht, nach wie vor kontrovers diskutiert. Nicht immer geht dabei aus den Beiträgen klar hervor, ob sich die Verfasser nur auf Maschinengenerierte oder auch auf personenbezogene Daten beziehen. Die mittlerweile überwiegende Ansicht spricht sich inzwischen gegen die Schaffung eines eigentumsgleichen Ausschließlichkeitsrechts aus (Fries und Scheufen 2019, S. 726, dort m. w. N. Fußnote 31).

Befürworter eines gesetzlichen Datenerzeuger- oder Datenproduzentenrechts sehen die Möglichkeit, dem Erzeuger der Rohdaten ein gesetzliches Recht an Daten zuzusprechen (Fezer 2017, S. 103). Durch ein gewerbliches Schutzrecht an Daten beispielsweise, würde ein Anreiz entstehen, Daten zu produzieren und zu vermarkten. Zwar scheine es zurzeit so, als ob auch ohne ein solches Recht bereits große Mengen an Daten produziert werden, jedoch könnte ein Recht an Daten einen Anreiz für neue Geschäftsmodelle setzen oder den Zugang zu oder die Qualität der Daten verbessern (Wiebe 2016, S. 881). Außerdem könne ein solches Recht Ordnung auf dem Datenmarkt schaffen. Derzeit werden möglichst viele Daten von

[2] BGH 13. Oktober 2015, NJW 2016, 1094, Rz. 20.

[3] Siehe zum Meinungsstand und unterschiedlichen Zuordnungskriterien Vogt 2019, S. 77–80.

Internet-Unternehmen gesammelt und ohne Einschränkung gehandelt. Bei einem Recht an den Daten würde sich ein Unternehmen wohl überlegen, wie viele Daten mit welcher Qualität es erwerbe. Der Markt könnte dadurch effizienter werden (Wiebe 2016 S. 881). Im Ergebnis argumentiert dafür auch Ensthaler (2016, S. 3476), wenn auch lediglich in wirtschaftlicher Hinsicht. Ensthaler schlägt hierbei folgendes System der Zuordnung Maschinengenerierter Daten vor: Wer aus Datenanalysen aus Rohdaten neue Maschinengenerierte Daten gewinnt, ist Datenhersteller; der Inhaber der Ausgangs- bzw. Rohdaten hat sodann gemäß § 951 BGB analog einen Anspruch auf Entschädigung in Geld. Dieser Vorschlag setzt gedanklich ein eigentumsähnliches Recht des Inhabers der Rohdaten voraus. Ensthaler lehnt jedoch ein Ausschließlichkeitsrecht an Maschinengenerierten Daten ab und möchte letztlich nur die wirtschaftlichen Folgen der Weiterverarbeitung der Rohdaten regeln. Der Inhaber der Rohdaten hat nach diesem Konzept nicht die Möglichkeit, die Datenverwertung zu unterbinden.

Die überwiegende Mehrheit juristischer Autoren spricht sich inzwischen gegen die Schaffung von Dateneigentum aus. So argumentieren Kühling und Sackmann, dass der Inhaber (erzeugter) Daten zumindest im Hinblick auf die Ausschließungsfunktion bereits durch § 202a **Strafgesetzbuch** (**StGB**) geschützt sei. Im Kern sei der strafrechtliche Schutz der tatsächlichen Herrschaft an neu erzeugten Daten durch § 202a StGB („Ausspähen von Daten“) genau das, was vielfach unter dem Ausschließlichkeitsrecht an Daten bzw. „Dateneigentum“ diskutiert werde. Wenn untersagt wird, dass sich Unbefugte Zugriff verschaffen, setze dies einen Berechtigten voraus. Setzt der Berechtigte technische Sicherungsmaßnahmen ein, so genießen diese Sicherungsmaßnahmen strafrechtlichen Schutz (Kühling und Sackmann 2020, S. 28). Diese strafrechtliche Argumentation überzeugt nur bedingt, da das Strafrecht nicht in erster Linie dazu dient, zivilrechtliche Rechtspositionen durchzusetzen. Weiter argumentieren Kühling und Sackmann, dass die generierten Daten durch technische Zugangsbarrieren und vertragliche Regelungen ausreichend vor dem Zugriff durch die Endnutzer geschützt werden könnten. So verlöre beispielsweise ein Endnutzer, der unerlaubte Modifizierungen an einem System vornimmt, um sich unberechtigt Zugang zu den Daten zu verschaffen, seine Gewährleistungsrechte in Bezug auf das System. Aus diesen Gründen mangele es nicht am Schutz des Erzeugers (Kühling und Sackmann 2020, S. 28). Zudem bestünde bei Einräumung von Ausschließlichkeitsrechten die Gefahr der Monopolbildung und einer Lähmung der Informationsgesellschaft (Kühling und Sackmann 2020, S. 29).

Auch Determann lehnt Ausschließlichkeitsrechte an Daten im Ergebnis unter anderem mit dem Argument ab, dass dies nicht der richtige Innovationsanreiz wäre, sondern hierdurch vielmehr Innovationen behindert würden (Determann 2018, S. 508). Gegen auf letztlich wirtschaftlichen Überlegungen basierende Zuordnungsmethoden für Rechte an Maschinengenerierten Daten wendet Vogt zudem zu Recht ein, dass es kein einzelnes wirtschaftliches Zuordnungskriterium gibt, welches allen Einzelfällen gerecht wird (Vogt 2019, S. 80). Auch Fries und Scheufen sehen den Zugang zu Daten als für die Zukunft wichtig an. Nur so könnten KI-Lernprozesse und datenbasierte Produktinnovationen ermöglicht werden. Es müsse daher insbesondere durch wettbewerbsrechtliche Instrumente eine Balance geschaffen werden zwischen dem Interesse von Dateninhabern an Aus-

schließlichkeit und dem Interesse anderer Stakeholder an Datenzugang. Vertragliche Gestaltungsmöglichkeiten in Verbindung mit der Anwendung und Verschärfung des europäischen Wettbewerbsrechts auch auf die großen Oligopole aus den USA seien daher zukunftsträchtige Lösungen für rechtliche Fragen des Datenaustauschs. Die besondere Grenzkostenstruktur von maschinengenerierten Daten (die zusätzlichen Kosten für ein weiteres Datum, nachdem die Erhebungsmechanismen (kostenaufwendig) geschaffen wurden, sind nämlich marginal) führe dazu, dass die Anreizfunktion, die ein Eigentumsrecht rechtsökonomisch verfolge, nicht greife. Zudem seien die Gefahren, die mit Marktmacht einhergehen, wesentlich intensiver, wenn dem jeweiligen mächtigen Akteur unbegrenzte Ausschließungsrechte zustehen (Fries und Scheufen 2019, S. 725 f.).

Auch das Max-Planck-Institut für Innovation und Wirtschaft sieht keine Notwendigkeit, gesetzliche Ausschließlichkeitsrechte an Daten zu schaffen (Drexl et al. 2016, S. 915). Es bestehe kein Grundsatz, wonach Rechte an Daten von vornherein einem bestimmten Rechtssubjekt zuzuweisen wären (Drexl et al. 2016, S. 914; Drexl 2017, S. 339). Kürzlich hat auch das OLG Brandenburg eine analoge Anwendung der Regelungen des BGB zum Besitzschutz mit dem Argument abgelehnt, dass Daten sich anders als körperliche Gegenstände durch ihre Nicht-Rivalität, Nicht-Exklusivität und Nicht-Abnutzbarkeit auszeichnen.[4] Auch wenn sich das Urteil mit Fragen des Besitzschutzes und nicht des Eigentums befasst, lässt sich aus der Urteilsbegründung schließen, dass das Gericht ein Eigentum an Daten nicht nur als aktuell nicht existent, sondern auch als nicht geboten ansieht.

Im Ergebnis ist daher nicht zu erwarten, dass in naher Zukunft gesetzliche Ausschließlichkeitsrechte an Daten geschaffen werden. Daher sollten Sie Rechte an (Maschinengenerierten) Daten vertraglich regeln. Die vertragliche Zuordnung von Rechten an Maschinengenerierten Daten hat durchaus Vorteile, insbesondere den eines flexiblen Systems, welches mit dem technischen Fortschritt wächst (Vogt 2019, S. 80). Prüfen Sie hierbei stets, ob wirklich nur Maschinengenerierte Daten Vertragsgegenstand sind oder ob (auch) personenbezogene Daten vorliegen. In letzterem Fall sind die Regelungen der DS-GVO zu beachten. Denken Sie daran, dass vertragliche Vereinbarungen keine Wirkung gegenüber Dritten, die nicht Vertragspartei sind, entfalten. Im Rahmen des wettbewerbsrechtlich und kartellrechtlich Zulässigen kann der Schutz vor (unberechtigtem) Zugriff durch Dritte auch durch die Herstellung ausschließlicher faktischer Zugriffsmöglichkeiten mittels entsprechender technischer Maßnahmen bewirkt werden.

Literatur

Bundesregierung (2018) „Ein neuer Aufbruch für Europa – Eine neue Dynamik für Deutschland – Ein neuer Zusammenhalt für unser Land“ – Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode. https://www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906. Zugegriffen am 18.03.2020

[4] OLG Brandenburg 6. November 2019, NJW-RR 2020, 54, Rz. 44.

Determann L (2018) Gegen Eigentumsrechte an Daten – Warum Gedanken und andere Informationen frei sind und es bleiben sollten. ZD 2018:503–508
Drexl J (2017) Neue Regeln für die europäische Datenwirtschaft? – Ein Plädoyer für einen wettbewerbspolitischen Ansatz- Teil 1. NZKart 2017:339–344
Drexl J, Hilty R, Desaunettes L, Greiner F, Kim D, Richter H, Surblytė G, Wiedemann K (2016) Ausschließlichkeits- und Zugangsrechte an Daten – Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb vom 16.8.2016 zur aktuellen europäischen Debatte. GRUR Int 2016:914–918
Ellenberger J (2020) In: Palandt O (Hrsg) Bürgerliches Gesetzbuch: BGB, 79. Aufl. Verlag C.H. Beck, München
Ensthaler J (2016) Industrie 4.0 und die Berechtigung an Daten. NJW 2016:3473–3478
Europäische Kommission (2017) Mitteilung der Kommission an das Europäische Parlament, Den Rat, Den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – „Aufbau einer Europäischen Datenwirtschaft". https://ec.europa.eu/transparency/regdoc/rep/1/2017/DE/COM-2017-9-F1-DE-MAIN-PART-1.PDF. Zugegriffen am 18.03.2020
Fezer K-H (2017) Dateneigentum der Bürger. ZD 2017:99–105
Fries M, Scheufen M (2019) Märkte für Maschinendaten. MMR 2019:721–726
Kühling J, Sackmann F (2020) Irrweg „Dateneigentum". ZD 2020:24–30
Mitterer K, Wiedemann M, Zwissler T (2017) BB-Gesetzgebungs- und Rechtsprechungsreport zu Industrie 4.0 und Digitalisierung. BB 2017:3–13
Paal B, Hennemann M (2017) Wettbewerbs- und daten(schutz)rechtliche Herausforderungen. NJW 2017:1697–1701
Vogt A (2019) Automatisch meins? – Die Rechte an maschinengenerierten Daten. Bonner Rechtsjournal 2019:77–80
Wiebe A (2016) Protection of industrial data – a new property right for the digital economy? GRUR Int. 2016:877–884
Wiebe A (2017) Von Datenrechten zu Datenzugang, ein rechtlicher Rahmen für die europäische Datenwirtschaft. CR 2017:87–93

Wertschöpfung mittels KI (insbesondere aus Daten)

6

Johannes Graf Ballestrem

Zusammenfassung

Bei Einsatz von KI in der Wertschöpfungskette stellen sich rechtliche Zuordnungs- und Haftungsfragen.

Wer haftet, wenn es bei dem Einsatz von KI zu Schäden an Gegenständen oder sogar Menschen kommt? Hier ist insbesondere die Haftung nach dem Produkthaftungsgesetz (ProdHaftG) und die richterrechtlich entwickelte Produzentenhaftung im Rahmen des deliktischen § 823 Abs. 1 BGB von Bedeutung.

Was sind die Rechtsfolgen, wenn die KI absichtlich oder unbeabsichtigt auf Datensätze zugreift, die einem Dritten „gehören"?

Und wie können die schöpferischen und technischen Leistungen von KI vor Nachahmern geschützt werden? Dabei stellen sich sowohl im Patent- als auch im Urheberrecht jeweils zwei zentrale Fragen: Zum einen, ob der Algorithmus, welcher der KI zugrunde liegt, durch Patent- und/oder Urheberrechte geschützt werden kann. Zum anderen wird diskutiert, ob KI selbst Leistungen schaffen kann, die durch diese Rechte geschützt werden.

6.1 Produkthaftung und Produzentenhaftung beim Einsatz von KI

Beim Einsatz von KI stellen sich vielfältige Haftungsfragen für den Fall, dass es dabei zu Schäden an Gegenständen oder sogar Menschen kommt. Da ein System künstlicher Intelligenz jedoch nach aktueller Rechtslage weder eigene Rechtspersönlichkeit besitzt noch

J. G. Ballestrem (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: johannes.ballestrem@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_6

ein eigenständiges Haftungssubjekt ist bzw. eine eigene Haftungsmasse darstellt (siehe zu Erwägungen in Bezug auf mögliche Änderungen des Rechts hinsichtlich dieser Aspekte auf europäischer Ebene die Ausführungen unter Kap. 11), kann eine aus dem KI-Einsatz resultierende Haftung nur auf eine menschliche (oder jedenfalls juristische) Person zurückgeführt werden. Neben den vielfältigen vertraglichen Haftungsmöglichkeiten kommt auch eine vertragsunabhängige Haftung in Betracht. Hier ist insbesondere die Haftung nach dem **Produkthaftungsgesetz** (**ProdHaftG**) und die richterrechtlich entwickelte Produzentenhaftung im Rahmen des deliktischen § 823 Abs. 1 BGB von Bedeutung. Zentrale Frage einer jeden Haftung ist jedoch, ob sich eine KI derart eigenständig fortentwickeln kann, dass jegliche Zurechnung zu einer natürlichen oder juristischen Person verloren geht.

Bei der Haftung für Schäden muss zwischen einer verschuldensabhängigen und einer verschuldensunabhängigen Haftung, sog. Gefährdungshaftung, unterschieden werden. Das deutsche Zivilrecht geht grundsätzlich von einer verschuldensabhängigen Haftung aus, die an ein menschliches Verhalten – entweder in Form eines aktiven Tuns oder in Form eines Unterlassens von Verkehrssicherungspflichten – anknüpft. Nur ausnahmsweise ist eine Gefährdungshaftung für speziell definierte Fallkonstellationen vorgesehen.

▶ **Praxistipp** Die Haftung für mögliche KI-Fehler richtet sich primär nach dem vertraglichen Verhältnis. Im Regelfall ist diese vertragliche Haftung nicht gegeben, wenn sich der Anbieter der KI entlasten kann, weil er bei der Programmierung die notwendige Sorgfalt hat walten lassen. Unabhängig von der vertraglichen Konstellation können Anbieter und Verwender der KI allerdings dennoch Ansprüche aus Deliktsrecht oder der sogenannten Gefährdungshaftung treffen. Für diese Fälle ist ein passender betrieblicher Versicherungsschutz besonders wichtig.

6.1.1 Verschuldensabhängige Haftung

Die verschuldensabhängige Haftung knüpft an das Verhalten der handelnden Person an. Als solche kommen bei Einsatz von KI der Hersteller, Eigentümer und Nutzer in Betracht. Soweit diese Akteure nicht aktiv handeln, d. h. den Schaden selbst aktiv (durch ihre letzte menschliche Handlung) herbeiführen – woran es bei zunehmend komplexerer, selbstlernender KI häufig scheitern könnte[1] –, muss der Person demnach in irgendeiner Weise mangelnde Sorgfalt vorgeworfen werden können. Die verschuldensabhängige Haftung wird hier häufig auf ihre Grenzen stoßen, da das selbstlernende Verhalten der KI für deren Her-

[1] Ein möglicher Anknüpfungspunkt wäre der Nachweis einer fehlerhaften Programmierung, die gerade ursächlich für den eingetretenen Schaden war und – z. B. durch Protokolle oder Logdateien – von dem Geschädigten nachgewiesen werden kann. Grützmacher (2016, S. 697) sieht hier zukünftig aufgrund der Datenmassen Beweisprobleme.

[2] Ebenso kritisch und als „unbefriedigenden Zustand" bezeichnet dies Graf v. Westphalen (2018, S. 19).

steller und/oder Nutzer häufig nicht vorhersehbar sein wird und den in Anspruch genommenen Personen mithin kein Verschulden vorgeworfen werden kann.[2] Dies gilt trotz einer von der Rechtsprechung entwickelten Beweislastumkehr bei der Produzentenhaftung. Danach hat im Zweifel der Produzent der KI nachzuweisen, dass der Fehler nicht aus seiner Sphäre stammt. Letztlich bestehen gerade an dieser Stelle aber noch erhebliche Unsicherheiten. Sofern keine allgemeine gesetzliche Regelung erfolgt, bleibt damit die gerichtliche Bewertung den Umständen des jeweiligen Einzelfalles vorbehalten. Besondere Bedeutung hat hier der Autonomie-Grad der KI und der entsprechend zugrunde liegende Algorithmus.

Im Kontext der richterrechtlich entwickelten Produzentenhaftung im Rahmen von § 823 Abs. 1 BGB haben sich vier Verkehrssicherungspflichten entwickelt: die Konstruktionspflicht, Fabrikationspflicht, Instruktionspflicht und die Beobachtungspflicht. Es versteht sich von selbst, dass den Hersteller nach dem Inverkehrbringen einer von ihm geschaffenen KI (und auch den Nutzer während der Benutzung) fortdauernde aktive und passive Beobachtungspflichten treffen, die im Falle einer von der KI für die Allgemeinheit ausgehenden Gefahr Reaktionspflichten auslösen können (von einfachen Warnungen über die Bereitstellung von Sicherheitsupdates bis hin zu Produktrückrufen). Daneben dürfte die bedeutendste Pflicht des Herstellers im Vorfeld jedoch die Pflicht zur dem Stand der Wissenschaft und Technik entsprechenden Konstruktion (Programmierleistung) sein. Diese Pflicht gewährleistet zumindest vor dem Inverkehrbringen, dass die KI mit dem Maximum an technischer Sicherheit hergestellt bzw. programmiert werden muss, die zu diesem Zeitpunkt als State of the Art (nicht Branchenüblichkeit)[3] gilt. Waren bestimmte Gefahren noch nicht erkennbar und eine Verhinderung nicht möglich bzw. zumutbar, verwirklicht sich aus deliktischer Perspektive jedoch lediglich das allgemeine Lebensrisiko. Eine Haftung entfällt.

Nach § 831 Abs. 1 BGB besteht ebenfalls eine Haftung für die eigene sorgfaltswidrige Auswahl und Überwachung von dritten Personen, an die Aufgaben übertragen werden. Wenn diese Verrichtungsgehilfen bei Ausführung der Verrichtung rechtswidrig einen Schaden verursachen, haftet der Auftraggeber sofern eine sorgfaltswidrige Auswahl oder Überwachung der Hilfsperson durch den Auftraggeber vorliegt. Voraussetzung ist jedoch bislang, dass es sich bei dem Verrichtungsgehilfen um eine menschliche Person handelt. Die KI kommt natürlich nicht als eine solche „Person“ in Betracht. Daher könnte eine Haftung des Nutzers einer KI für durch die KI verursachte Schäden nur begründet werden, wenn man die Norm analog anwendet. Eine derartige Analogie wird in der Literatur – nicht zuletzt wegen der vorhandenen Beweislastumkehr und der strengen Haftung – als mögliche interessengerechte Lösung diskutiert.[4] In der Praxis mangelt es bislang jedoch an derartigen Ansätzen. Ob Gerichte auf dieses Haftungskonzept zurückgreifen werden, bleibt abzuwarten.

[3] BGH 16. Juni 2009, NJW 2009, 2952 (2953).

[4] Siehe m. w. N. zu dieser Auffassung Denga (2018, S. 74–76); Horner und Kaulartz (2016, S. 8–9).

▶ **Praxistipp** Wenn Sie KI-Lösungen bereitstellen und/oder einsetzen haben Sie in besonderem Maße darauf zu achten, dass die KI nach dem jeweils aktuellen Stand der Technik erstellt und trainiert wird. Abhängig von der Sicherheitsrelevanz der genutzten Anwendungen sind hersteller- und anwenderseitig alle zumutbaren Anstrengungen zu unternehmen, um sicherzustellen, dass die KI nur dort zum Einsatz kommt, wo hinreichend sichere Resultate zu erwarten sind. Beispielsweise dürfte die Steuerung eines Herzschrittmachers zweifellos so lange keiner KI überlassen werden, bis die menschlich trainierte und programmierte Softwarelösung statistisch eine geringere Fehlertoleranz erwarten lässt.[5] Berücksichtigen Sie nach Möglichkeit branchenübliche Standards und Normen und beobachten Sie auch nach Inverkehrbringen aktiv Ihre KI-Lösung im Markt im Hinblick auf versteckte Mängel und Risiken.

6.1.2 Verschuldensunabhängige Haftung (Gefährdungshaftung)

Bei autonom gesteuerten Fahrzeugen kann vom Grundsatz her immerhin auf die Gefährdungshaftung nach dem **Straßenverkehrsgesetz** (**StVG**) zurückgegriffen werden, soweit dessen Anwendungsbereich eröffnet ist. Nach § 7 Abs. 1 StVG ist der Halter verpflichtet, dem Verletzten den Schaden zu ersetzen, der daraus entsteht, dass bei dem Betrieb eines Kraftfahrzeugs oder eines Anhängers, der dazu bestimmt ist, von einem Kraftfahrzeug mitgeführt zu werden, ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt wird. Eine ähnliche Regelung enthält das **Luftverkehrsgesetz** (**LuftVG**), für den Halter eines Luftfahrzeugs, § 33 LuftVG.

Außerhalb des StVG und des LuftVG sind spezielle Gefährdungstatbestände für den Einsatz von KI derzeit praktisch nicht vorhanden bzw. relevant. Im Regelfall greift auch nicht das **Haftpflichtgesetz** (**HPflG**). Insbesondere das BGB sieht lediglich eine verschuldensabhängige, deliktische Haftung vor. Der existierende allgemeine Gefährdungstatbestand gemäß § 833 BGB bezieht sich lediglich auf die Tierhalterhaftung und ist aufgrund des gesetzgeberischen Ausnahmecharakters auf andere Fallkonstellationen nicht analog anwendbar (m. w. N. Spindler 2019, § 823 Rn. 6). Der Grundsatz ist nämlich: Keine Haftung ohne Verschulden. Die Schaffung eines KI-spezifischen Gefährdungstatbestandes wäre somit nur durch eine gesetzliche Neuregelung möglich (so auch Bräutigam und Klindt 2015, S. 1139; Ammann 2017, S. 509–510).

Als Anknüpfungspunkt für eine Gefährdungshaftung käme zumindest bei Verbraucherschäden allerdings das ProdHaftG in Betracht. Die Anwendung der Produkthaftungsregeln ist bei KI jedoch alles andere als geklärt. Nach § 1 Abs. 1 Satz 1 ProdHaftG ist der Hersteller des Produkts verpflichtet, dem Geschädigten den entstehenden Schaden zu er-

[5] Ganz abgesehen davon sind in besonders gefahrträchtigen Bereichen zahlreiche Sondervorschriften zu berücksichtigen, etwa die Zulassungsvoraussetzungen für Medizinprodukte.

setzen, wenn durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt wird. Zentrale Voraussetzung ist somit das Vorliegen eines „Produkts". Konkret lautet die Frage also: Ist ein KI-System ein Produkt? Ob Daten, insbesondere im technischen Kontext von KI, ein „Produkt" im Sinne des Gesetzes sind, ist bislang offen und noch nicht höchstrichterlich geklärt. Dabei sprechen grundsätzlich gute Argumente dafür. Ein „Produkt" ist gemäß § 2 ProdHaftG jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet, sowie Elektrizität. Die Anknüpfung an eine bewegliche Sache lässt Daten nur dann völlig unproblematisch unter die „Produkt"-Definition fallen, wenn diese auf einem (fehlerhaften) Datenträger[6] gespeichert sind, da insofern eine Verkörperung vorhanden ist (so auch Graf v. Westphalen 2018, S. 18). Etwas umstrittener ist bereits die Situation, in welcher der verkörpernde Datenträger fehlerfrei, die darauf befindlichen Daten jedoch fehlerhaft sind.[7] Sind die Daten – oder genauer gesagt die Information selbst – dagegen überhaupt nicht derart verkörpert (bspw. aus dem Internet heruntergeladen, aus einer Cloud heraus genutzt, usw.), ist die Anwendung des ProdHaftG zu Recht sehr strittig.[8] Dafür könnte sprechen, dass § 2 ProdHaftG Elektrizität – als ebenfalls nicht-körperliches Produkt – explizit erwähnt. Derselbe Umstand kann jedoch auch als explizit genannte Ausnahme angesehen werden mit der Folge, dass bei reiner Software die „Produkt"-Eigenschaft zu verneinen wäre. Gegen diese Ansicht spricht jedoch, dass es als willkürlich betrachtet werden muss, nach dem „Grad" der Verkörperung von Algorithmen und der Ursache für einen eingetretenen Schaden zu unterscheiden. So sollte die rechtliche Einstandspflicht z. B. nicht unterschiedlich ausfallen, wenn ein Kühlschrank aufgrund des Versagens einer in ihn von Beginn an eingebauten Software in Flammen aufgeht (= „Produkt" bejaht, Haftung des Kühlschrankherstellers) oder der Nutzer später eine fehlerhafte Software aus dem Internet herunterlädt, aufspielt (z. B. Geräte-Update) und infolgedessen der Kühlschrank Feuer fängt (= „Produkt" verneint, keine Haftung des KI-Programmierers oder ggf. Kühlschrankherstellers selbst) (so Wagner 2017, § 2 ProdHaftG Rn. 19). Mit Wagner und einigen anderen Autoren erscheint es daher plausibel, Software, die zur Gerätesteuerung eingesetzt wird, unabhängig von der Art der Verkörperung wie eine bewegliche Sache und somit als „Produkt" im Sinne von § 2 ProdHaftG zu qualifizieren (Wagner 2017, § 2 ProdHaftG Rn. 19; u.w. die Nachweise in Fn. 6). Selbst wenn man die Produkt-Eigenschaft vollumfänglich bejaht, ergeben sich aber noch weitere Probleme. Nach § 1 Abs. 2 Nr. 5 ProdHaftG ist die Haftung des Herstellers ausgeschlossen, wenn der

[6] Zur umsatzsteuerrechtlichen Bewertung von Software auf Datenträgern siehe Kap. 7 Abschn. 7.2.1.

[7] Die wohl h.M. bejaht hier die Produkt-Eigenschaft noch. Vgl. zum Streitstand Wagner (2017, § 2 ProdHaftG Rn. 14–16).

[8] Dafür Wagner (2017, § 2 ProdHaftG Rn. 17–20) unter Verweis auf eine richtlinienkonforme Auslegung von Art. 2 der RL 85/374/EWG; ebenso m. w. N. Rebin (2019, § 2 ProdHaftG Rn. 49–54, 56–59) unter Verweis auf den Sinn und Zweck des ProdHaftG; offen, jedoch eher zögerlich Graf v. Westphalen (2018, S. 18–19); zögerlich, jedoch für eine Erweiterung de lege ferenda Förster (2019, § 2 ProdHaftG Rn. 22–24).

Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. Ähnlich liegt bereits gem. § 3 Abs. 1 ProdHaftG kein Produktfehler vor, wenn das Produkt beim Inverkehrbringen die Sicherheit bietet, die berechtigterweise erwartet werden konnte. Bei selbstlernender und sich selbst entwickelnder KI stellen sich hier somit dieselben offenen (und rechtspolitischen) Fragen wie bei der an eine Verkehrspflichtverletzung anknüpfenden verschuldensabhängigen Haftung nach § 823 Abs. 1 BGB. Weitere Einschränkungen des ProdHaftG ergeben sich im Hinblick auf den sachlichen und persönlichen Anwendungsbereich sowie existierende Haftungshöchstbeträge.

Im Ergebnis erscheint eine Anwendung des verschuldensunabhängigen ProdHaftG bei Schäden, die durch den Einsatz von KI entstehen – je nach Einzelfall –, zukünftig zwar grundsätzlich möglich, hinreichend „passend" ist das Gesetz jedoch nicht (ebenso m. w. N. Ammann 2017, S. 510). Insbesondere im B2B-Bereich kommt es aufgrund der Haftungsbegrenzung auf Sachen zum privaten Ge- und Verbrauch zu Haftungslücken.

▶ **Praxistipp** Bis zu einer abschließenden Klärung oder eindeutigen gesetzlichen Regelung kann argumentiert werden, dass KI-Lösungen nicht dem Produkthaftungsgesetz unterfallen. Dies gilt insbesondere bei **Software as a Service Lösungen** (**SaaS**). Rechtlich betrachtet stellen diese eine reine Dienstleistung dar, für die das Produkthaftungsgesetz von vornherein nicht greift.[9] Ein allgemeines deliktisches Haftungsrisiko allein für den Vertrieb oder Gebrauch von KI kann andererseits aber auch nicht gänzlich ausgeschlossen werden. Im Zweifel trifft die Haftung jedenfalls denjenigen, der KI für bestimmte Zwecke einsetzt, denen die Lösung im Ergebnis nicht gerecht wird. Klar ist, dass KI-Lösungen nicht zu haftungsfreien Räumen führen. Für sicherheitskritische Systeme wird daher vor allem die Versicherbarkeit des Haftungsrisikos über deren kommerziellen Erfolg entscheiden. Sie sollten daher Ihre Betriebshaftpflichtversicherung überprüfen, ob diese den Vertrieb bzw. Einsatz derartiger Lösungen ausreichend deckt.

6.2 Rechte Dritter in der Wertschöpfungskette

KI-Systeme müssen zunächst trainiert werden. Das Training erfolgt entweder durch Menschen, zunehmend auch automatisiert. Dabei werden vielfach auch große Datenmengen genutzt, die über das world wide web frei zugänglich sind. Die Nutzung dieser Daten ist im Regelfall rechtlich unproblematisch möglich sofern keine technischen Zugangsbarrie-

[9] Ebenfalls kein Hersteller ist ein Dienstleister, der im Rahmen der Erbringung von Dienstleistungen fehlerhafte Geräte oder Produkte (in obigem Sinne also auch KI-Software) eines anderen verwendet. Er ist lediglich ein Verwender, der nicht als Beteiligter der Herstellungs- und Vertriebskette des entsprechenden Produkts tätig wird.

ren umgangen oder vertragliche Regelungen missachtet werden. Auf Einzelheiten sind wir bereits in Kap. 3 eingegangen. Was aber sind die Rechtsfolgen, wenn die KI absichtlich oder unbeabsichtigt auf Datensätze zugreift, die einem Dritten „gehören“?

6.2.1 Rechtsfolgen nach § 97 UrhG

Sofern die KI-Lösung in Urheberrechte Dritter eingreift, drohen gerichtliche Inanspruchnahme mittels Klage auf Unterlassung, Auskunft und Rechnungslegung. Zudem bestehen urheberrechtliche Beseitigungsansprüche auf Löschung der Datensätze und Schadensersatz nach § 97 UrhG bei Verletzung von Datenbankrechten. Anspruchsberechtigt ist hierbei der Inhaber des verletzten Urheberrechts. Anspruchsgegner ist derjenige, der die entsprechende Verletzungshandlung vornimmt. Die KI als solche kommt nicht als Täter in Frage, da sie nicht in den möglichen „Täterkreis“ des § 97 UrhG fällt. Nach § 97 UrhG kann vielmehr ausschließlich derjenige in Anspruch genommen werden, dem ein Verursachungsbeitrag nachgewiesen werden kann. Primär ist daher Täter wer letztlich hinter der Nutzung der KI steht. Daneben kommt auch der Hersteller der KI als Täter oder Teilnehmer in Betracht.

▶ **Praxistipp** Aufgrund der zunehmenden Autonomie der KI-Lösung wird erörtert, inwieweit die etablierten Haftungskonzepte überhaupt noch passend sind. Solange diesbezüglich jedoch keine gesetzliche Spezialregelung erfolgt, ist im Zweifel von einer Haftung des Anwenders auszugehen. Dies gilt jedenfalls für die Haftung auf Unterlassen der Rechtsverletzung. Letztere setzt nämlich kein Verschulden, sondern bloße Ursächlichkeit voraus.

6.2.1.1 Unterlassungsanspruch

Im Zentrum der Rechtsdurchsetzung nach § 97 UrhG steht der verschuldensunabhängige Unterlassungsanspruch nach § 97 Abs. 1 UrhG. Er dient der Abwehr andauernder oder künftiger Rechtsverletzungen und ist regelmäßig zugleich das Hauptinteresse des Anspruchsinhabers. Der Unterlassungsanspruch setzt entweder Wiederholungsgefahr voraus (§ 97 Abs. 1 S. 1 UrhG), oder dass hinreichend konkret eine erstmalige Verletzung der Urheberrechte droht (§ 97 Abs. 1 S. 2 UrhG). Die sog. Wiederholungsgefahr wird dabei grundsätzlich schon durch eine einzige Rechtsverletzung begründet.[10] Damit kann etwa die einmalige Verwendung eines urheberrechtlich geschützten Inhalts das Risiko begründen, vom Rechteinhaber auf Unterlassung in Anspruch genommen zu werden.

[10] BGH 6. Januar 1954, NJW 1954, 1628.

▶ **Praxistipp** In der Praxis wird der Unterlassungsanspruch meist außergerichtlich erledigt. In aller Regel mahnt der Rechteinhaber die Verletzung zunächst ab. Der vermeintliche Verletzer hat dann Gelegenheit die Wiederholungsgefahr durch Abgabe einer vertragsstrafebewehrten Unterlassungserklärung aus der Welt zu räumen. Gibt er eine solche Erklärung jedoch nicht ab, kann der Rechteinhaber auf Unterlassung klagen und seine für die Abmahnung entstandenen Kosten geltend machen.

6.2.1.2 Beseitigungsanspruch

§ 97 Abs. 1 UrhG gewährt als weitere Rechtsfolge zudem einen Beseitigungsanspruch. Dieser ist gerichtet auf die Beseitigung des durch die Verletzung gegebenen Störungszustandes. Wie der Unterlassungsanspruch ist auch der Beseitigungsanspruch verschuldensunabhängig. Im Unterschied zur Unterlassung, reicht hingegen einfaches Unterlassen nicht aus. Der Verletzer muss aktiv tätig werden und Daten oder urheberrechtswidrige Vervielfältigungen von Software aktiv löschen, Zugänge abschalten, etc. Von besonderer Bedeutung ist die vollständige Vernichtung bei digitalen Werken (zB Computerdateien). Hier kann der Verletzte – sofern verhältnismäßig – verlangen, dass der Verletzer eine Spezialsoftware zur Vernichtung einsetzt, da das einfache Überschreiben von Dateien oftmals nicht ausreichend sein kann (Spindler 2011, § 98 UrhG Rn. 11). § 69f UrhG enthält Sondervorschriften hinsichtlich rechtswidriger Vervielfältigungsstücke von Computerprogrammen und Mitteln, die zur unerlaubten Umgehung von Programmschutzmechanismen bestimmt sind.

▶ **Praxistipp** Im Rahmen der KI-Lösung wird der Beseitigungsanspruch oftmals auf die Löschung von unberechtigt verwendeten Datensätzen gerichtet sein. Auch anderes urheberrechtlich geschütztes Material kommt hier in Frage, beispielsweise Fotos und genutzte Softwarefragmente – sofern letztere eigenständig Schutz genießen. Auf durch KI generierte Daten dürfte der Anspruch hingegen in aller Regel nicht durchschlagen. Dies gilt jedenfalls sofern das von der KI erstellte Ergebnis eine eigenständige Bearbeitung des Ausgangsmaterial darstellt in der das Ausgangswerk verblasst. Der Inhaber der Bildrechte an einem Lichtbild kann dementsprechend keine Löschung des Ergebnisses verlangen. Beispiel: Die KI nutzt Lichtbilder lediglich als Ausgangsgröße, um hiervon unabhängige Abbildungen von nichtexistierenden Personen zu kreieren.

6.2.1.3 Schadensersatzanspruch

Dem in seinen Urheberrechten Verletzten kann zudem auch ein Schadensersatzanspruch nach § 97 Abs. 2 S. 1 UrhG zustehen. Im Gegensatz zum Unterlassungs- und Beseitigungsanspruch ist dieser Anspruch verschuldensabhängig. Fahrlässigkeit reicht allerdings aus. In der Regel wird von der Rechtsprechung angenommen, dass der Nutzer die Rechtsverletzung erkennen und vermeiden konnte. Insbesondere kann der Nutzer sich im Regelfall nicht damit entschuldigen, er habe die Urheberrechte des Dritten nicht gekannt. Vor

der Nutzung von geschütztem Material ist er zu entsprechender aktiver Aufklärung der Rechtesituation verpflichtet. Ob sich diese Grundsätze auf ein Umfeld übertragen lassen, dass verstärkt auf KI-Lösungen setzt ist fraglich. Im Ergebnis darf der Fortschritt der Technik aber nicht dazu führen, dass Rechteinhaber berechtigte Kompensationsansprüche für die unerlaubte Nutzung ihrer Werke verlieren. Im Zweifel wird daher nach wie vor davon auszugehen sein, dass der Nutzer für Fehleinschätzungen der KI ebenso einzustehen hat wie für „eigene" Fehler. Ist diese Voraussetzung gegeben, kann der Anspruchsberechtigte Schadensersatzansprüche nach der sogenannten „dreifachen Schadensberechnung" auswählen. Meist wählt der Rechteinhaber die Methode der Lizenzanalogie oder versucht alternativ den gemachten Gewinn des Verletzers abzuschöpfen. Alternativ kann er jedoch auch den eigenen entgangenen Gewinn ansetzen, wobei er hierfür allerdings seine interne Kalkulation offenlegen und seinen ohne die Verletzung gemachten Gewinn „beweisen" muss. Dies ist meist unattraktiv. Das Wahlrecht erlischt erst, sobald der nach einer der drei Berechnungsmethoden geltend gemachte Anspruch erfüllt oder rechtskräftig zuerkannt worden ist.[11] § 97 II S. 4 UrhG gewährt dem in seinen Urheberrechten Verletzten zudem Ersatz des immateriellen Schadens.

Der Verletzergewinn umfasst nur den Reinerlös. Dabei gilt der Grundsatz: berücksichtigungsfähig sind nur diejenigen Kosten, die den schutzrechtsverletzenden Gegenständen unmittelbar und konkret zugerechnet werden können, Gemeinkosten „die im Unternehmen sowieso anfallen" werden hingegen nicht abgezogen. Beispiel: Lohnkosten sind nur dann abzugsfähig, wenn der Arbeitnehmer gerade für die verletzende Tätigkeit neu eingestellt oder intern freigestellt wurde.

Der Schadensersatz nach der Lizenzanalogie wird durch die Gerichte geschätzt, § 287 ZPO. Zur Ermittlung der Lizenzhöhe kann in erster Linie an die Lizenzierungspraxis des Verletzten angeknüpft werden. Fehlt eine solche, so kommt es auf bestehende, branchenübliche Tarife oder sonstige Anhaltspunkte an. Die Höhe des Lizenzsatzes hängt im Einzelfall zum einen von der Qualität des Werkes ab. Zum anderen kommt es auf den Umfang der Rechtsverletzung an. Die fiktiven Lizenzgebühren fallen im Einzelfall entsprechend sehr unterschiedlich aus.

Für die Verletzung von Datenbankrechten wurden beispielsweise Schadensersatzzahlungen in Höhe von lediglich 1800 Euro bei Nutzung von Kartenausschnitten im Internet angenommen,[12] rund 18.700 Euro bei Nutzung von Karten und Datenbanken[13] und 56.000 Euro bei Nutzung von Wetterdaten aus einer Datenbank über einen längeren Zeitraum.[14] Im Einzelfall sind – abhängig vom Wert der Nutzung – auch deutlich höhere Summen realistisch.

[11] BGH 22. September 1999, GRUR 2000, 226.

[12] OLG München 11. April 2019 – 29 U 3773/17.

[13] KG 21. März 2012, MMR 2013, 53.

[14] OLG Köln 15. Dezember 2006 – 6 U 229/05.

6.2.1.4 Auskunft und Rechnungslegung

Dem Verletzten kann zudem ein Auskunfts- und/oder Rechnungslegungsanspruch zustehen. Dieser Anspruch dient unter anderem der Vorbereitung und Durchsetzung des Schadensersatzanspruchs in einem Schadensersatzhöheverfahren. Um den Schadensersatzanspruch möglichst zutreffend berechnen zu können, benötigt der Verletzte Informationen über Umfang und Dauer der Verletzungshandlung. Auf diese kann er nicht ohne Weiteres zugreifen, da diese Informationen zumeist vollumfänglich in der Sphäre des Rechtsverletzers liegen. Der Auskunftsanspruch kann allerdings nicht dazu verwendet werden überhaupt erst in Erfahrung zu bringen, ob eine Verletzungshandlung durch den in Anspruch Genommenen stattgefunden hat um anhand dessen dann weitere Ansprüche geltend zu machen. Dies käme einer unzulässigen Ausforschung gleich. Das Vorliegen einer Rechtsverletzung muss vielmehr bereits erwiesen sein. Besteht ein Auskunftsanspruch, verpflichtet er zu allen Angaben, die der Verletzte zur Ermöglichung einer sachgerechten Rechtsverfolgung benötigt.[15] Neben dem einfachen Auskunftsanspruch kann auch ein detaillierterer „qualifizierter" Auskunftsanspruch auf Rechnungslegung bestehen. Ob dies der Fall ist entscheidet sich anhand Informationsbedürfnis, Zumutbarkeit und Verhältnismäßigkeit.[16]

6.2.2 Rechtsfolgen nach §§ 106 ff. UrhG (Strafrecht)

Im Extremfall kann zudem auch eine strafrechtliche Verantwortung gegeben sein. Die §§ 106 ff. UrhG normieren verschiedene Straftatbestände, die den Urheberrechtsschutz betreffen. Im Rahmen der KI-Lösung relevant sind hierbei insbesondere § 106 UrhG und § 108b Abs. 1 und 2 UrhG. In § 106 UrhG werden urheberrechtlich relevante Verwertungshandlungen mit einer Strafandrohung von bis zu drei Jahren Freiheitsstrafe oder mit Geldstrafe belegt. In § 108b Abs. 1 und 2 UrhG werden bestimmte Eingriffe in technische Schutzmaßnahmen und in zur Rechtewahrung erforderliche Informationen unter Strafe gestellt. Zu beachten ist allerdings, dass es sich bei den Straftatbeständen des Urhebergesetzes um Antragsdelikte handelt (§ 109 UrhG). Eine Ausnahme gilt, wenn ein besonderes öffentliches Interesse an der Strafverfolgung vorliegt oder der Täter im Sinne des § 108a UrhG gewerbsmäßig handelt. Vor allem die Alternative des gewerbsmäßigen Handelns ist praktisch relevant. Zu beachten ist außerdem, dass die Urheberrechtsdelikte in den Katalog der Privatklagedelikte gemäß § 374 Abe. 1 Nr. 8 StPO fallen. Sie werden dementsprechend auch bei gestelltem Strafantrag nur verfolgt, wenn ein (einfaches) öffentliches Strafverfolgungsinteresse besteht. Ist dies nicht der Fall, wird das Verfahren eingestellt und der Betroffene auf den Privatklageweg verwiesen. Für die Praxis bedeutet dies, dass

[15] BGH 27. September 1990, GRUR 1991, 153.

[16] BGH 13. März 1962, GRUR 1962, 398.

es im Rahmen von Urheberrechtsverletzungen eher selten zu strafrechtlicher Verfolgung kommt. Zum einen ist das Hauptinteresse des Geschädigten in der Regel ohnehin auf seine zivilrechtlichen Ansprüche gerichtet. Zum anderen ist ein öffentliches Interesse an der Strafverfolgung bei den wenigsten Urheberrechtsverletzungen gegeben.

▶ **Praxistipp** Gleichwohl wird das Mittel der Strafverfolgung insbesondere zur Beweissicherung vergleichsweise häufig genutzt. Insbesondere strafrechtliche Durchsuchungsanordnungen auf Antrag des Rechteinhabers sind ein gängiges Mittel um mit staatlicher Hilfe an die notwendigen Beweise (Beispiel: unberechtigte Verwendung von Software) für den nachgelagerten Zivilprozess zu gelangen.

6.2.3 Rechte an Algorithmen

Für KI-Lösungen besonders relevant sind schließlich Rechte an Algorithmen und Schutz vor Dekompilieren. Generell ist die Nutzung von Drittsoftware riskant, wenn keine hinreichenden Rechtfertigungsgründe (beispielsweise eine Lizenz) vorliegen. Bei unzulässigen Eingriffen in Softwareurheberrechte droht ebenfalls die Inanspruchnahme auf Unterlassung und Schadensersatz. Bei Überschreitung vertraglicher Regelungsbefugnisse kommen daneben auch vertragliche Unterlassungsansprüche in Betracht. Die Grenze zwischen zulässiger und unzulässiger Nutzung ist im Detail aber nicht immer leicht zu erkennen. Der Schutz von Softwareurheberrechten ist in den §§ 69a ff. UrhG geregelt. Einerseits sollen die Regelungen den umfassenden Urheberschutz an Computerprogrammen gewährleisten. Gleichzeitig soll aber ein Gleichgewicht zwischen den Geheimhaltungsinteressen des Softwareherstellers und dem Erfordernis eines auf Kompatibilität gerichteten Wettbewerbs herrschen. Nach § 69a Abs. 2 S. 1 UrhG sind zunächst „alle Ausdrucksformen“ eines Computerprogramms geschützt. Vom Softwareschutz nicht umfasst sind lediglich die Programmiersprache selbst (Beispiel: JAVA) und Dateiformate. Problematisch ist der Schutz des Algorithmus. Den Algorithmus qualifiziert die Rechtsprechung als „die in dem Computerprogramm berücksichtigte, sich auf einen vorgegebenen Rechner beziehende Rechenregel“.[17] Er ist daher von dem geschützten konkreten Programmcode zu unterscheiden. Folglich unterliegt der Algorithmus auch nicht dem Urheberrechtsschutz. Der BGH berücksichtig Algorithmen gleichwohl indirekt dort, wo es um die „Art und Weise der Implementierung und Zuordnung zueinander“ geht.[18] Da KI Lösungen oftmals mit Drittsoftware interagieren ist ferner besonders praxisrelevant inwieweit legale Schnittstellen zu Drittprogrammen geschaffen werden dürfen. Zentral ist dabei § 69e UrhG, der

[17] OLG Frankfurt am Main 13. Juni 1983, GRUR 1983, 753.

[18] BGH 04. Oktober 1990, NJW 1991, 1231.

sich auf die hierfür notwendige Dekompilierung der Schnittstelle bezieht. Das Dekompilieren eines Computerprogramms wird lediglich in sehr eng begrenztem Umfang erlaubt. Wichtigste Voraussetzung ist hierbei insbesondere die Unerlässlichkeit zur Erlangung der Schnittstelleninformationen. Dies scheitert oft schon daran, dass viele Hersteller gewisse Schnittstelleninformationen freiwillig offenlegen. Dekompilieren ist darüber hinaus nur zum Zwecke der Herstellung von Interoperabilität zwischen Programmen zugelassen. Entsprechend darf maximal so viel Code dekompiliert werden, wie für den Zweck der Verbindung der fremden Programme zwingend nötig ist. Der Dekompiler darf schließlich gemäß § 69e Abs. 1 Nr. 1 UrhG nur durch einen zur Verwendung der Software bereits Berechtigten genutzt werden. Dies ist allerdings typischerweise der Käufer oder sonstige berechtigte Nutzer der Software.

6.3 Urheber- und Erfinderrechte

In der analogen Welt schreibt Johann Wolfgang von Goethe weltberühmte literarische Werke wie „Faust“, die Beatles besingen unter John Lennon und Paul McCartney „Jude“ in einem ihrer erfolgreichsten Lieder, Thomas Alva Edison bringt die Glühbirne zum Leuchten und Karl Benz gilt mit seinem dreirädrigen Fahrzeug mit Gasmotorenbetrieb als Erfinder des Automobils. Um die schöpferischen und technischen Leistungen dieser Personen vor Nachahmern zu sichern, gibt es den rechtlichen Schutz durch Urheber- und Patentrechte.[19]

Nach § 2 Abs. 2 UrhG sind Werke der Literatur, Wissenschaft und Kunst persönliche geistige Schöpfungen und Patente werden gemäß § 1 **Patentgesetz** (**PatG**) für Erfindungen auf allen Gebieten der Technik erteilt, sofern sie neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind. Das Recht auf das Patent hat nach § 6 Satz 1 PatG der Erfinder oder sein Rechtsnachfolger. All diesen Regelungen ist gemein, dass ihr Schutz nach traditionellem Verständnis ausschließlich Rechtssubjekten vorbehalten ist. Rechtsobjekte, also insbesondere Sachen, können dagegen nicht Träger von Rechten und Pflichten sein.

Die praktische Realität im Zeitalter von KI zeigt jedoch, dass dieses, über Jahrhunderte entwickelte Rechtsverständnis immer häufiger an Grenzen stößt und Fragen aufwirft. KI ist schon längst in der Lage, Lieder im Stil der Beatles zu komponieren (Kühl 2017, S. 2), selbstständig Lebensmittel- und Getränkebehälter zu „erfinden“ oder auch komplexere Vorrichtungen zur Erkennung von Personen in Notsituation.[20]

[19] Zu steuerrechtlichen Besonderheiten im Zusammenhang mit dem Urheberrecht vgl. Kap. 7 Abschn. 7.1.3.2 sowie 7.2.4.

[20] Vgl. zu den Patentanmeldungen EP 3 564 144 A1 (Food container) und EP 3 563 896 A1 (Devices and methods for attracting enhanced attention) und den hierzu ergangenen, ablehnenden Entscheidungen des Europäischen Patentamtes. http://patentblog.kluweriplaw.com/2020/01/29/epo-a-machine-cannot-be-an-inventor/. Zugegriffen am 04.02.2020.

Sowohl im Patent- als auch im Urheberrecht stellen sich somit jeweils zwei zentrale Fragen, wenn KI immaterialgüterrechtlich bewertet werden soll. Zum einen ist dies die Frage, ob der Algorithmus, welcher der KI zugrunde liegt, durch Patent- und/oder Urheberrechte geschützt werden kann. Zum anderen wird diskutiert, ob KI selbst Leistungen schaffen kann, die durch Patent- und/oder Urheberrechte geschützt werden.

6.3.1 Patentrechtlicher Schutz

6.3.1.1 Schutz des der KI zugrunde liegenden Algorithmus

Im Zentrum der Diskussion um den Schutz von KI durch Patentrechte steht die Frage der patentrechtlichen Schutzfähigkeit von Software als sogenannte „softwareimplementierte Erfindung". Erfindungen beruhen auf der Kreativität der menschlichen Geistestätigkeit, durch die eine konkrete Lehre zum technischen Handeln geschaffen wird, um ein technisches Problem mit technischen Mitteln zu lösen. Der Bundesgerichtshof (BGH) urteilte hierzu 1969 in einer Grundsatzentscheidung: „Dem Patentschutz zugänglich ist eine Lehre zum planmäßigen Handeln unter Einsatz beherrschbarer Naturkräfte zur Erreichung eines kausal übersehbaren Erfolges".[21] Vergegenwärtigt man sich, dass die Basis einer jeden Software eine Abfolge von Zahlen darstellt, die nach festgelegten, logischen Regeln abgearbeitet werden („wenn …, dann …"), wird deutlich, dass hier – im Ausgangspunkt – keine beherrschbaren Naturkräfte zum Einsatz kommen. Auf Technizität im patentrechtlichen Sinne lässt sich also nicht schon deshalb schließen, weil Technik und Daten (z. B. ein Computer) benutzt werden. § 1 Abs. 3 Nr. 1, 3 und 4 PatG sieht daher auch u. a. einen Ausschluss vom Patentschutz für mathematische Methoden, Programme für Datenverarbeitungsanlagen oder die Wiedergabe von Informationen vor. Nach § 1 Abs. 4 PatG steht dieser Ausschluss der Patentfähigkeit jedoch „nur insoweit entgegen, als für die genannten Gegenstände oder Tätigkeiten *als solche* Schutz begehrt wird". Dies bedeutet, dass das abstrakte Konzept des Algorithmus als solches zwar nicht dem Patentschutz zugänglich ist, darüber hinausgehend patentfähige Technizität jedoch auch nicht gänzlich ausgeschlossen ist. Im Einzelfall muss immer ein technisches Ergebnis erreicht werden, eine Art technische Wirkung auf die Außenwelt.

Die Rechtsprechung und Spruchpraxis der Gerichte und Patentämter ist im Bereich der softwareimplementierten Erfindungen hochgradig einzelfallabhängig und fortlaufend im Wandel. Insbesondere im Zusammenhang mit KI befindet sich die Erteilungs- und Verletzungspraxis noch vergleichsweise in den Kinderschuhen. Die Anzahl der angemeldeten Patente hat in diesem Bereich in den letzten Jahren rasant zugenommen, die Anzahl der erteilten (und rechtsbeständigen) Patente ist dagegen jedoch noch verhältnismäßig gering. In den Richtlinien für die Prüfung im Europäischen Patentamt (EPA) (Stand November 2019) heißt es zur Patentierbarkeit von KI und maschinellem Lernen:

[21] BGH 27. März 1969, GRUR 1969, 672.

„Künstliche Intelligenz und maschinelles Lernen" basieren auf Rechenmodellen und Algorithmen zur Klassifizierung, Bündelung, Regression und Dimensionalitätsreduktion wie zum Beispiel neuronalen Netzen, genetischen Algorithmen, Support Vector Machines, k-Means, Kernel-Regression und Diskriminanzanalyse. Solche Rechenmodelle und Algorithmen sind per se von abstrakter mathematischer Natur, unabhängig davon, ob sie anhand von Trainingsdaten „trainiert" werden können. […]

Ausdrücke wie „Support Vector Machine", „Reasoning Engine" oder „neuronales Netz" können sich je nach Kontext lediglich auf abstrakte Modelle oder Algorithmen beziehen und implizieren deshalb für sich genommen nicht unbeding [sic!] die Verwendung technischer Mittel. Bei der Prüfung, ob der beanspruchte Gegenstand insgesamt technischen Charakter hat, ist dies zu berücksichtigen […].

Künstliche Intelligenz und maschinelles Lernen finden auf verschiedenen Gebieten der Technik Anwendung. So leistet zum Beispiel die Verwendung eines neuronalen Netzes in einem Herzüberwachungsgerät zum Identifizieren unregelmäßiger Herzschläge einen technischen Beitrag. Die Klassifizierung von digitalen Bildern, Videos, Audio- und Sprachsignalen auf der Grundlage von Low-level-Merkmalen (z. B. Kanten oder Pixelattributen für Bilder) ist eine weitere typische technische Anwendungsform von Klassifizierungsalgorithmen. Dagegen gilt die Klassifizierung von Textdokumenten ausschließlich nach ihrem Textinhalt per se nicht als technischer, sondern als linguistischer Zweck (T 1358/09). Die Klassifizierung von abstrakten Datensätzen oder sogar „Telekommunikationsnetzwerk-Datensätzen" ohne Angabe einer technischen Verwendung der resultierenden Klassifikation stellt per se ebenfalls keinen technischen Zweck dar, auch wenn dem Klassifikationsalgorithmus wertvolle mathematische Eigenschaften wie Robustheit zugeschrieben werden können (T 1784/06).

Wenn eine Klassifizierungsmethode einem technischen Zweck dient, können die Schritte „Erzeugung des Trainings-Datensatzes" und „Training des Klassifikators" auch zum technischen Charakter der Erfindung beitragen, wenn sie das Erreichen dieses technischen Zwecks unterstützen (Europäisches Patentamt 2019, Teil G Kap. 2 Ziffer 3.3.1; vgl. in diesem Kontext auch Lederer 2019, S. 153–154).

Diese Ausführungen des Europäischen Patentamts machen deutlich, dass die Erteilungspraxis bei KI noch durchaus restriktiv gehandhabt wird, jedoch keineswegs nicht erfolgsversprechend wäre.

▶ **Praxistipp** Der patentrechtliche Schutz von KI als solcher ist aufgrund der Notwendigkeit eines technischen Charakters, der über die bloße Softwarenutzung hinausgeht, eingeschränkt. Gänzlich ausgeschlossen ist er jedoch nicht, weshalb für die Bewertung im Einzelfall immer ein Patentanwalt hinzugezogen werden sollte. Zukünftig muss man sich wohl fragen, ob die klassischen Ausschluss-Argumente für die Patentierung von Software als solche auf selbstlernende und sich selbst weiterentwickelnde KI tatsächlich noch derart „klassisch" Anwendung finden bzw. Anwendung finden sollten. Es wäre zumindest denkbar, alleine die Fähigkeit einer Ma-

schine, selbst zu lernen und sich selbst weiterzuentwickeln, als hinreichend technisch zu betrachten.

6.3.1.2 KI als Erfinder einer technischen Lehre

Die Leistungen, die von einer KI generiert werden, können grundsätzlich dem Patentrecht zugänglich sein. Einen pauschalen Ausschluss gibt es hier nicht. Vielmehr muss auch hier immer der Einzelfall betrachtet werden. So kann nach dem BGH z. B. eine Datenfolge patentrechtlichen Schutz als unmittelbares Verfahrenserzeugnis gemäß § 9 Satz 2 Nr. 3 PatG genießen, „wenn sie sachlich-technische Eigenschaften aufweist, die ihr durch das Verfahren aufgeprägt worden sind, und sie daher ihrer Art nach tauglicher Gegenstand eines Sachpatents sein kann".[22] Bei dem sog. derivativen Erzeugnisschutz muss jedoch bedacht werden, dass das durch das Verfahren hergestellte Erzeugnis nach dem sog. Offenbarungsgrundsatz für den Fachmann hinreichend genau in dem Verfahrenspatent offenbart sein muss. Je autonomer die KI und je komplexer das Verfahrenserzeugnis, desto eher muss hieran gezweifelt werden (Hetmank und Lauber-Rönsberg 2018, S. 576–577). Dass eine KI jedoch viel mehr kann, als lediglich abstrakte Datenfolgen zu kreieren, zeigen schon die eingangs erwähnten Patentanmeldungen zum Schutz eines Getränkebehälters (EP 3 564 144 A1) sowie einer Vorrichtung und eines Verfahrens „zur Erregung einer erhöhten Aufmerksamkeit" (EP 3 563 896 A1).[23] Hierfür steht patentrechtlicher Erzeugnisschutz nach § 9 Satz 2 Nr. 1 PatG sowie Verfahrensschutz nach § 9 Satz 2 Nr. 2 PatG zur Verfügung. Grundvoraussetzung der Schutzfähigkeit ist stets, dass die Erfindung auf technischem Gebiet liegt, neu ist, auf einer erfinderischen Tätigkeit beruht und gewerblich anwendbar ist (§ 1 Abs. 1 PatG). Gerade bei der Frage der Neuheit ergeben sich durch die KI selbst interessante Perspektiven. KI und machine learning könnten durchaus das Patentsystem durch einen unendlich großen Stand der Technik auf den Kopf stellen, der entweder aus allen vorhandenen Quellen recherchiert oder im Extremfall sogar rein computer-generiert in Datenbanken abgespeichert wird. Für die Frage der Technizität gelten die Ausführungen zur Patentierbarkeit von KI als solcher. In jedem Fall müssen die Ausschlüsse nach § 1 Abs. 3 PatG beachtet werden. KI-gesteuerte Verfahren zur komplexen Datenanalyse und Datensammlung (z. B. das sog. Data Mining) werden daher z. B. in den allermeisten Fällen nicht patentierbar sein, da es sich um vom Patentschutz ausgeschlossene Software als solche handelt.[24] Hierzu heißt es in den bereits zitierten Richtlinien für die Prüfung im Europäischen Patentamt: „Die Klassifizierung von abstrakten

[22] BGH 27. September 2016, GRUR 2017, 261; In diesem Fall wäre der Inhaber des Verfahrenspatents als Inhaber der Datenfolge anzusehen, weil § 9 Satz 2 Nr. 3 PatG unmittelbar an das geschützte Herstellungsverfahren anknüpft. Dies wird in der Regel eine natürliche oder juristische Person sein, jedoch nicht die KI (hierzu im weiteren Verlauf).

[23] Siehe die Patentanmeldungen EP 3 564 144 A1 (Food container) und EP 3 563 896 A1 (Devices and methods for attracting enhanced attention).

[24] Zur steuerrechtlichen Bewertung des Data Minings siehe Kap. 7, Abschn. 7.1.1 und 7.1.1.4.

Datensätzen […] ohne Angabe einer technischen Verwendung der resultierenden Klassifikation stellt per se ebenfalls keinen technischen Zweck dar, auch wenn dem Klassifikationsalgorithmus wertvolle mathematische Eigenschaften […] zugeschrieben werden können […].“ (Europäisches Patentamt 2019, Teil G Kap. 2 Ziffer 3.3.1)

▶ **Praxistipp** An patentrechtlichen Schutzmöglichkeiten für die von KI geschaffenen Leistungen mangelt es der derzeitigen Gesetzeslage grundsätzlich nicht. In Betracht kommt ein Erzeugnisschutz, ein Verfahrensschutz und ein vom Verfahren abgeleiteter Schutz als unmittelbares Verfahrenserzeugnis, § 9 Satz 2 Nr. 1, 2 und 3 PatG. Wenn Sie eine KI-Anmeldung planen, sollten Sie darauf achten auch einen weitergehenden technischen Effekt mit Bezug zu einer Anwendung oder zu einer besonders bevorzugten Implementierung auf einer Plattform (Application Specific Integrated Circuit, GPU, GPU-Netzwerk, etc.) zu beanspruchen.

Deutlich problematischer ist, wer Erfinder[25] der von einer KI generierten Leistung bzw. Anmelder/Inhaber des Patents ist. Nach § 6 Satz 1 PatG steht das Recht auf das Patent dem Erfinder oder dem Rechtsnachfolger des Erfinders zu (entsprechend Art. 60 Abs. 1 Satz 1 EPÜ für Europäische Patente). Da eine KI kein Rechtssubjekt und deshalb nicht Träger von Rechten und Pflichten ist, dürfte es völlig unbestritten sein, dass eine KI selbst nicht Inhaber eines Patents sein kann. In Betracht käme folglich nur die Möglichkeit, die KI als Erfinder zu betrachten und einen Menschen als Rechtsnachfolger der KI als letztlichen Patentinhaber. Genau diesen Weg versuchte 2019 der Eigentümer einer KI namens DABUS gegenüber dem Europäischen Patentamt (EPA) im Zusammenhang mit den bereits erwähnten Patentanmeldungen EP 3 564 144 A1 und EP 3 563 896 A1 zu gehen. Sein Kernargument war, dass eine KI auch „Erfinder“ im Sinne von Art. 81 Satz 1 EPÜ (ähnlich § 37 Abs. 1 Satz 1 PatG) sein und folglich in der Patentanmeldung als solcher benannt werden könne; eine Beschränkung der Erfindereigenschaft auf natürliche Personen ergebe sich nicht aus den gesetzlichen Regelungen.[26] Das EPA folgte dem Anmelder nicht und verneinte die Erfindereigenschaft einer KI auf Basis der existierenden, gesetzlichen Regelungen, die nach Wortlaut sowie Sinn und Zweck auf natürliche Personen zugeschnitten seien.[27] Die einzelnen Argumente mögen rechtlich mehr oder weniger überzeugen. Her-

[25] Zur Einkommensteuerpflicht von Erfindern siehe Kap. 7, Abschn. 7.1.2.1.

[26] Vgl. repräsentativ für beide Patentanmeldungen die Erklärung des Anmelders vom 24. Juli 2019 zu EP 3 564 144 A1. https://register.epo.org/application?documentId=E3L3E6US2358DSU&number=EP18275163&lng=de&npl=false. Zugegriffen am 04.02.2020.

[27] Für die Entscheidungen des EPA vom 27. Januar 2020. https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=de&npl=false (für EP 3 564 144 A1) sowie https://register.epo.org/application?documentId=E4B63OBI2076498&number=EP18275174&lng=de&npl=false (für EP 3 563 896 A1) (jeweils zugegriffen am 04.02.2020).

vorzuheben ist in jedem Fall, dass auch Erfindern originäre Rechte zukommen wie z. B. das Recht auf Erfindernennung. Diese Rechte sind sog. Erfinderpersönlichkeitsrechte. Dies macht deutlich, dass – nach derzeitiger Rechtslage – nicht nur Anmelder/Inhaber Rechtssubjekte sein müssen, sondern auch die Erfinder selbst. Selbst wenn man die Erfindereigenschaft einer KI annehmen würde, so könnte das hierauf basierende Patent aber auch nicht auf den Anmelder als „Rechtsnachfolger" der KI übertragen werden. Mangels Rechtsfähigkeit einer KI kann diese niemals Partei einer hierfür notwendigen Rechteübertragung sein. Hier ist dem EPA ebenfalls zuzustimmen.

Interessant wäre gewesen, ob das EPA den Eigentümer der KI zwangsläufig als Erfinder ansieht bzw. akzeptiert. Dies ist in Europa bislang ungeklärt. Eine solche pauschale Erfindereigenschaft des KI-Eigentümers wäre nach aktueller Rechtslage aber kaum möglich. Eine andere Möglichkeit wäre die Anknüpfung an die Person des Programmierers der KI. Auch dies erscheint jedoch nicht sachgerecht, weil diese Person nicht selten sachlich (und räumlich) am allerweitesten von der autonom agierenden KI entfernt ist. Eine Schutzrechtszuordnung nach mehreren Jahren der KI-Arbeit wäre hier ebenso willkürlich. Am ehesten erscheint es daher sachgerecht, den konkreten Nutzer der KI als Erfinder bzw. Anmelder/Inhaber des Patents anzusehen. So ist auch bei „klassischen Computererfindungen" derjenige Erfinder, „der durch die Programmgestaltung und die Auswertung der Ergebnisse des Computers die Lösung der technischen Problemstellung erreicht und erkennt, nicht dagegen, der Konstrukteur des Computers, dessen Eigentümer oder Besitzer und das sonstige Bedienungspersonal" (Melullis 2015, § 6 Rn. 32). Ist derjenige, der mithilfe der KI die technische Problemstellung „erreicht und erkennt" immer der Nutzer, selbst bei einer autonom handelnden, selbstlernenden und sich selbst weiterentwickelnden KI? Dies muss mit zunehmendem Autonomiegrad wohl verneint werden. Die KI kann in einem solchen Fall nicht mehr nur als „Werkzeug" des konkreten Nutzers angesehen werden (Hetmank und Lauber-Rönsberg 2018, S. 576).

▶ **Praxistipp** Eine KI kann weder Erfinder noch Inhaber eines Patents sein. Am ehesten kommt für diese Stellung der konkrete Nutzer der KI in Betracht. Das kann jedoch nur solange gelten, wie KI als „Werkzeug" dieser Person qualifiziert werden kann. Zukünftig wird auch dies immer schwieriger möglich sein. Eine pauschale Zuordnung zu dieser Person scheitert daher mit steigender Autonomie der KI. Eine Gesetzesänderung dürfte dann am wahrscheinlichsten sein.

6.3.2 Urheberrechtlicher Schutz

6.3.2.1 Schutz des der KI zugrunde liegenden Algorithmus

Anders als im Patentrecht bedarf es für den urheberrechtlichen Schutz von Software keiner technischen Wirkung. Ausreichend ist eine hinreichende Individualität bei der Programmgestaltung (sog. „kleine Münze"), die bei der Programmierung von KI im Grunde

immer vorhanden sein wird. Somit steht für die der KI zugrunde liegende Software Schutz nach den §§ 69a ff. UrhG zur Verfügung. Wichtig zu berücksichtigen ist jedoch, dass der Schutzumfang ein anderer ist als im Patentrecht. Die Schutzschwelle ist im Patentrecht aufgrund der Forderung einer technischen Wirkung zwar höher, dafür ist der Schutzumfang jedoch auch breiter, da (je nach Anspruchsformulierung) auch die Idee der der KI zugrunde liegenden Software mit geschützt sein kann. Der urheberrechtliche Softwareschutz dagegen beschränkt sich nach § 69a Abs. 2 Satz 1 UrhG auf alle Ausdrucksformen eines Computerprogramms. Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrunde liegenden Ideen und Grundsätze, sind dagegen gemäß § 69a Abs. 2 Satz 2 nicht geschützt.

▶ **Praxistipp** Urheberrechtlicher Schutz kommt primär (nur) dem „Herz" einer KI zugute, namentlich dem Quellcode. Ein darüber hinausgehender Schutz der Ideen und Grundsätze wäre dagegen nur durch das Patentrecht möglich. Das Urheberrecht schützt somit nur vor einer direkten Kopie oder sonstigen unberechtigten Nutzung der „DNA" der KI. Aufgrund der Komplexität mancher KI bedeutet dies jedoch nicht, dass der Schutzbereich enorm eingeschränkt wäre. Häufig wird eine exakte Kopie der einfachste und einzig mögliche Weg sein, eine KI nachzuahmen.

6.3.2.2 KI als Urheber einer geistigen Schöpfung

Wie im Patentrecht gilt auch für das Urheberrecht, dass dieses – vor allem in Deutschland – originär persönlichkeitsrechtlich geprägt ist. Der kreative Mensch ist es, der seinem Werk Ausdruck und Individualität verleiht. Dies wird besonders in der Definition des Werkes in § 2 Abs. 2 UrhG als persönliche geistige Schöpfung oder den Urheberpersönlichkeitsrechten gemäß den §§ 12 ff. UrhG deutlich. Gleiches gilt für den urheberrechtlichen Schutz von Computerprogrammen, die nach § 69a Abs. 3 UrhG nur geschützt werden, wenn sie individuelle Werke in dem Sinne darstellen, dass sie das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers sind. Der Werkschutz steht somit alleine Menschen zur Verfügung. Ohne eine fundamentale gesetzliche Änderung könnte KI nicht Urheber eines urheberrechtlich schutzfähigen Werkes sein.

Etwas anders fällt die Bewertung von urheberrechtlichen Leistungsschutzrechten aus. Hierunter fallen z. B. der Lichtbild-Leistungsschutz nach § 72 UrhG oder der Datenbankhersteller-Leistungsschutz nach den §§ 87a ff. UrhG. Derartige Leistungsschutzrechte schützen in erster Linie nicht die persönliche geistige Schöpfung, sondern den Aufwand, der betrieben wurde, um den jeweiligen Schutzgegenstand zu generieren. Auch hier kann eine KI jedoch nicht Inhaber eines solchen Leistungsschutzrechts sein. Eine KI mag – was durchaus möglich ist – zwar eine schutzfähige Datenbank i.S.v. § 87a Abs. 1 UrhG oder Lichtbilder im Sinne von § 72 UrhG erstellen, weshalb sie als Leistungserbringer und somit theoretisch auch als Rechteinhaber angesehen werden könnte. Datenbankinhaber wäre aber nur derjenige, der auch das Amortisierungsrisiko trägt, d. h. die maßgeblichen Investitionen getätigt hat. Eine KI ist jedoch nicht rechtsfähig, ist daher kein Träger von eigenen Rechten und Pflichten und besitzt folglich keine eigene Haftungs-

masse. Auch Lichtbildner nach § 72 Abs. 2 UrhG kann nur eine natürliche Person sein.[28] Je nach Einzelfall ist es jedoch durchaus möglich, dass – mangels Notwendigkeit einer persönlichen geistigen Schöpfung – der hinter der KI agierende Mensch Inhaber des Leistungsschutzrechts wird. Da es bei diesen Schutzrechten primär um die hierfür notwendige Leistung geht, erscheint es wohl meist am sachgerechtesten, dem Nutzer der KI dieses Schutzrecht zuzusprechen. Liegt der Schwerpunkt dagegen z. B. in der Entwicklung einer KI-Software zum Aufbau einer Datenbank, könnte auch der Programmierer der Software als Leistungsschutzrechtsinhaber angesehen werden (Lauber-Rönsberg 2019, S. 258). Eine pauschale Zuordnung wäre jedenfalls verfehlt, weil die Inhaberschaft des Leistungsschutzrechts zutreffend nur im individuellen Fall bewertet werden kann.[29]

Sowohl für urheberrechtlich geschützte Werke als auch – im Ausgangspunkt – für Leistungsschutzrechte besteht folglich nur die Möglichkeit, die „Handlungen" einer KI als „Werkzeug" einem Menschen zuzuordnen. Entsprechend ist diese Person dann Inhaber des Immaterialgüterrechts. Von Bedeutung für diese Beurteilung können wie auch im Patentrecht z. B. sein: der Autonomiegrad der KI, die Kontrollierbarkeit der Umgebung, in der sich die KI bewegt, samt eigenem Gestaltungsspielraum des Menschen und die Vorhersehbarkeit des Handelns der KI (vgl. hierzu bspw. Lauber-Rönsberg 2019, S. 247–248; Ory und Sorge 2019, S. 711). Kurz gesagt: Je stärker die Faktoren ausgeprägt sind, die eine KI zu einem autonom handelnden Objekt machen, desto eher ist von einer gemeinfreien Leistung auszugehen, die urheberrechtlich schutzlos ist, da die KI nicht mehr als Werkzeug des Menschen qualifiziert. In – allerdings engem – Rahmen können dann nur Leistungsschutzrechte weiterhelfen. Das Datenbankherstellerrecht nach den §§ 87a ff. UrhG bietet keinen umfänglichen Schutz (hierzu näher Hetmank und Lauber-Rönsberg 2018, S. 578–579).

▶ **Praxistipp** KI selbst kann keine Urheberrechte innehaben. In Betracht käme allenfalls die Inhaberschaft von Urheberrechten der hinter der KI stehenden Personen (Nutzer, Programmierer oder Eigentümer). Relevant für die Zuordnung von Urheberrechten ist jedoch der Autonomiegrad der KI. Je komplexer und autonomer die KI, desto weniger Schutz besteht unter Umständen für die aus dem Einsatz der KI entstehenden Leistungen, weil die KI nicht mehr als „Werkzeug" der Person angesehen werden kann. Dies ist – genau wie im Patentrecht – das Problem der bestehenden Rechtslage. Leistungsschutzrechte, die nicht unmittelbar an eine persönliche geistige Schöpfung anknüpfen, werden daher im Zusammenhang mit KI-Leistungen an Bedeutung gewinnen. Eine Möglichkeit diesem Problem rechtlich zu begegnen, zeigen gesetzliche Regelungen zur Zuordnung von KI-Leistungen in England. Dort ist nicht die menschliche Schöpfung das entscheidenden Kriterium. Maßgeb-

[28] LG Berlin 30. Mai 1989, GRUR 1990, 270.

[29] Zu den Problemen bei der Bestimmung der Person des Rechteinhabers Dornis (2019, S. 1261–1263).

> lich ist vielmehr die Erzeugung einer Leistung durch einen Computer aufgrund der Veranlassung einer Person. Urheber ist entsprechend derjenige, der die erforderlichen Maßnahmen dafür trifft, dass der Computer das Werk erschaffen kann.[30]

6.3.3 Fazit

Die Herausforderungen, die diese Diskussionen mit sich bringen, sind – wie die Einleitung dieses Abschnitts zeigt – weit mehr als nur rechtspolitischer Natur. Es stellen sich ethische und ökonomische Fragen, deren Antworten die Rechtssysteme weltweit beeinflussen werden. Stehen immaterielle Schutzgüter nur Menschen zu oder auch intelligenten Maschinen? Soll die Maschine gleichrangig neben dem Menschen stehen oder handelt es sich allenfalls um einen vom Menschen abgeleiteten Schutz? Jedenfalls aus patentrechtlicher Perspektive ist zu fragen, ob für KI-Entwickler genügend Anreize bestehen, die technischen Entwicklungen auf diesem Gebiet voranzutreiben. Die Erstreckung des patentrechtlichen Schutzes auf KI als Patentgegenstand und/oder KI als Erfinder könnte daher geboten sein. Nationale Unterschiede könnten jedenfalls zu Verringerung oder gar Verlust der Wettbewerbsfähigkeit im KI-Bereich führen. Für eine belastbare Prognose und gesetzgeberische Handlungsempfehlung bedarf es aber in jedem Fall tiefergehender Untersuchungen, die nicht nur rechtlicher, sondern auch ökonomischer Natur sind.

Literatur

Ammann T (2017) Künstliche Intelligenz und ihre Herausforderungen bei der Gestaltung von IT-Verträgen. DSRITB 2017:503–515

Bräutigam P, Klindt T (2015) Industrie 4.0, das Internet der Dinge und das Recht. NJW 2015:1137–1142

Denga M (2018) Deliktische Haftung für künstliche Intelligenz. CR 2018:69–78

Dornis T (2019) Der Schutz künstlicher Kreativität im Immaterialgüterrecht. GRUR 2019:1252–1264

Eurpäisches Patentamt (Hrsg) (2019) Richtlinien für die Prüfung im Europäischen Parlament, November 2019. https://www.epo.org/law-practice/legal-texts/guidelines_de.html. Zugegriffen am 19.02.2020

Förster C (2019) In: Bamberger HG, Roth H, Hau W, Poseck R (Hrsg) BeckOK BGB, 52. Edition 2019, Band 3. C.H. Beck, München

Graf von Westphalen F (2018) Datenvertragsrecht – disruptive Technik – disruptives Recht. Kollisionsrecht und Haftungsrecht. IWRZ 2018:9–21

[30] Vgl. Sec. 9 (3) UK Copyright, Designs and Patents Act 1988: In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken.

Grützmacher M (2016) Die deliktische Haftung für autonome Systeme – Industrie 4.0 als Herausforderung für das bestehende Recht? Ein Plädoyer für die Nutzung von Beweislastregeln und wider den vorschnellen Ruf nach der Einführung einer Gefährdungshaftung. CR 2016:695–698

Hetmank S, Lauber-Rönsberg A (2018) Künstliche Intelligenz – Herausforderungen für das Immaterialgüterrecht. GRUR 2018:574–582

Horner S, Kaulartz M (2016) Haftung 4.0. Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme. CR 2016:7–14

Kühl E (2017) KI will rock you. https://www.zeit.de/digital/internet/2017-12/kuenstliche-intelligenz-musik-produktion-melodrive. Zugegriffen am 19.02.2020

Lauber-Rönsberg A (2019) Autonome „Schöpfung" – Urheberschaft und Schutzfähigkeit. GRUR 2019:244–253

Lederer T (2019) Patentierung im Bereich Künstlicher Intelligenz. GRUR-Prax 2019:152–154

Melullis K-J (2015) In: Benkard G (Hrsg) Patentgesetz, 11. Aufl., § 6 PatG, C.H. Beck, München

Ory S, Sorge C (2019) Schöpfung durch Künstliche Intelligenz? NJW 2019:710–713

Rebin I (2019) In: Gsell B, Krüger W, Lorenz S, Reymann C (GesamtHrsg.) beck-online.Grosskommentar, § 2 ProdHaftG. C.H. Beck, München

Spindler G (2011) In: Spindler G, Schuster F (Hrsg) Recht der elektronischen Medien, 2. Aufl., § 98 UrhG. C.H. Beck, München

Spindler G (2019) In: Gsell B, Krüger W, Lorenz S, Reymann C (GesamtHrsg.) beck-online.Grosskommentar, § 823 BGB. C.H. Beck, München

Wagner G (2017) In: Säcker FJ, Rixecker R, Oetker H, Limperg B (Hrsg) Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd 6, 7. Aufl., § 2 ProdHaftG. C.H. Beck, München

Steuerrechtliche Aspekte

7

Ulrike Bär

Zusammenfassung

Mit Hilfe künstlicher Intelligenz (KI) sollen Maschinen programmiert werden, so dass diese selbst lernen und Handlungen autonom ausführen. Dabei basiert KI auf Software und den damit verknüpften Rechten, d. h. auf immateriellen Vermögenswerten. Immaterielle Vermögenswerte unterliegen in Deutschland keiner eigenen, auf sie zugeschnitten Steuer, die sämtliche Vorgänge – Erwerb, Nutzung, Halten, Übertragung – für alle Rechtssubjekte einheitlich erfasst. Das deutsche Steuerrecht knüpft vielmehr durch unterschiedliche Steuerarten an einzelne Vorgänge an. So unterliegen die Nutzung und die entgeltliche Übertragung von immateriellen Vermögenswerten der Einkommensteuer oder Körperschaftsteuer, sowie der Gewerbesteuer und können auch Umsatzsteuer auslösen. Eine besondere steuerrechtliche Herausforderung im Kontext von KI ist, dass die steuerrechtlichen Regeln auf „brick and mortar" Unternehmen zugeschnitten sind. Infolgedessen stellen sich vor allem im Umgang mit Daten eine Reihe von ungeklärten, aber spannenden Fragen.

Das Forschungsumfeld der **künstlichen Intelligenz** (**KI**) hat sich zur Aufgabe gemacht, Maschinen so zu programmieren, dass sie in der Lage sind, menschliche Intelligenz zu erlangen (Hinerasky und Kurschildgen 2016, S. 38). KI arbeitet folglich nicht nur nach festgeschriebenen Programmcodes, sondern lernt dazu und führt gewünschte Handlungen autonom aus. KI basiert somit in erster Linie auf Software und den damit verknüpften Rechten, d. h. auf immateriellen Vermögenswerten. Immaterielle Vermögenswerte unterliegen in

U. Bär (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: ulrike.baer@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_7

Deutschland keiner eigenen, auf sie zugeschnitten Steuer, die sämtliche Vorgänge – Erwerb, Nutzung, Halten, Übertragung – für alle Rechtssubjekte einheitlich erfasst. Das deutsche Steuerrecht knüpft vielmehr durch unterschiedliche Steuerarten an einzelne Vorgänge an. So unterliegen die Nutzung und die entgeltliche Übertragung von immateriellen Vermögenswerten, insbesondere **Intellectual Property** (**IP**), der Einkommensteuer oder Körperschaftsteuer, sowie der Gewerbesteuer und können auch Umsatzsteuer auslösen.

Infolgedessen können sich in jedem Abschnitt des KI-Wertschöpfungsprozesses Steuerfolgen ergeben. Für Zwecke der steuerrechtlichen Beurteilung lässt sich der KI-Wertschöpfungsprozess in eine Schöpfungs- und eine Verwertungsphase aufteilen. In der Schöpfungsphase sind vor allem die Datenerhebung und – verarbeitung sowie die Entwicklung von KI-Software relevant, in der Verwertungsphase das am Markt erwirtschaftete Einkommen durch Veräußerung und Lizenzierung der entwickelten KI-Software sowie die entgeltliche Überlassung von Daten.

Bieten Unternehmen ihre Vermögenswerte, z. B. KI-generierte Daten, auf dem internationalen Markt an, löst dies oftmals Quellensteuer aus. Die Quellenbesteuerung sichert die Besteuerungsrechte des Staates, in dessen Territorium die Einkunftsquelle eines im Ausland ansässigen Vergütungsgläubigers liegt, indem der inländische Vergütungsschuldner zum Steuerabzug sowie zur Steuerabführung verpflichtet wird. Die Pflicht zum Steuerabzug an der sog. Quelle kann z. B. durch eine grenzüberschreitende Überlassung von KI-Software an einen inländischen Nutzer ausgelöst werden.

KI-Sachverhalte innerhalb einer Konzernstruktur geben Gestaltungsspielräume durch sog. Verrechnungspreise, d. h. die Preise, die für den Leistungsaustausch im Konzern vereinbart werden. Um mittels dieser Preise Verschiebungen von Steuersubstrat in andere Länder zu vermeiden, müssen die Vereinbarungen steuerrechtlich dem Fremdvergleichsgrundsatz entsprechen. Dies muss das jeweilige Konzernunternehmen für steuerrechtliche Zwecke auch dokumentieren.

Der Austausch von sonstigen Leistungen und Lieferungen eines Unternehmers an einen Abnehmer hat jedoch bei der Umsatzbesteuerung praktisch weitaus größere Relevanz. Entgeltliche Überlassungen von Daten bzw. KI-Systemen werfen in diesem Zusammenhang mehrere umsatzsteuerrechtliche Diskussionspunkte auf, auf die in diesem Kapitel ebenfalls eingegangen wird.

7.1 Ertragsteuerliche Beurteilung

7.1.1 Datenbeschaffung und ihre Bilanzierung

Die Erzeugung bzw. Generierung von großen Datenmengen ist Voraussetzung für den Lernprozess von KI und einer der ersten Schritte im Wertschöpfungsprozess eines Unternehmens. Bei der Datenbeschaffung ist der Datenerwerb von der Datenherstellung zu unterscheiden. Letztere kann originären oder derivativen Ursprungs sein. In der Regel erfolgt eine derivative Datenherstellung im Wege der Datenverarbeitung aus bereits vorhandenen Rohdaten. Hierzu zählen z. B. die Bereiche *Data Analytics* und *Data Mining*.

Mithilfe des *Data Analytics* werden gespeicherte, unstrukturierte und umfangreiche Datensammlungen (**Big Data**) analysiert oder um weitere Daten ergänzt und in neuen Zusammenhängen dargestellt bzw. ausgewertet. Mittels *Data Mining*s können die Analyseergebnisse sodann Prognosen über zukünftige Entwicklungen im unternehmerischen Tätigkeitsbereich liefern. Diese Schritte können KI in die Lage versetzen, das ihr anvertraute Problem autonom zu lösen. KI-basierte *Big-Data-Analysen* kommen mittlerweile in vielseitigen Bereichen zum Einsatz: In der Medizin dienen sie Ärzten bei der Entwicklung präziser und individueller Behandlungsmethoden. Sie werden als Sprachassistenten in elektronischen Geräten wie *Smartphones* oder *Personal Computern* verbaut, wo sie Anwenderwünsche autonom ausführen. Die Einsatzbereiche von KI weiten sich zudem stetig aus: beim autonomen Fahren soll KI zu mehr Sicherheit im Straßenverkehr beitragen, in einer Smart Factory soll sie durch intelligente Roboter die Effizienz der Produktion steigern, in der Verteidigung neue Lösungen ermöglichen, z. B. bei der Evakuierung von Verwundeten.

Liegt eine Pflicht zur Buchführung vor oder führt das Unternehmen freiwillig Buch, so sind steuerrechtliche Regeln bei der Bilanzierung und Bewertung einzelner Wirtschaftsgüter zu beachten (vgl. §§ 140 ff. **Abgabenordnung** (**AO**), 238 ff. **Handelsgesetzbuch** (**HGB**), 5 Abs. 1 **Einkommensteuergesetz** (**EStG**), 8 Abs. 1 **Körperschaftsteuergesetz** (**KStG**)). Diese Regeln dienen der Ermittlung der steuerrechtlichen Bemessungsgrundlage. Ob Vermögenswerte in der Steuerbilanz anzusetzen sind, hängt insbesondere davon ab, ob ein Wirtschaftsgut vorliegt, dem kein Bilanzierungsverbot entgegensteht. In einem weiteren Schritt wird das jeweilige Wirtschaftsgut der Höhe nach bewertet. Hierbei werden abnutzbare Wirtschaftsgüter des Anlagevermögens mit den Anschaffungs- oder Herstellungskosten angesetzt und ggf. um die sog. **Absetzung für Abnutzung** (**AfA**) gemindert (vgl. §§ 7 ff. EStG, 8 Abs. 1 KStG). Die AfA bewirkt, dass der Aufwand für die Anschaffung oder Herstellung eines abnutzbaren Wirtschaftsguts des Anlagevermögens über mehrere Jahre verteilt wird und somit der zunächst erfolgsneutrale Erwerb des Wirtschaftsguts über die AfA zu einer jährlich erfolgswirksamen Minderung der steuerrechtlichen Bemessungsgrundlage führt.

7.1.1.1 Daten als immaterielle Wirtschaftsgüter

Die Bilanzierung von Daten richtet sich nach § 5 Abs. 2 EStG, einer zentralen Bilanzierungsvorschrift für immaterielle Wirtschaftsgüter. Nach § 5 Abs. 2 EStG ist für Wirtschaftsgüter, bei denen es sich um immaterielle Wirtschaftsgüter handelt, ein Aktivposten nur anzusetzen, wenn sie dem Anlagevermögen zugerechnet werden und entgeltlich erworben wurden. Demzufolge müssen Daten nur und erst dann aktiviert werden, wenn sie Wirtschaftsgüter im Sinne dieser Vorschrift sind. Wirtschaftsgüter werden als „Werte" definiert, denen im Geschäftsverkehr ein selbstständiger wirtschaftlicher Vorteil beigemessen wird, der allein oder mit dem Betrieb gesondert veräußert werden kann und gesondert bewertbar ist.[1] Der immaterielle Charakter eines Wirtschaftsguts erfolgt dabei in Abgren-

[1] BFH, 12. Februar 2015, IV R 29/12, Rn. 14.

zung zu körperlich fassbaren Sachen, d. h. Sachanlagen des Aktivvermögens sowie Finanzanlagen. Können Daten als Vorteile für den Betrieb angesehen werden, deren Erlangung sich der Kaufmann etwas kosten lässt, so sind sie als Wirtschaftsgüter zu beurteilen. Aus der Sicht eines potenziellen Betriebserwerbers müssen Daten zudem einen eigenständigen Wert haben (Hennrichs 2018, Rn. 126) und als Gut bei wirtschaftlicher Betrachtungsweise und nach der Verkehrsauffassung (einzeln) verwertbar sein. Die Verkehrsfähigkeit wird bei der Verwertung durch Veräußerung oder anderweitig, z. B. durch Verarbeitung, Verbrauch oder Nutzungsüberlassung angenommen (Hennrichs 2018, Rn. 126). Beim Datenhandel wird zwar kein absolutes Recht an den Daten verschafft, die vertragliche Verschaffung einer faktischen Position ist für die Annahme einer Verkehrsfähigkeit aber ausreichend (vgl. Hennrichs 2018, Rn. 126).

7.1.1.2 Strukturierte und unstrukturierte Daten

Ob Daten einen wirtschaftlichen Vorteil für ein Unternehmen darstellen, orientiert sich nicht am Vorgang, der die Daten zum Wirtschaftsgut macht. Entscheidend ist, ob das Wirtschaftsgut selbst aufgrund seiner Aufgabe und Funktion einen betriebswirtschaftlichen Nutzen für das Unternehmen hat. Der wirtschaftliche Vorteil strukturierter Daten, ob personenbezogen oder maschinengeneriert, liegt in der Regel darin, dass sie für das Unternehmen schnell abrufbar sind und so betriebswirtschaftlich nutzbar gemacht werden können. Ein Unternehmen wird für die Erlangung solcher geordneten Daten Kosten aufbringen. Anders verhält es sich bei unstrukturierten Ansammlungen von Nummern oder Zahlen, die für Unternehmen im Zeitpunkt der Erhebung noch nicht handhabbar sind. Solche Datenbestände müssen erst durch weitere Softwareanwendungen verarbeitet werden, um wirtschaftlich nutzbaren Wert zu erlangen. Hier wird sich ein Unternehmen die Daten als Ausgangsrohstoffe nur etwas kosten lassen, wenn ihm dies leicht möglich oder sein Unternehmenszweck darauf gerichtet ist, Daten vorzusortieren und ihnen ein Ordnungssystem zu Grunde zu legen.

7.1.1.3 Beispiel zum Datentausch/Datenerwerb

Der Hersteller einer Turbine, die zur Erhebung technischer Daten mit einer Software ausgestattet wurde, baut diese in die Anlage eines Kunden ein. Die Turbine generiert mittels der Software bei ihrer Inbetriebnahme technische Daten. Werden diese maschinengenerierten Daten an den Hersteller zur Datenstrukturierung und weiteren Auswertung übermittelt, stellt sich die Frage, ob er sie als Wirtschaftsgüter § 5 Abs. 2 EStG entsprechend zu bilanzieren hat und welche sonstigen steuerrechtlichen Konsequenzen sich aus der Aktivierung als Wirtschaftsgut ergäben. Die Antwort hängt u. a. von den Vereinbarungen zwischen den Parteien ab. Daraus kann sich ergeben, dass die Datenübermittlung Teil der Gegenleistung, d. h. des „Kaufpreises“ ist, die der Erwerber der Turbine an den Hersteller zahlen muss. In diesem Fall lag dem Übermittlungsvorgang ein tauschähnlicher Vorgang zu Grunde. Aus Sicht des Herstellers wurden die Daten angeschafft. Sie wurden mit der Herstellung der Turbine „bezahlt“, sodass der Hersteller die Daten grds. in seinem Anlagevermögen zu aktivieren hat. Zugleich ergäbe sich beim Hersteller eine Ertragsrealisie-

rung in Höhe der Anschaffungskosten für die Daten. Nicht geklärt ist in diesem Zusammenhang, ob und wie der Wert dieser Daten zu bestimmen ist. § 6 Abs. 6 S. 1 EStG bestimmt dazu, dass im Falle eines Tausches der gemeine Wert des hingegebenen Wirtschaftsguts maßgebend ist. Der gemeine Wert wird durch den Preis bestimmt, der im gewöhnlichen Geschäftsverkehr nach der Beschaffenheit des Wirtschaftsguts bei einer Veräußerung zu erzielen wäre. Im konkreten Fall hilft diese Vorschrift jedoch nicht weiter, da es sich nicht um einen reinen Tausch (Turbine gegen Daten), sondern um einen Tausch mit Baraufgabe (Turbine gegen Geld und Daten) handelt. Um Diskussionen mit der Finanzverwaltung im Rahmen einer späteren Betriebsprüfung zu vermeiden und das Ertragsrisiko überschaubar zu gestalten, empfiehlt es sich, in den Vereinbarungen einen Wert für die Übermittlung der Daten festzulegen und die Grundlagen der Ermittlung dieses Wertes zu dokumentieren. Oftmals wird dieser Wert im Zeitpunkt der Übermittlung noch sehr gering sein.

Läge keine Anschaffung der Daten durch den Hersteller der Turbine vor, sondern eine eigene Herstellung, weil z. B. die Daten „heimlich" oder ohne ausdrückliche Vereinbarung an den Hersteller übermittelt werden, können sich ebenfalls Schwierigkeiten in der Bewertung ergeben. Dies gilt insbesondere dann, wenn die Daten beim Hersteller als Umlaufvermögen[2] einzuordnen wären. Dann fände das Aktivierungsverbot des § 5 Abs. 2 EStG keine Anwendung und die Daten müssten für ihren Ausweis in der Steuerbilanz bewertet werden. Maßstab bei selbst hergestellten Wirtschaftsgütern sind die Herstellungskosten (vgl. § 6 EStG). Zu den aktivierungspflichtigen Herstellungskosten zählen Material- und Fertigungskosten, die der Datenherstellung direkt zugeordnet werden könnten. Vor diesem Hintergrund sollten die Arbeitsschritte bei der „Datenherstellung" mit den zugehörigen angefallenen Kosten sorgfältig dokumentiert werden, um eine steuerliche Anerkennung der Herstellungskosten zu gewährleisten.

7.1.1.4 Beispiel zur Datenherstellung

Unterzieht der Hersteller der Turbine die erworbenen technischen Rohdaten nun einem weiteren Datenverarbeitungsvorgang, der die unstrukturierten Daten ordnet, stellt er aus ihnen wiederum neue Daten her. Verbleiben diese Daten im Anlagevermögen des Herstellers, weil er sie dazu bestimmt hat, dem Geschäftsbetrieb dauernd zu dienen, dürfen sie gemäß § 5 Abs. 2 EStG nicht bilanziert werden. Sind die neu hergestellten Daten hingegen dem Umlaufvermögen zuzuordnen, da sie als Wirtschaftsgüter zur sofortigen Veräußerung bestimmt sind, werden sie regelmäßig mit den Herstellungskosten anzusetzen sein.

[2] Der Begriff des Anlagevermögens ist durch das Merkmal „dauernd dem Geschäftsbetrieb dienen" definiert, § 247 Abs. 2 HGB. Im Umkehrschluss werden Gegenstände, die dem Geschäftsbetrieb nur vorübergehend zu dienen bestimmt sind, dem Umlaufvermögen zugerechnet. Nach R. 6.1 Abs. 2 Einkommensteuer-Richtlinie (EStR) gehören zum Umlaufvermögen die Wirtschaftsgüter, die zur Veräußerung, Verarbeitung oder zum Verbrauch angeschafft oder hergestellt worden sind.

Ein weiteres Beispiel selbst hergestellter, „neuer Daten“ ist das oben bereits erwähnte *Data Mining*. Hat das Unternehmen durch *WebCrawling*[3] Daten gesammelt, ohne dafür eine Gegenleistung zu erbringen, sind die gesammelten Daten ebenfalls selbst geschaffene immaterielle Wirtschaftsgüter.

7.1.1.5 Personenbezogene Nutzerdaten

Auch personenbezogene Nutzerdaten können nach den obigen Rechtsprechungsgrundsätzen werthaltige immaterielle Vermögenswerte darstellen. Unter Umständen können sich auch dann steuerrechtlich Bewertungsfragen stellen. Willigt der Nutzer wirksam in die Datenüberlassung/-verwertung ein, geschieht dies allerdings oftmals aus der Notwendigkeit, den eigentlichen Vertragsgegenstand überhaupt nutzen zu können. Aus steuerrechtlichem Blickwinkel läge dann eine unentgeltliche Datenüberlassung vor. Die Frage der Bewertung der Daten für steuerrechtliche Zwecke stellte sich dann nicht. Anders liegt der Fall, wenn das Unternehmen Nutzerdaten aufbereitet, um die aufbereiteten Daten zu veräußeRn. Durch die Aufbereitung wird ein „neues“ Wirtschaftsguts hergestellt, das dem Umlaufvermögen zuzuordnen wäre. Mangels Eingreifens des Aktivierungsverbots im Sinne des § 5 Abs. 2 EStG müsste es aktiviert und daher auch bewertet werden.

7.1.1.6 Fazit

Die steuerbilanzielle Behandlung der Datenbeschaffung ist noch weitgehend ungeklärt. Je nachdem welche Werte im Raum stehen, kann es sich daher anbieten, für bestimmte Sachverhalte eine verbindliche Auskunft zu beantragen (§ 89 AO), um spätere böse Überraschungen im Rahmen einer Betriebsprüfung zu vermeiden. Zu beachten ist, dass die verbindliche Auskunft nur für einen zukünftigen, noch nicht realisierten Sachverhalt beantragt werden kann und eine erteilte Auskunft nur dann Bindungswirkung entfaltet, wenn der später verwirklichte Sachverhalt dem in dem Antrag darstellten entspricht.

7.1.2 Verwertung von Daten/KI im Ertragsteuerrecht

Im Hinblick auf das Ertragsteuerrecht ist die Verwertungsphase eines KI-Unternehmens vor allem dadurch gekennzeichnet, dass geschaffene Vermögenswerte wie Daten und KI-Systeme am Markt nutzbar gemacht werden. Die entgeltliche Datenüberlassung bzw. Veräußerung oder Lizenzierung von KI-Systemen führt zu einem Einkommenszuwachs, welcher durch Ertragsteuerarten wie die Einkommensteuer, Körperschaftsteuer sowie die Gewerbesteuer abgeschöpft wird.

Im Ertragsteuerbereich hängt die Besteuerung maßgeblich von der Rechtsform sowie der Ansässigkeit des Inhabers der Vermögenswerte ab. Während das Einkommensteuerge-

[3] Beim *WebCrawling* verwenden Suchmaschinenbetreiber ein automatisiertes Programm, das den Inhalt diverser Webseiten scannt, analysiert und in den Suchindex des Suchmaschinensystems einspeist (Roggenkamp 2006, S. 405).

setz die Besteuerung des Einkommens natürlicher Personen regelt, enthält das Körperschaftsteuergesetz Bestimmungen zur Besteuerung des Einkommens von juristischen Personen wie Kapitalgesellschaften. Personengesellschaften, insbesondere die **offene Handelsgesellschaft** (**OHG**), **Kommanditgesellschaft** (**KG**) und die **Gesellschaft des bürgerlichen Rechts** (**GbR**) sind weder einkommen- noch körperschaftsteuerpflichtig. Sie sind insoweit transparent. Ihre Einkünfte werden den Gesellschaftern zugerechnet und dort versteuert.

7.1.2.1 Natürliche Person als Inhaber

Natürliche Personen, die in Deutschland ansässig sind, sind gemäß § 1 Abs. 1 S. 1 EStG unbeschränkt einkommensteuerpflichtig. Steuergegenstand sind die in § 2 Abs. 1 S. 1 EStG aufgelisteten Einkünfte. Unterschieden wird zwischen zwei Kategorien von Einkünften: Gewinn- und Überschusseinkünften. Bedeutung hat die Unterscheidung für Art und Umfang der Einkünfteermittlung. In welche Kategorie Erträge aus der Verwertung von KI fallen, hängt davon ab, ob die zugrunde liegenden Vermögenswerte im steuerrechtlichen Betriebs- oder Privatvermögen gehalten werden.

Zu den Gewinneinkünften zählen gemäß § 2 Abs. 2 S. 1 Nr. 1 EStG insbesondere Einkünfte aus Gewerbebetrieb, §§ 15–17 EStG, sowie Einkünfte aus selbstständiger Arbeit, § 18 EStG. Überschusseinkünfte umfassen u. a. Einkünfte aus Vermietung und Verpachtung, § 21 EStG, Einkünfte aus privaten Veräußerungsgeschäften, §§ 22 Nr. 2, 23 EStG und Einkünfte aus nichtselbstständiger Arbeit, § 19 EStG.

Befinden sich Daten oder KI-Systeme im Betriebsvermögen eines Unternehmers, so stellen Vergütungen für jegliche Verwertungsvorgänge Einkünfte aus Gewerbebetrieb dar. Bei natürlichen Personen wie Erfindern, Ingenieuren oder selbstständigen Wissenschaftlern, kann eine Lizenzvergabe oder Veräußerung zu Einkünften aus selbstständiger Tätigkeit führen, § 18 EStG. Bedeutung hat die Unterscheidung für die Gewerbesteuer: Einkünfte aus nicht selbständiger Tätigkeit sind nicht gewerbesteuerpflichtig.

Wird KI-Software im Privatvermögen gehalten, kommen Einkünfte aus Vermietung und Verpachtung gemäß § 21 Abs. 1 S. 1 Nr. 3 EStG (z. B. durch Lizenzierung) oder sonstige Einkünfte aus privatem Veräußerungsgeschäft gemäß §§ 22 Nr. 2, 23 EStG oder aus Zufallserfindungen, § 22 Nr. 3 EStG, in Betracht. Zu den Überschusseinkünften gehören auch arbeitgeberseitig gezahlte Erfindervergütungen, die als Einkünfte aus nichtselbständiger Arbeit im Sinne des § 19 EStG qualifiziert werden.

7.1.2.2 Steuerrechtliche Zuordnung von KI-Software

Bei den Gewinneinkünften wird der zu versteuernde Gewinn grds. als Unterschiedsbetrag zwischen dem Betriebsvermögen am Schluss des Wirtschaftsjahres und dem Betriebsvermögen am Schluss des vorangegangenen Wirtschaftsjahres ermittelt, d. h. es sind sämtliche „Betriebsvermögenszuwächse“ zu erfassen und zu versteuern. Grundlage für die Ermittlung des Betriebsvermögens ist die Steuerbilanz und die darin enthaltenen Wirtschaftsgüter. Welche Wirtschaftsgüter sie enthält, bestimmt sich nach den Regeln über die Zurechnung von Wirtschaftsgütern, § 39 AO.

Im Fall der Verwertung von KI-Software kommt es für den Umfang und Zeitpunkt eines „Betriebsvermögenszuwachses“ darauf an, ob die Software steuerrechtlich betrachtet im Wege einer Veräußerung oder im Wege der Einräumung eines Nutzungsrechts verwertet wird. Die vertragliche Bezeichnung durch die Parteien ist für diese steuerrechtliche Unterscheidung nicht maßgebend. Eine Veräußerung führt steuerrechtlich zur Aufdeckung sämtlicher stiller Reserven der Software. Die Software scheidet als Wirtschaftsgut aus der Bilanz des Veräußernden aus. Eine Nutzungsüberlassung hingegen führt zu Ertragsrealisierung „nur“ in Höhe des vereinbarten Entgelts. Die Software ist steuerrechtlich weiterhin dem Lizenzgeber zuzurechnen und daher in seiner Bilanz zu aktivieren.

Gerade für den Bereich von Software stellen sich oftmals Fragen der Zurechnung und damit des Umfangs des Betriebsvermögenszuwachses, d. h. der Ertragsrealisierung. Die Zurechnung eines Wirtschaftsguts erfolgt grds. beim zivilrechtlichen Eigentümer, § 39 Abs. 1 AO. Das Steuerrecht kennt neben dem zivilrechtlichen Eigentum jedoch auch das sog. „wirtschaftliche Eigentum“. Fällt beides auseinander, ist für die steuerrechtliche Zurechnung das wirtschaftliche Eigentum maßgebend, vgl. § 39 Abs. 2 Nr. 1 AO.

Vorsicht ist daher bei der Lizenzierung von KI-Software geboten. Bei der Einräumung eines Nutzungsrechts an der KI-Software wird trotz fehlenden rechtlichen Eigentums dem Lizenznehmer das wirtschaftliche Eigentum zugewiesen, wenn dieser über das Wirtschaftsgut die tatsächliche Herrschaft in der Weise ausübt, dass er den rechtlichen Eigentümer im Regelfall für die gewöhnliche Nutzungsdauer von der Einwirkung auf das Wirtschaftsgut wirtschaftlich ausschließen kann. Dies beurteilt sich nach dem Gesamtbild der vertraglichen Vereinbarung (Brühl 2020, § 39 AO, Rn. 92). Kriterien sind hierfür insbesondere die Laufzeit und Art des Lizenzvertrags, das Lizenzentgelt sowie bei wem die Chancen und Risiken aus dem Geschäft liegen und ob Rechte zur Einräumung von Unterlizenzen, ordentliche und außerordentliche Kündigungsrechte und Kaufoptionsrechte eingeräumt wurden (Greinert und Metzner 2015, S. 257). Eine Besonderheit gilt in diesem Kontext für das Urheberrecht, welches nach § 29 UrhG unveräußerlich ist. Scheidet die Veräußerung eines Rechts von Gesetzes wegen aus, entsteht grds. auch kein wirtschaftliches Eigentum im Sinne des § 39 Abs. 2 Nr. 1 AO beim Erwerber.

7.1.2.3 KI-Systeme: getrenntes oder einheitliches Wirtschaftsgut?

Grundsätzlich wird Software wegen der im Vordergrund stehenden geistigen Leistung als immaterielles Wirtschaftsgut behandelt. Besteht ein Wirtschaftsgut aus einem materiellen und einem immateriellen Bestandteil, so gilt der Grundsatz, dass die Bestandteile als getrennte Wirtschaftsgüter zu behandeln sind. Stellt das körperliche Substrat aber einen unselbstständigen Teil des immateriellen Wirtschaftsguts dar oder ist die funktions- oder wertmäßige Trennung der Bestandteile nicht möglich, werden die Bestandteile einheitlich als ein immaterielles Wirtschaftsgut bilanziert, wenn der geistige Gehalt im Vordergrund steht. Diese Grundsätze gelten auch bei der Frage, ob Hardware und Software bei KI-Technologien als einheitliches immaterielles Wirtschaftsgut bilanziert werden dürfen. Als Kriterien für eine Zuordnung können das Wertverhältnis zwischen den

Kosten für die körperliche Substanz und dem Wert des verkörperten geistigen Werks, sowie die Verkehrsauffassung herangezogen werden (Hennrichs 2013, § 246 HGB Rn. 61).

7.1.2.4 Unterscheidung zwischen Standard- und Individualsoftware

Die Bilanzierung als immaterielles Wirtschaftsgut erfolgt unabhängig davon, ob es sich um System- oder Anwendungssoftware handelt. Bedeutung hat die Unterscheidung für Zwecke der Abschreibung.

Anwendungssoftware beschreibt alle Programme, die die Datenverarbeitungsaufgaben des Anwenders lösen, während Systemprogramme allein zum Betreiben des Computers eingesetzt werden (Schmidl 2014, Anwendungsprogramm). Zu den Systemprogrammen zählt die Gruppe der Betriebssysteme, wie Microsoft Windows, Mac OS X oder Linux. Da KI-Software letztlich dem Ziel dient, intelligente Lösungen für spezielle Anwenderprobleme zu finden, ist sie als Anwendungssoftware zu klassifizieren. Anwendungssoftware wird zusätzlich in Standard- und Individualsoftware unterteilt. Standardsoftware liegt vor, wenn ein fertiges Computerprogramm dem Anwender zur Nutzung überlassen wird, auch wenn für den individuellen Gebrauch durch den Anwender weitere Anpassungen vorgenommen werden. Hierzu zählt beispielsweise das Microsoft Office-Packet. Individualsoftware liegt demgegenüber vor, wenn der Anbieter der Software im Auftrag des Kunden eine individuelle Anwendung der bereits hergestellten Basissoftware zur Lösung spezieller Anwenderbedürfnisse schafft. Wird die Standardsoftware wiederum individualisiert, z. B. durch ein ***Enterprise – Resource – Planning Programm (ERP)***, also einer Zusammenstellung verschiedener Module, die der Optimierung von Geschäftsprozessen dienen, so wird die *ERP-Software* als einheitliches immaterielles Wirtschaftsgut klassifiziert.[4] Grund hierfür ist, dass bei *ERP-Software* von einem einheitlichen Nutzungs- und Funktionszusammenhang ausgegangen wird. Zukünftig wird sich der ERP- Markt zu intelligenten ERP-Lösungen weiterentwickeln und dem Kunden neben standardisierten KI-Funktionen die Möglichkeit bieten, KI-Technologien individuell anzuwenden (bitkom 2019, S. 6, 23). Je spezifischer die Aufgabenstellung für die KI, desto aufwändiger muss sie zur Aufbereitung der Daten trainiert werden und umso umfangreicher fällt ihr Lernprozess aus. Je nach Fallgestaltung werden zukünftige intelligente ERP-Lösungen daher als Standard- oder Individualsoftware zu klassifizieren sein. Dabei wird Standardsoftware regelmäßig über einen Zeitraum von 3 Jahren abgeschrieben (Krumm 2019, § 5 EStG, Rn. 644), Individualsoftware und ERP-Software über einen Zeitraum von 5 Jahren.[5] Die sich überschlagenden Entwicklungszyklen im Softwarebereich führen zudem nicht selten dazu, dass vor Ablauf der betriebsgewöhnlichen Nutzungsdauer außerplanmäßig nach § 7 Abs. 1 S. 7 EStG wegen außergewöhnlicher, wirtschaftlicher Abnutzung abgeschrieben werden darf.

[4] BMF, Schreiben vom 18. November 2005, IV B 2 – S 2172 – 37/05, Rn. 2.

[5] BMF, Schreiben vom 18. November 2005, IV B 2 – S 2172 – 37/05, Rn. 22.

7.1.2.5 KI-Software: Herstellung oder entgeltliche Anschaffung?

In der Praxis führt insbesondere die „Auftragsentwicklung“ von KI-Sofware immer wieder zu Schwierigkeiten. In erster Linie geht es dabei um die Abgrenzung, ob der Auftraggeber die KI-Software aus steuerrechtlicher Sicht selbst hergestellt oder ob er sie angeschafft hat. Bedeutung hat die Frage für die Aktivierungspflicht der KI-Software beim Auftraggeber und daran anknüpfend für den Umfang seines Betriebsausgabenabzugs.

Der Erwerb eines immateriellen Wirtschaftsguts mit anschließender Aktivierungspflicht liegt vor, wenn die Herstellung der KI-Software auf Basis eines Werkvertrags in Auftrag gegeben wurde. Eine Auftragsentwicklung auf Basis eines „Werkvertrags“ teilt das Herstellungsrisiko der Sphäre des Herstellers zu und verpflichtet ihn, das hergestellte immaterielle Wirtschaftsgut an den Auftraggeber zu veräußern. Der Hersteller hat folglich die Herstellungskosten im Umlaufvermögen zu aktivieren. Die Gewinnrealisierung tritt beim ihm mit Abnahme der KI-Software ein. Beim Auftraggeber wird die werkvertragliche Vergütung als Anschaffungskosten für das Wirtschaftsgut „KI-Software“ aktiviert. Sie wirkt sich nur ratierlich über Abschreibungen als Betriebsausgabe aus.

Hiervon abzugrenzen ist die Auftragsentwicklung auf Basis eines Dienstvertrags, wo das Herstellungsrisiko beim Auftraggeber verbleibt. Diese Konstellation ist einer Eigenherstellung vergleichbar. In steuerlicher Hinsicht greift das Aktivierungsverbot des § 5 Abs. 2 EStG. Die vereinbarten Vergütungen können beim Auftraggeber nicht als Herstellungskosten aktiviert werden, sondern stellen sofort abziehbare Betriebsausgaben dar (Backu und Bayer 2017, Rn. 52).

Denkbar ist eine Softwareherstellung auch in dem Fall, dass KI durch autonomes Lernverhalten ihre eigene Software über den ursprünglichen Zustand hinaus derart umfangreich verändert, dass diese wesensveränderte Software bilanziell unter dem Gesichtspunkt der Softwareherstellung neu zu bewerten ist. Ob die wesensveränderte Software dem zivilrechtlichen bzw. wirtschaftlichen Eigentümer der KI-Software vor Wesensänderung zuzurechnen ist, hängt insbesondere von den vertraglichen Vereinbarungen der Parteien ab. Steuerrechtlich greift das Aktivierungsverbot, wenn die neu hergestellte KI-Software dem Anlagevermögen zuzurechnen ist. Im Unterschied zur umfangreichen Wesensänderung sind Kosten im Zusammenhang mit Modifikationen, Erweiterungen oder Verbesserung einzelner Funktionen so zu behandeln und daher ggf. zu bilanzieren, wie die ursprünglich angesetzte Software (Zwirner et al. 2019, S. 7). Indizien für Erweiterungen bzw. Verbesserungen sind z. B., dass der Software eine zusätzliche Funktion zukommt, ihr Anwendungsbereich erweitert wurde oder wesentliche Änderungen am Quellcode bzw. Umprogrammierungen im Programmablauf vorgenommen wurden.[6] Kann die Software auf der Grundlage der bisherigen Lizenz weiter genutzt werden, spricht dies zusätzlich gegen eine Wesensveränderung.[7]

[6] BMF, Schreiben vom 18. November 2005, IV B 2-S 2172-37/05, Rn. 8.

[7] BMF, Schreiben vom 18. November 2005, IV B 2-S 2172-37/05, Rn. 10.

7.1.2.6 Personengesellschaft als Inhaber

Eine Personengesellschaft ist einkommen- (und körperschaft)steuerrechtlich transparent. Ihre Einkünfte werden den jeweiligen Gesellschaftern entsprechend ihrer Beteiligungsverhältnisse anteilig zugerechnet und dort versteuert.

Bei einer originär gewerblich tätigen oder gewerblich geprägten Personengesellschaft stellen Einnahmen aus KI-Systemen Einkünfte aus Gewerbebetrieb dar. Der erwirtschaftete Gewinn wird den Gesellschaftern, steuerrechtlich den sog. „Mitunternehmern", entsprechend ihres Gewinnanteils zugerechnet und unterliegt in Abhängigkeit von der Rechtsform des einzelnen Mitunternehmers der Einkommen- oder Körperschaftsteuer. Gleiches gilt für Veräußerungen aus dem Gesamthandvermögen.

Anderes gilt für die Gewerbesteuer (dazu näher Abschn. 7.1.4). Soweit die Einkünfte gewerbesteuerpflichtig sind, ist die Personengesellschaft selbst Steuerschuldner.

7.1.2.7 Sonderfall Betriebsaufspaltung

Eine Betriebsaufspaltung ist anzunehmen, wenn ein Unternehmen (Besitzunternehmen) mindestens eine wesentliche Betriebsgrundlage an eine gewerblich tätige Personen- oder Kapitalgesellschaft (Betriebsunternehmen) zur Nutzung überlässt (sachliche Verflechtung) und eine Einzelperson oder mehrere Personen zusammen (Personengruppe) sowohl das Besitz- als auch das Betriebsunternehmen dergestalt beherrschen, dass sie in der Lage sind, in beiden Unternehmen einen einheitlichen geschäftlichen Betätigungswillen durchzusetzen (personelle Verflechtung) (Wittkowski 2018, Rn. 570).

Eine Nutzungsüberlassung von KI-Software kann ungewollt oder zum Teil unwissentlich zu einer solchen Betriebsaufspaltung führen. So kann in der Anfangsphase eines KI-Unternehmens zunächst auf der Ebene eines Gesellschafters eine KI-Software entwickelt worden sein, die anschließend dem später gegründeten Betriebsunternehmen entgeltlich zur Nutzung überlassen wird. Stehen die Wirtschaftsgüter im zivilrechtlichen Eigentum nur eines Gesellschafters, wird durch das Rechtsinstitut der Betriebsaufspaltung ein Einzelunternehmen dieses Gesellschafters im steuerlichen Sinne begründet. Dies hat zur Folge, dass die Einkünfte, die der Gesellschafter aus der Nutzungsüberlassung der KI-Software an die später gegründete Betriebsgesellschaft erzielt, gewerbliche Einkünfte darstellen. Letztlich wird durch das Institut der Betriebsaufspaltung eine der Art nach vermögensverwaltende Tätigkeit des Besitzunternehmens in eine gewerbliche Tätigkeit umqualifiziert und der Gewerbesteuer unterworfen.

Die Betriebsaufspaltung führt zu einer steuerlichen Verstrickung der überlassenen Wirtschaftsgüter, indem diese steuerlich dem Betriebsvermögen zugerechnet werden. Wird das Vorliegen der Betriebsaufspaltung nicht erkannt, droht die Gefahr einer ungewollten Beendigung der Betriebsaufspaltung mit der Folge, dass die im Betriebsvermögen enthaltenen stillen Reserven aufgedeckt und versteuert werden müssen. Eine Beendigung kann z. B. dadurch eintreten, dass die personelle Verflechtung durch Veräußerung/unentgeltliche Übertragung der Beteiligung an der Betriebsgesellschaft gelöst wird.

7.1.2.8 Körperschaft als Inhaber

In Deutschland erzielen unbeschränkt steuerpflichtige Körperschaften stets Einkünfte aus Gewerbebetrieb, § 8 Abs. 2 KStG, und sind damit körperschaftsteuerpflichtig, §§ 1, 2 KStG, und gemäß § 2 Abs. 1 S. 1 **Gewerbesteuergesetz** (**GewStG**) gewerbesteuerpflichtig. Ist also der Lizenzgeber oder Veräußerer von KI-Software eine Kapitalgesellschaft, erzielt diese stets gewerbliche Einkünfte. Gleiches gilt für die entgeltliche Überlassung/Übertragung von Daten. In Deutschland nicht ansässige Körperschaften sind hingegen nur mit den Einkünften, die sie in Deutschland erzielen, gemäß § 2 Nr. 1 KStG beschränkt körperschaftsteuerpflichtig. Auch sie können der Gewerbesteuer unterliegen, sofern sie im Inland eine Betriebsstätte unterhalten, § 2 Abs. 1 S. 3 GewStG.

7.1.3 Quellensteuer

Unternehmen kooperieren vielfach in Querschnittstechnologien wie der KI und stellen ihre Systeme zur Weiterentwicklung und Verwertung anderen Unternehmen entgeltlich zur Nutzung zur Verfügung. So kann ein Unternehmen z. B. seine auf KI-Software basierende Technologie zum Parkraum-Management um eine KI-Software zur Spracherkennung erweitern bzw. fortentwickeln, um sie anschließend in bearbeiteter Form kommerziell zu vertreiben.

Ist der Inhaber der KI-Software ein im Ausland ansässiges Unternehmen und lizenziert dieses Unternehmen die KI-Software an ein im Inland ansässiges Unternehmen, wird das ausländische Unternehmen durch die Lizenzierung mit dem erzielten Entgelt, d. h. der Lizenzgebühr, grds. in Deutschland beschränkt steuerpflichtig. Die daraus resultierende Einkommensteuer- oder Körperschaftsteuerpflicht des Lizenzgebers wird dann unter bestimmten Voraussetzungen durch die Pflicht des Lizenznehmers zur Einbehaltung und Abführung der Steuer „an der Quelle“, d. h. durch Abzug der Steuer von der zu zahlenden Lizenzgebühr, abgegolten, vgl. § 50 Abs. 2 S. 1 EStG i. V. m. § 50a Abs. 1 Nr. 3 EStG. Soweit inländische Einkünfte vorliegen, das Gesetz jedoch keinen Quellensteuerabzug vorsieht, wird die Steuer im Wege der Veranlagung erhoben.

7.1.3.1 Inländische Einkünfte nach § 49 EStG

Die beschränkte Steuerpflicht setzt zum einen voraus, dass eine natürliche Person weder

Wohnsitz noch gewöhnlichen Aufenthalt bzw. eine Kapitalgesellschaft weder Sitz noch Geschäftsleitung im Inland hat und dass „inländische Einkünfte“ im Sinne des § 49 EStG erzielt werden. Die Struktur des § 49 EStG orientiert sich an den Einkünften des § 2 EStG, d. h. der Liste für unbeschränkt Steuerpflichtige, verlangt aber zusätzlich einen Inlandsbezug als Rechtfertigung für eine Besteuerung. Danach handelt es sich bei Einkünften aus Gewerbebetrieb dann um inländische Einkünfte, wenn im Inland eine Betriebsstätte unterhalten wird oder ein ständiger Vertreter bestellt ist, vgl. § 49 Abs. 1 Nr. 2 Buchst. a EStG. Bei der Veräußerung bzw. Vermietung und Verpachtung von Rechten im Betriebsvermögen liegen Einkünfte aus Gewerbebetrieb vor, wenn die überlassenen Rechte im

Inland belegen sind,[8] vgl. § 49 Abs. 1 Nr. 2 Buchst. f Doppelbuchst. aa, bb EStG. Einkünfte aus der Nutzungsüberlassung von rechtlich nicht geschützten Positionen wie Know-how unterfallen § 49 Abs. 1 Nr. 9 EStG, wenn sie im Inland genutzt werden oder worden sind. Wird **geistiges Eigentum** (**IP**) im steuerlichen Privatvermögen gehalten und gegen Entgelt überlassen, kommt eine beschränkte Steuerpflicht gemäß § 49 Abs. 1 Nr. 6 EStG in Betracht, wenn die überlassenen Rechte in Deutschland „belegen", in ein inländisches Register eingetragen sind oder in einer inländischen Betriebsstätte oder Einrichtung verwertet werden. Private Veräußerungsgeschäfte von geistigen Eigentumsrechten begründen hingegen grds. keine beschränkte Steuerpflicht.

7.1.3.2 Überlassung von Nutzungsrechten

Das Steuerabzugsverfahren nach § 50a Abs. 1 S. 1 Nr. 3 EStG setzt eine Überlassung der Nutzung oder des Rechts auf Nutzung von Rechten voraus. Erfasst wird nur die zeitlich begrenzte Nutzungsüberlassung, nicht aber die Übertragung des Rechts. Infolgedessen ist die Abgrenzung zwischen Nutzungsüberlassung und Übertragung für die Frage des Quellensteuerabzugs virulent. Eine Nutzungsüberlassung setzt dabei voraus, dass das Recht nach Ablauf der Nutzungsberechtigung an den Lizenzgeber zurückfällt und dem Recht in diesem Zeitpunkt auch noch ein wirtschaftlicher Wert beigemessen werden kann, d. h. es nicht „verbraucht" ist. Für den Bereich der Urheberrechte hat dies zur Konsequenz, dass bei ihrer grenzüberschreitenden Überlassung grds. Quellensteuer ausgelöst wird. Sie sind bereits zivilrechtlich unveräußerlich. Nach Ansicht des BFH kann grds. auch kein wirtschaftliches Eigentum übertragen werden, so dass ungeachtet der zivilrechtlichen Vereinbarungen der Parteien steuerrechtlich immer von einer Nutzungsüberlassung auszugehen ist.

Ein weiteres Problem, das sich insbesondere bei der Überlassung von (KI-)Software in der Praxis oftmals ergibt, ist die Abgrenzung einer „Rechteüberlassung" von sonstigen Dienstleistungen. Letztere lösen keine Quellensteuer aus. Das BMF hat dazu mit Schreiben vom 27.10.2017[9] Stellung genommen. Danach ist erforderlich, dass dem Nutzer umfassende Nutzungsrechte an der Software zur wirtschaftlichen Weiterverwertung eingeräumt werden. Dies können insbesondere Vervielfältigungs-, Bearbeitungs-, Verbreitungs- oder Veröffentlichungsrechte sein. Allein das Recht zum Vertrieb einzelner Programmkopien ohne weitergehende Nutzungs- und Verwertungsrechte an der Software selbst reicht nicht aus. Ferner ist als Negativkriterium zu berücksichtigen, dass die Software nicht lediglich zum „bestimmungsgemäßen Gebrauch" überlassen wird. Folglich fehlt es an einer Rechteüberlassung, wenn die Software lediglich installiert wird oder im Arbeitsspeicher heruntergeladen wird. Gleiches gilt bei bloßer Softwareanwendung bzw. notwendigen Bearbeitungs- oder Vervielfältigungshandlungen für eine Softwareanwendung (Warnke 2018, S. 70). Wird im obigen Beispiel die Spracherkennungssoftware mit

[8] Inlandsbezug durch Eintragung in ein deutsches Register (Patentregister etc.) oder Verwertung in einer inländischen Betriebsstätte oder Einrichtung eines Dritten.

[9] BMF, Schreiben vom 27. Oktober 2017, IV C 5-S 2300/12/10003:004.

der Erlaubnis zur Fortentwicklung und zum kommerziellen Vertrieb[10] überlassen und nicht lediglich zum bestimmungsgemäßen Gebrauch, ggf. auch innerhalb des Konzerns für eigenbetriebliche Zwecke,[11] liegt eine Rechteüberlassung vor, die Quellensteuer nach § 50a Abs. 1 Nr. 3 EStG auslöst.

7.1.3.3 Pflichten im Abzugsverfahren nach § 50a Abs. 1 Nr. 3 EStG

Liegen die Voraussetzungen des § 50a Abs. 1 Nr. 3 EStG vor, hat der Vergütungsschuldner, d. h. der Lizenznehmer der KI-Software, den Steuerabzug von der Bruttovergütung mit einem Steuersatz von 15 %, zzgl. 5,5 % **Solidaritätszuschlag** (**SolZ**) vorzunehmen, vgl. § 50a Abs. 2 S. 1 EStG, § 3 Abs. 1 Nr. 6 und §§ 4, 5 SolZG (sog. **Bruttoprinzip**). Mit dem Gesetz zur Rückführung des Solidaritätszuschlags vom 10.12.2019[12] wird der Solidaritätszuschlag allerdings ab dem Veranlagungszeitraum 2021 für natürliche Personen weitestgehend abgeschafft. Die Neuregelungen lassen jedoch nicht eindeutig erkennen, inwieweit beschränkt Steuerpflichtige im Rahmen des Steuerabzugsverfahren nach § 50a EStG hiervon profitieren werden. Neben dem Bruttoprinzip hat das BMF[13] für EU-Angehörige verfügt, dass das in § 50a Abs. 3 EStG normierte „Nettoprinzip" über den Wortlaut der Vorschrift hinaus entsprechend bei Rechteüberlassungen im Sinne des § 50a Abs. 1 Nr. 3 EStG angewendet werden darf. Bei Anwendung des Nettoprinzips ist Bemessungsgrundlage für den Steuerabzug die Bruttovergütung abzüglich etwaiger Betriebsausgaben und Werbungskosten, die in unmittelbarem wirtschaftlichem Zusammenhang mit der inländischen Vergütung stehen. Bei diesem „Nettoabzug" beträgt der anzuwendende Steuersatz 30 %, wenn der Gläubiger der Vergütung eine natürliche Person ist; ansonsten bleibt es bei dem Steuersatz von 15 %.

Der Steuerabzug ist im Zeitpunkt des Zuflusses der Vergütung vorzunehmen, § 50a Abs. 5 S. 1 EStG, bei Verrechnung mit einer Gegenforderung im Zeitpunkt der Verrechnung, § 73c Nr. 1 EStDV. Neben der Abzugsverpflichtung hat der Vergütungsschuldner auch eine Steueranmeldung abzugeben. Die Pflichten aus dem Abzugsverfahren greifen auch dann, wenn das deutsche Besteuerungsrecht durch ein **Doppelbesteuerungsabkommen** (**DBA**) ausgeschlossen oder beschränkt wird, § 50d Abs. 1 S. 1 EStG, oder sich eine Entlastung von der Quellensteuer aus der Zins- und Lizenz-Richtlinie ergibt. Um in den Genuss der Entlastung von der Quellensteuer zu kommen, d. h. die vollständige oder überschießende Steuererhebung auf das materiell-rechtlich zulässige Maß zurückzuführen, bestehen zwei Möglichkeiten: Die (nachträgliche) Erstattung der einbehaltenen und abgeführten Quellensteuer, § 50d Abs. 1 EStG; oder ein Antrag auf Erteilung einer Freistellungsbescheinigung aufgrund derer ein Steuerabzug unterbleiben kann, § 50d Abs. 2 EStG. Beide Möglichkeiten stehen allerdings unter dem „Missbrauchsvorbehalt" des § 50d Abs. 3 EStG. Greift § 50d Abs. 3 EStG ein, scheidet eine Entlastung aus. Quellen-

[10] BMF, Schreiben vom 27. Oktober 2017, IV C 5-S 2300/12/10003:004, Rn. 19.

[11] BMF, Schreiben vom 27. Oktober 2017, IV C 5-S 2300/12/10003:004, Rn. 17.

[12] Gesetz zur Rückführung des Solidaritätszuschlags 1995, BGBl. 2019 Teil I S. 2115.

[13] BMF, Schreiben vom 17. Juni 2014, IV C 3-S 2303/10/10002:001.

steuer ist einzubehalten bzw. wird nicht erstattet und hat regelmäßig abgeltende Wirkung, §§ 50 Abs. 2 S. 1 EStG, 32 Abs. 1 Nr. 2 KStG.

Unterbleibt ein Steuerabzug trotz einer bestehenden Pflicht, haftet der inländische Vergütungsschuldner (Lizenznehmer) neben dem ausländischen Unternehmen grds. für die nicht einbehaltene Quellensteuer, § 50a Abs. 5 S. 4, 5 EStG. Mit Blick auf die Vollstreckungsschwierigkeiten im Ausland wird die Finanzverwaltung ihre Ermessensentscheidung, wen sie in Anspruch nimmt, dabei regelmäßig zu Lasten des inländischen Vergütungsschuldners ausüben.

7.1.4 Gewerbesteuer

Gewerbebetriebe in der Rechtsform eines Einzelunternehmens, einer Personengesellschaft und einer Körperschaft unterliegen grds. zusätzlich der Gewerbesteuer. Die Bemessungsrundlage wird mit Hilfe des Gewerbeertrags ermittelt. Zur Bestimmung des Gewerbeertrags wird der nach dem Einkommensteuergesetz bzw. dem Körperschaftsteuergesetz ermittelte Gewinn aus dem Gewerbebetrieb durch Hinzurechnungen und Kürzungen modifiziert, vgl. §§ 8, 9 GewStG. Im Unterschied zur Einkommensteuer und Körperschaftsteuer erfasst die Gewerbesteuer auf diese Weise die objektive Ertragskraft des Gewerbebetriebs ohne Rücksicht auf die persönlichen Merkmale des Steuersubjekts. Im Zusammenhang mit der Verwertung von KI-Systemen ist § 8 Nr. 1 Buchst. f GewStG zu beachten. Danach sind Zahlungen für die zeitlich befristete Überlassung von Rechten nur beschränkt abzugsfähig, d. h. zur Ermittlung des Gewerbeertrags werden 6,25 % der Lizenzzahlungen dem Gewinn wieder hinzugerechnet. Dabei ist ein Freibetrag für die Summe aller Hinzurechnungen des § 8 GewStG i. H. v. € 100.000 abzuziehen.

Der Begriff „Rechte“ im Sinne des § 8 Nr. 1. Buchst. f GewStG meint subjektive Rechte an immateriellen Wirtschaftsgütern mit selbstständigem Vermögenswert, die eine Nutzungsbefugnis und entsprechende Abwehrrechte enthalten.[14] Aufwendungen für die Überlassung ungeschützter Erfindungen oder für Know-how fallen daher nicht unter die Hinzurechnungsvorschrift, zeitlich befristete Lizenzierungen von KI-Software hingegen schon. Nicht erfasst sind die zeitlich unbefristete Überlassung von KI-Software oder ihre Übertragung. Ausgenommen sind auch reine Vertriebslizenzen, nicht aber Rechte, die nach der vertraglichen Vereinbarung über eine bloße „Weiterleitung“ hinaus verändert, bearbeitet oder genutzt werden dürfen (vgl. Rapp 2017, S. 567).

7.1.5 Verrechnungspreise

Der Begriff „Verrechnungspreise“ bezeichnet im steuerrechtlichen Kontext schuldrechtlich vereinbarte Entgelte für den Austausch von Lieferungen oder Leistungen zwischen

[14] Vgl. BFH, 31. Januar 2012, I R 105/10 – Rn. 11.

„nahestehenden Personen“, d. h. insbesondere Konzerngesellschaften. Der oftmals fehlende oder weniger stark ausgeprägte Interessengegensatz, der in der Regel dem einheitlichen Konzerninteresse geschuldet ist, ermöglicht es diesen Unternehmen in größerem Maße, Gestaltungsspielräume zu nutzen und ggf. Gewinne in Niedrigsteuerländer zu verlagern. Infolgedessen unterliegen Vereinbarungen zwischen nahestehenden Personen steuerrechtlich einer Angemessenheitsprüfung und erhöhten Dokumentationspflichten. Maßstab für die Angemessenheitsprüfung ist ein Fremdvergleich (**Fremdvergleichsgrundsatz**). Der Fremdvergleichsgrundsatz fordert eine Verrechnung konzerninterner Lieferungen und Leistungen zu Preisen, die voneinander unabhängige Dritte unter gleichen oder ähnlichen Verhältnissen vereinbart haben oder vereinbart hätten.

In der Praxis führt diese Anforderung bei immateriellen Wirtschaftsgütern wie den KI-Systemen regelmäßig zu Schwierigkeiten, da sich aufgrund ihrer Einzigartigkeit oftmals kein vergleichbares Wirtschaftsgut am Markt für einen Fremdvergleich finden lässt. Umso wichtiger ist dann die Dokumentation nachvollziehbarer wirtschaftlicher Gründe aus Sicht beider Parteien für die letztlich gewählte Vertragsgestaltung.

7.1.5.1 Dokumentationspflichten

Um der Finanzverwaltung eine Überprüfung zu erleichtern, hat der Steuerpflichtige erhöhte Dokumentationspflichten zu erfüllen. § 90 Abs. 3 AO i. V. m. ergänzenden Vorschriften der Gewinnaufzeichnungsverordnung[15] verlangt bei Sachverhalten mit Auslandsbezug u. a. eine Sachverhalts- und Angemessenheitsdokumentation. Überlässt z. B. ein ausländisches Unternehmen KI-spezifisches Know-how, also die Gesamtheit nicht patentgeschützter, geheimer und nützlicher Kenntnisse, Erfahrungen und Erprobungen, an ein inländisches, verbundenes Unternehmen im Wege einer Lizenzierung, so sollte aus der Verrechnungspreisdokumentation deutlich hervorgehen, dass es sich nicht um allgemein verfügbares Erfahrungswissen handelt. Denn nur bei der Überlassung von Spezialwissen ist davon auszugehen, dass Dritte ein Entgelt hierfür entrichten würden (Baumhoff und Kluge 2017, § 14 Rn. 164). Für die Ermittlung des Verrechnungspreises der Höhe nach ist auch der Nutzen des Spezialwissens von wesentlicher Bedeutung. Zu berücksichtigende Faktoren sind ferner die Laufzeit der Überlassung von Know-how, in welcher Weise Fortentwicklungen des Know-hows zu erwarten sind und ob zukünftig mit einer Verbreitung des Spezialwissens zu rechnen ist (Finsterwalder 2006, S. 357).

Verletzt der Steuerpflichtige seine Mitwirkungspflichten nach § 90 Abs. 3 AO, indem er Dokumentationsaufzeichnungen nicht, zu spät oder unverwertbar vorlegt, drohen ihm Sanktionen. Nach § 162 Abs. 3 S. 1 AO wird widerlegbar vermutet, dass die steuerpflichtigen Einkünfte höher sind als die erklärten Einkünfte. Hierbei kann die Finanzverwaltung den Schätzungsrahmen zu Lasten des Steuerpflichtigen ausschöpfen. Nach § 162 Abs. 4 AO können zudem empfindliche Strafzuschläge festgesetzt werden. Derartige Risiken las-

[15] Verordnung zu Art, Inhalt und Umfang von Aufzeichnungen im Sinne des § 90 Absatz 3 der Abgabenordnung (**Gewinnabgrenzungsaufzeichnungs-Verordnung - GAufzV**), BGBl. 2017 Teil I S. 2367; BMF, Schreiben vom 12. April 2005, IV B 4-S 1341-1/05, Rn. 3.4.1.

sen sich mit einem innerbetrieblichen Kontrollsystem oftmals erheblich reduzieren. Die Existenz eines solchen Systems lässt sich in der Regel als gewichtiges Indiz für die Beachtung des Fremdvergleichsgrundsatzes werten, ggf. mit der Konsequenz, dass die Schätzungsbefugnis nach § 162 Abs. 3 und 4 AO zurückhaltender ausgeübt wird (vgl. auch Engelen 2018, S. 373).

7.1.5.2 Verdeckte Gewinnausschüttung/Kapitalertragsteuer

Beim Leistungsaustausch innerhalb einer Unternehmensgruppe bezogen auf KI kommt nicht nur ein Steuerabzug im Sinne des § 50a Abs. 1 Nr. 3 EStG in Betracht, sondern ein Verstoß gegen den Fremdvergleichsgrundsatz kann auch Kapitalertragsteuer auslösen. So werden beispielsweise überhöhte Entgeltzahlungen eines inländischen Tochterunternehmens für die Überlassung von KI-Software oder Daten an das Mutterunternehmen steuerrechtlich als verdeckte Gewinnausschüttungen qualifiziert, vgl. § 8 Abs. 1 KStG i. V. m. § 20 Abs. 1 Nr. 1 S. 2 EStG. Auf die verdeckte Gewinnausschüttung (Differenz zwischen dem tatsächlichen gezahlten und dem angemessenen Entgelt) wird grds. Kapitalertragsteuer in Höhe von 25 % erhoben, § 43 Abs. 1 Nr. 1, S. 3 EStG, § 43a Abs. 1 S. 1 Nr. 1 EStG. Auf Ebene des inländischen Tochterunternehmens ist der unangemessene Teil des Entgelts steuerrechtlich nicht abzugsfähig (§ 8 Abs. 3 S. 2 KStG). Auf Ebene des Mutterunternehmens folgt die steuerrechtliche Behandlung aus deutscher Perspektive den allgemeinen Grundsätzen für Gewinnausschüttungen.

7.2 Umsatzsteuerliche Implikationen bei der Überlassung von Daten bzw. KI-Lösungen

7.2.1 Lieferung und sonstige Leistung

Die entgeltliche Überlassung von Daten bzw. von KI-Software fällt grundsätzlich in den Anwendungsbereich der Umsatzsteuer. Die umsatzsteuerrechtlichen Rechtsfolgen hängen im Wesentlichen davon ab, ob es sich bei der Daten- bzw. Softwareüberlassung um eine Lieferung oder sonstige Leistung im Sinne des **Umsatzsteuergesetzes** (**UStG**) handelt. Diese Qualifizierung bestimmt die Regeln, nach denen sich richtet, in welchem Staat der Umsatz als ausgeführt gilt und damit steuerpflichtig wird.

Lieferungen setzen die Verschaffung der Verfügungsmacht an einem Gegenstand voraus, § 3 Abs. 1 UStG. Der Begriff „Gegenstand“ umfasst dabei grds. nur körperliche Gegenstände (Leonard 2019, § 3 UStG Rn. 34). Sonstige Leistungen sind solche, die keine Lieferungen sind, § 3 Abs. 9 UStG. Die Nutzungsüberlassung/Übertragung von Daten oder von Software stellt mangels Körperlichkeit in der Regel eine sonstige Leistung dar. Von diesem Grundsatz gibt es jedoch Ausnahmen.

So wird die Veräußerung von Standardsoftware (z. B. Software für den Heimcomputer oder für Computerspiele und Updates auf Datenträgern) im Gegensatz zu Individualsoft-

ware[16] von der deutschen Finanzverwaltung stets als Lieferung qualifiziert,[17] es sei denn sie wird auf elektronischem Wege, z. B. durch Internet-Downloads, übertragen.

Schwierigkeiten bei der Abgrenzung zwischen Lieferung und sonstiger Leistung können sich ergeben, wenn die Übertragung oder Nutzungsüberlassung von Daten/Software mit der Übertragung körperlicher Gegenstände verknüpft ist (z. B. Datenträger, Skizzen, Pläne). Dann stellt sich die Frage, ob beide Leistungen im Verhältnis Haupt – Nebenleistung zueinanderstehen, die umsatzsteuerrechtlich einheitlich nach den für die Hauptleistung geltenden Grundsätzen zu behandeln sind (Leonard 2019, § 3 UStG Rn. 22). Dies ist der Fall, wenn die „Verkörperung" für den Leistungsempfänger keinen eigenen Zweck hat, sondern lediglich ein Mittel ist, um die eigentlich gewünschte Leistung optimal in Anspruch zu nehmen. Im Zusammenhang mit KI-Systemen wird die Überlassung von Nutzungsrechten an KI-Systemen regelmäßig die Hauptleistung darstellen und etwaige körperliche Gegenstände daher lediglich das Mittel dafür sein, die KI-Software optimal zu nutzen.

Schließlich kann abhängig vom Geschäftsmodell, bei der Datenüberlassung eine sog. „Leistungsbeistellung" in Betracht kommen. Bei der Leistungsbeistellung stellt der Leistungsempfänger dem Leistenden ausschließlich zum Zwecke der Ausführung der vereinbarten Leistung selbst eine Leistung zur Verfügung (hier z. B. Überlassung von Daten). Diese Leistung des Leistungsempfängers nimmt umsatzsteuerlich nicht am Leistungsaustausch teil, d. h. sie ist weder Entgelt für die Leistung des Leistenden, noch ist sie eine Leistung des Leistungsempfängers, die Umsatzsteuer auslöst.

7.2.2 Ort für Lieferung und sonstige Leistung

Handelt es sich bei Umsätzen mit KI ausnahmeweise um eine Lieferung, gelten für die Ortsbestimmung v. a. die Regelungen des § 3 Abs. 6 – Abs. 8 UStG. Danach ist entscheidend, ob die Lieferung i. R. einer Beförderung oder Versendung erfolgt. Ist dies der Fall, liegt der Lieferort am Beginn der Beförderung oder Versendung. Liegt eine innergemeinschaftliche Lieferung zwischen Unternehmern nach § 4 Nr. 1 Buchst. b UStG i. V. m. § 6a UStG vor, ist diese Lieferung im Ursprungsland in der Regel steuerfrei. Findet keine Beförderung oder Versendung statt, liegt der Lieferort dort, wo die Verfügungsmacht an der Standardsoftware verschafft wird, § 3 Abs. 7 UStG. Bei einer Beförderung oder Versendung aus einem Drittland nach Deutschland befindet sich der Ort der Lieferung gemäß § 3 Abs. 8 UStG in Deutschland, wenn der Lieferer oder sein Beauftragter Schuldner der Einfuhrumsatzsteuer ist.

Für den Ort einer sonstigen Leistung gelten folgende Grundregeln: Sonstige Leistungen an einen Unternehmer werden im Bestimmungsland besteuert, § 3a Abs. 2 UStG, d. h. der Ort der sonstigen Leistung ist der Unternehmenssitz oder die Betriebsstätte des Leis-

[16] Abs. 3 Nr. 8 **Umsatzsteuer-Anwendungserlass** (**UStAE**).

[17] Abs. 2 Nr. 1 UStAE.

tungsempfängers. Demgegenüber werden sonstige Leistungen an einen privaten Endverbraucher grundsätzlich im Ursprungsland besteuert, § 3a Abs. 1 UStG, d. h. dort, wo der Leistende sein Unternehmen betreibt bzw. eine Betriebsstätte unterhält. Dieser Auffangregelung des § 3a Abs. 1 UStG gehen jedoch spezielle Sonderregeln vor. So legt § 3a Abs. 5 UStG für Dienstleistungen, die auf elektronischem Weg an einen Nichtunternehmer erbracht werden, das Bestimmungslandprinzip fest. Zur Entlastung von Startups und Unternehmen aus Mitgliedstaaten mit geringfügigen Umsätzen gilt diese Sonderregel jedoch nur bei Überschreitung einer Umsatzschwelle von 10.000 Euro im Vorjahr und im laufenden Kalenderjahr. Zur Vereinfachung des Besteuerungsverfahrens von elektronischen Dienstleistungen, die an Nichtunternehmer ausgeführt werden, kann zudem das sog. MOSS-Verfahren *(„Mini One Stop Shop")* in Anspruch genommen werden. Der Unternehmer hat hierbei die Möglichkeit, den Umsatz in besonderen Umsatzsteueranmeldungen in seinem Sitzstaat zu erklären und ausländische Umsatzsteuer bei seiner inländischen dafür zuständigen Behörde (in Deutschland: Bundeszentralamt für Steuern (BZSt)) zu entrichten (Zwirner et al. 2019, S. 13). Diese Behörde leitet entsprechende Daten und Zahlungen an betroffene Steuerbehörden des Empfängerstaates weiter.

Eine weitere Ausnahme enthält § 3a Abs. 4 UStG für die Einräumung, Übertragung und Wahrnehmung von Patenten, Urheberrechten, Markenrechten und ähnlichen Rechten (Nr. 1) sowie für die Überlassung von Informationen einschließlich gewerblicher Verfahren und Erfahrungen (Nr. 5) an Nichtunternehmer im Drittland. Auch in diesem Fall gilt das Bestimmungslandprinzip.

7.2.3 Daten als Entgelt

Bei Lieferungen und sonstigen Leistungen bemisst sich der Umsatz nach dem Entgelt, § 10 Abs. 1 S. 1 UStG. Zum Entgelt zählt alles, was den Wert der Gegenleistung bildet, die der leistende Unternehmer vom Leistungsempfänger für die Leistung erhält oder erhalten soll, abzüglich der für diese Leistung gesetzlich geschuldeten Umsatzsteuer. Als Entgelte können neben Geldleistungen auch Sach- oder Dienstleistungen in Betracht kommen. Fraglich ist in diesem Zusammenhang, ob die Überlassung von Daten ein Entgelt i. R. eines sog. tauschähnlichen Umsatzes darstellen kann, § 3 Abs. 12 S. 2 UStG.

Ein tauschähnlicher Umsatz liegt vor, wenn das Entgelt für eine sonstige Leistung in einer Lieferung oder sonstigen Leistung besteht. Denkbare Fälle sind z. B. der unentgeltliche Zugang zu IT-Diensten (z. B. Nutzung von E-Mail-Konten, Streaming-Diensten oder Apps) gegen die Einwilligung zur Verwertung persönlicher Nutzerdaten (vgl. Art. 6 Abs. 1 lit. a DS-GVO) oder die Hingabe maschinengenerierter Daten als Entgelt für die Nutzung von KI-Systemen.

Die Qualifizierung personenbezogener Daten als Entgelt für den Zugang zu IT-Leistungen ist vom Mehrwertsteuerausschuss grundsätzlich abgelehnt worden (Mehrwertsteuer-Ausschuss 2019, S. 575–576). Die Leitlinien des Mehrwertsteuerausschusses sind allerdings nicht bindend, sondern eine Orientierung zur Auslegung. Wenn der IT-

Dienst allen Nutzern unter denselben Bedingungen angeboten werde, bestehe keine direkte Verbindung zwischen IT-Dienstleistung und Gegenleistung in Form von personenbezogenen Daten. Eine solche ist für die Annahme eines steuerbaren Umsatzes aber erforderlich. Auch sei der wirtschaftliche Vorteil des Anbieters aus der zunächst erteilten Einwilligung zu ungewiss, um ein steuerwürdiges Entgelt zu begründen. Der monetäre Wert der Gegenleistung hinge vom Nutzerverhalten und damit aus Sicht des Anbieters von unsicheren Faktoren und Zufälligkeiten ab (Englisch 2017, S. 882), sodass auch eine Wertbemessung der Einwilligung kaum möglich sei.

Diese Betrachtung ist nicht zweifelsfrei. So wird der IT-Dienst nur und gerade wegen der Übertragung und Einwilligung in die weitere Verwendung der persönlichen Daten erbracht, was für die erforderliche Verbindung von IT-Dienst und Daten ausreichen sollte. Durch die Einwilligung des Nutzers entsteht zudem ein DS-GVO-konformer Datensatz, der am Markt gehandelt wird und dem daher auch ein wirtschaftlicher Wert zukommt. Gleichwohl scheint die deutsche Finanzverwaltung den Leitlinien des Mehrwertsteuerausschusses zu folgen und in diesen Fällen keinen steuerbaren Umsatz anzunehmen.

Im Gegensatz zur Hingabe personenbezogener Daten bleibt der Entgeltcharakter bei der Hingabe maschinengenerierter Daten aber weiterhin fraglich. Insoweit fehlt es bislang an ausdrücklichen Stellungnahmen.

7.2.4 Steuerschuldnerschaft

Grundsätzlich schuldet der leistende Unternehmer dem Fiskus die Steuerentrichtung als eigene Verbindlichkeit und ist zur Abgabe von Umsatzsteuervoranmeldungen und – erklärungen verpflichtet, § 13a Abs. 1 Nr. 1 UStG. In bestimmten Fällen geht jedoch die Steuerschuldnerschaft auf den Leistungsempfänger über, sog. Reverse-Charge-Verfahren, vgl. § 13b UStG. Dies gilt insbesondere, wenn ein im Ausland ansässiger Unternehmer an einen inländischen Unternehmer eine sonstige Leistung erbringt. Diese Umsatzsteuer kann der Leistungsempfänger unter den allgemeinen Voraussetzungen als Vorsteuer abziehen, § 15 Abs. 1 Nr. 4 UStG. Die Rechnung muss die Angabe *„Steuerschuldnerschaft des Leistungsempfängers“* enthalten; ein gesonderter Steuerausweis ist nicht zulässig, vgl. § 14a Abs. 5 UStG.

Der Umsatzsteuersatz beträgt regelmäßig 19 %. Sind Rechte aus dem Urheberrechtsgesetz betroffen, gilt der ermäßigte Steuersatz i. H. v. 7 %, vgl. § 12 Abs. 2 Nr. 7c UStG.

7.3 Vertragsgestaltung

Bei der Gestaltung von Verträgen ist es wichtig zu regeln, wer möglicherweise anfallende Steuern zu tragen hat. Dies gilt auch für den KI-Bereich und dort insbesondere für Lizenzverträge. Dabei ist zwischen den Ertragsteuern und der Umsatzsteuer zu unterscheiden.

Wie eine Steuerklausel optimal auszugestalten ist, ist für den Lizenzgeber und Lizenznehmer aufgrund der unterschiedlichen Interessen getrennt zu beantworten.

7.3.1 Ertragsteuern

Aus Sicht des Lizenzgebers empfiehlt sich eine sog. Nettovereinbarung. Hierbei schuldet der Lizenznehmer den vereinbarten Betrag der Vergütung und muss etwaige einzubehaltende und abzuführende Abzugsteuern zusätzlich tragen. Der Lizenznehmer sollte eine Nettovereinbarung nur unter der Bedingung akzeptieren, dass der Lizenzgeber, soweit möglich, eine Freistellungsbescheinigung beantragt, § 50d Abs. 2 S. 1 EStG, und ihm, d. h. dem Lizenznehmer, ein möglicher Erstattungsbetrag der einbehaltenen Steuer zusteht.

Im Fall einer Bruttovereinbarung zahlt der Lizenznehmer einen festen Betrag, von dem die Abzugsteuer einbehalten wird. Diese Vereinbarung geht zu Lasten des Lizenzgebers. Der Lizenznehmer sollte daher verpflichtet werden, den Lizenzgeber bei der Erstattung oder der Erfüllung sonstiger steuerlicher Pflichten bei den Behörden vor Ort in zumutbarer Weise zu unterstützen.

7.3.2 Umsatzsteuer

Zudem sollte vertraglich vereinbart werden, ob es sich bei der geschuldeten Vergütung um einen Nettobetrag handelt und etwaig anfallende Umsatzsteuer zusätzlich zu zahlen ist. Fehlt eine derartige Regelung, ist nach der Rechtsprechung im Zweifel davon auszugehen, dass der Preis die Umsatzsteuer enthält.[18] In diesem Fall mindert die Umsatzsteuer die Marge des Lizenzgebers.

7.3.3 Zurechnung von Wirtschaftsgütern

Unsicherheiten bei der steuerlichen Zurechnung von Wirtschaftsgütern und daran anknüpfender Folgen (z. B. Bilanzierung) können in gewissem Maße durch vertragliche Regelungen vermieden werden. Dies gilt insbesondere bei Verträge zur Überlassung von Daten. Hier können Bestimmungen zu Verarbeitungs- und Verwertungsrechten die Beurteilung der wirtschaftlichen Eigentumsverhältnisse im Sinne des § 39 AO an verarbeiteten Daten erleichtern.

[18] Dieser Grundsatz, welcher der zivilrechtlichen Rechtslage in Deutschland entspricht, wurde durch den EuGH bestätigt, vgl. EuGH, Urteil vom 07.11.2013, C-249/12 und C-250/12.

Literatur

Backu F, Bayer I (2017) F. Die steuerliche Behandlung von Software und IT-Dienstleistungen. In: Schneider J (Hrsg) Handbuch EDV-Recht, 5. Aufl. Dr. Otto Schmidt, Köln

Baumhoff H, Kluge S (2017) § 14 III. 2. a) Fremdvergleich im Rahmen der Nutzungsüberlassung immaterieller Wirtschaftsgüter, Vorbemerkung. In: Henn G, Pahlow L (Hrsg) Patentvertragsrecht, 6. Aufl. C.F. Müller, Heidelberg

bitkom (2019) Positionspapier Künstliche Intelligenz und ERP. https://www.bitkom.org/sites/default/files/2019-04/190329_pp_ki_und_erp_final.pdf. Zugegriffen am 31.01.2020

Brühl M (2020) § 39 B. III. 2. b) Maßgeblichkeit des Gesamtbilds der Verhältnisse. In: Pfirrmann V, Rosenke T, Wagner K (Hrsg) Beck'scher Online-Kommentar AO 2020. C.H. Beck, München

Engelen C (2018) Ausgewählte Aspekte und Erwägungen zur neugefassten Gewinnabgrenzungsaufzeichnungsverordnung. DStR 2018:370–375

Englisch J (2017) ‚Kostenlose' Online-Dienstleistungen: tauschähnlicher Umsatz? UR 2017:875–885

Finsterwalder O (2006) Bemessung von Verrechnungspreisen bei grenzüberschreitenden Know-how-Überlassungen im Konzern. IStR 2006:355–360

Greinert M, Metzner S (2015) Eigentum an IP im Steuerrecht. IPRB 2015:256–260

Hennrichs J (2013) § 246 III. 2. e) cc) Immaterielle Rechte und Werte. In: Hennrichs J, Kleindiek D, Watrin C (Hrsg) Münchener Kommentar zum Bilanzrecht, Bd 2, 1. Aufl. C.H. Beck, München

Hennrichs J (2018) Steuerrechtliche Gewinnermittlung (Bilanzsteuerrecht). In: Tipke K, Lang J (Hrsg) Steuerrecht, 23. Aufl. Dr. Otto Schmidt, Köln

Hinerasky A, Kurschildgen M (2016) Künstliche Intelligenz und Blockchain – neue Technologien in der Besteuerungspraxis, Der Betrieb Beilage Nr. 4 zu Heft 47/2016 S 35–40

Krumm M (2019) § 5 E. I. 7. b) dd) Software, Internet. In: Heuermann B, Brandis P (Hrsg) Blümich EStG, KStG, GewStG, 149. Aufl. Franz Vahlen, München

Leonard A (2019) § 3 III. Lieferung. In: Bunjes J (Begr.) Umsatzsteuergesetz, 18. Aufl. C.H. Beck, München

Mehrwertsteuer-Ausschuss (2019) Bedingungen für das Vorliegen eines steuerbaren Umsatzes bei Bereitstellung von Internetdiensten im Austausch für Nutzerdaten. UR 2019:575–576

Rapp B (2017) Die gewerbesteuerliche Hinzurechnung in Zusammenhang mit digitalen Services und Produkten. FR 2017:563–572

Roggenkamp JD (2006) Verstößt das Content-Caching von Suchmaschinen gegen das Urheberrecht? K&R 2006:405–409

Schmidl M (2014) IT-Recht von A-Z, Anwendungsprogramm, 2. Aufl. C.H. Beck, München

Warnke K (2018) Grenzüberschreitende Überlassung von Software und Datenbanken. EStB 2018:69–74

Wittkowski A (2018) A. VI. 1. Einkommen- bzw. körperschaftsteuerliche Berücksichtigung. In: Pfaff D, Osterrieth C (Hrsg) Lizenzverträge Formularkommentar, A. Allgemeiner Teil, 4. Aufl. C.H. Beck, München

Zwirner C, Zieglmaier H, Heyd S (2019) Bilanzierung und Besteuerung digitaler Leistungen Ausgewählte handelsrechtliche, steuerbilanzielle und (umsatz-)steuerliche Aspekte, StuB 9/2019 Beilage, S 1–21

Kartellrechtliche Fallstricke beim Einsatz von KI

8

Sebastian Hack

Zusammenfassung

In diesem Kapitel wird untersucht und dargestellt, inwiefern das Kartellrecht für das Thema **Künstliche Intelligenz** („**KI**“ oder Artificial Intelligence, AI) eine Rolle spielt und was Unternehmen in diesem Zusammenhang beachten sollten. Technologien, die KI einsetzen, drängen in den letzten Jahren in immer mehr und mehr Lebensbereiche vor. Zugleich ist die Bedeutung des Kartellrechts, insbesondere wegen der enormen Bußgelder, die Unternehmen bei Verstößen gegen das Kartellrecht drohen, gewachsen. Diese parallele Entwicklung wirft zwangsläufig die Frage auf, inwieweit Schnittpunkte zwischen Kartellrecht und KI bestehen und wie Unternehmen mit diesen Schnittpunkten umgehen sollten. Im Folgenden wird für die kartellrechtlichen Themenblöcke Kartellverbot, Marktmachtmissbrauch, Compliance und Fusionskontrolle jeweils separat erläutert, wie sich Kartellrecht und KI gegenseitig beeinflussen und welche Strategien in der Praxis zu empfehlen sind.

Vorab ist zu betonen, dass die Entwicklung Künstlicher Intelligenz noch in den Kinderschuhen steckt und daher in naher Zukunft mit weiteren Fragestellungen und Problemen im Rahmen des Kartellrechts zu rechnen ist. Eine abschließende kartellrechtliche Beurteilung der Thematik „KI“ kann naturgemäß (noch) nicht stattfinden, was auch folgendes Zitat eines US-amerikanischen KI-Forschers zutreffend beschreibt: „Die größte Gefahr von künstlicher Intelligenz ist, dass die Menschen viel zu früh denken, dass sie KI verstanden haben.“ (Elizer Yudkowsky)

S. Hack (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: sebastian.hack@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_8

Bisher sticht vor allem eine Thematik besonders hervor, wenn im Rahmen von Kartellrechtsdiskussionen von KI die Rede ist. Hierbei handelt es sich um in der Praxis bereits eingesetzte Preissetzungsalgorithmen, die von Unternehmen aus den verschiedensten Branchen verwendet werden, um Verkaufspreise festzusetzen und zu ändern, also letztlich optimale Preise anzustreben. Die preissetzenden Algorithmen sind von dem Unternehmen selber oder einem Dritten so programmiert, dass Verkaufspreise automatisch, unter Berücksichtigung verschiedener Faktoren wie der Preisgestaltung der Konkurrenten, der eigenen Preisgestaltung in der Vergangenheit, Angebot und Nachfrage, dem Wochentag oder der Tageszeit, festgesetzt werden.

In diesem Kapitel wird untersucht und dargestellt, inwiefern das Kartellrecht für das Thema KI eine Rolle spielt und was Unternehmen in diesem Zusammenhang beachten sollten. Technologien, die KI einsetzen, drängen in den letzten Jahren in immer mehr und mehr Lebensbereiche vor (BKartA 2020). Zum Beispiel verfolgen die meisten Einzelhändler die Online Preise ihrer Wettbewerber. Zwei Drittel dieser Händler nutzen dann automatische Softwareprogramme zur Anpassung der eigenen Preise (Europäische Kommission 2017, Rn. 13). Besonders verbreitet ist die Nutzung solcher Preissetzungsalgorithmen bei der Vermittlung von Reisen und Flügen, Hotelzimmern, Transportdienstleistungen, Einzelhandel und Elektrizität (OECD 2017a, Rn. 26.). Zugleich ist die Bedeutung des Kartellrechts, insbesondere wegen der enormen Bußgelder, die Unternehmen bei Verstößen gegen das Kartellrecht drohen, gewachsen. Diese parallele Entwicklung wirft zwangsläufig die Frage auf, welche Bedeutung Kartellrecht für KI hat und wie Unternehmen hiermit umgehen sollen. Auch aus diesem Grund hat sich inzwischen eine Debatte darüber entwickelt, ob und inwiefern Algorithmen negative Effekte auf den Wettbewerb haben (könnten). Im Folgenden wird für die kartellrechtlichen Themenblöcke Kartellverbot, Marktmachtmissbrauch, Compliance und Fusionskontrolle jeweils separat erläutert, was aus kartellrechtlicher Sicht bei dem Einsatz von Künstlicher Intelligenz zu beachten ist.

Das Kartellrecht besteht im Wesentlichen aus den drei Säulen Kartellverbot, Missbrauchsaufsicht und Fusionskontrolle. Das in § 1 GWB und Art. 101 Abs. 1 AEUV kodifizierte Kartellverbot verbietet Vereinbarungen zwischen Unternehmen, Beschlüsse von Unternehmensvereinigungen und aufeinander abgestimmte Verhaltensweisen, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs (**Wettbewerbsbeschränkung**) bezwecken oder bewirken. Das Paradebeispiel für eine solche verbotene Absprache ist die Preisabsprache zwischen miteinander im Wettbewerb stehenden Unternehmen oder eine Aufteilung der Gebiete, in die diese Unternehmen ihre Produkte oder Dienstleistungen vertreiben. Aber auch bereits der bloße Austausch von wettbewerblich sensiblen Informationen (z. B. Preis- und Kostenbestandteile, Kundeninformationen) zwischen Wettbewerbern kann einen schwerwiegenden Kartellrechtsverstoß darstellen. Denn hierdurch wird der Geheimwettbewerb zwischen Wettbewerbern beschädigt – die Kenntnis von z. B. den tatsächlichen aktuellen Verkaufspreisen eines Wettbewerbers wird das eigene Wettbewerbs- und Preissetzungsverhalten verändern.

Das in § 19 GWB und Art. 102 AEUV statuierte Missbrauchsverbot verbietet die missbräuchliche Ausnutzung einer marktbeherrschenden Stellung. Dieser Tatbestand ist zum

Beispiel erfüllt, wenn ein marktbeherrschendes Unternehmen als Anbieter oder Nachfrager einer bestimmten Art von Waren oder gewerblichen Leistungen ungünstigere Entgelte oder sonstige Geschäftsbedingungen fordert, als sie das marktbeherrschende Unternehmen selbst auf vergleichbaren Märkten von gleichartigen Abnehmern fordert. Das Bundeskartellamt und die Europäische Kommission verfolgen illegale Kartelle und Marktmachtmissbräuche und können gegen die verantwortlichen Personen und Unternehmen empfindliche Bußgelder verhängen.

Die Fusionskontrolle ist eine präventive Strukturkontrolle. Sofern ein Zusammenschluss anmeldepflichtig ist, prüfen das Bundeskartellamt und die Europäische Kommission, ob der Zusammenschluss negative Auswirkungen auf den Wettbewerb haben wird. Überwiegen die wettbewerblichen Nachteile, kann ein Zusammenschlussvorhaben untersagt oder nur unter Bedingungen freigegeben werden.

Bei kartellrechtlicher Compliance geht es darum, sicherzustellen, dass das Verhalten der Unternehmen am Markt kartellrechtskonform ist. Mögliche Kartellrechtsverstöße sollen im besten Fall vermieden, ansonsten frühzeitig aufgedeckt und individuell optimale Maßnahmen, wie z. B. das Abstellen des Verstoßes oder eine „Selbstanzeige" bei einer Behörde, ergriffen werden, um einen etwaigen eigenen finanziellen Schaden zu vermeiden oder zumindest zu minimieren.

8.1 Kartellverbot

8.1.1 Horizontale Aspekte

In den kartellrechtlichen Expertenkreisen wird KI insbesondere im Zusammenhang mit Preissetzungsalgorithmen diskutiert. Denn diese können unter bestimmten Voraussetzungen gegen das Kartellverbot nach § 1 GWB und Art. 101 Abs. 1 AEUV verstoßen. Im Wesentlichen haben sich bisher drei verschiedene Grundkonstellationen für einen Verstoß herauskristallisiert.

Erstens kann ein Preissetzungsalgorithmus dazu eingesetzt werden, eine zuvor schon getroffene Preisabsprache durchzusetzen (Künstner 2019, S. 36). Der Algorithmus kann hierbei zur Durchführung oder Verschleierung der Absprache dienen. Unternehmen können z. B. versuchen, durch scheinbar komplexe Preissetzungsalgorithmen von den zuvor getroffenen kartellrechtswidrigen menschlichen Entscheidungen abzulenken. Ebenso können augenscheinlich unkoordinierte Preisbewegungen zu einem insgesamt koordinierten wirtschaftlichen Ergebnis führen. Eine solche kartellrechtswidrige Verwendung eines Algorithmus fand beim sogenannten Posterkartell, das sowohl von den US-amerikanischen als auch den britischen Behörden verfolgt wurde, statt (U.S. Department of Justice 2015). Hier koordinierten zwei Online-Händler ihre Preise und setzten anschließend einen Preisalgorithmus ein, um die Absprache umzusetzen. Die Anwendung des Äquivalenztests zeigt hier ohne Schwierigkeiten: Wäre die Absprache etwa durch Mitarbeiter der Händler umgesetzt worden, bestünden ebenso wenig Zweifel an der Kartellrechtswidrigkeit wie im Falle der Umsetzung durch die Algorithmen (Künstner und Franz 2017, S. 690; Käseberg und v. Kalben 2018, S. 4). Der eigentliche Kartellrechtsverstoß ist in dieser ersten

Fallkonstellation also häufig bereits (vollständig) begangen, bevor ein Algorithmus überhaupt eingesetzt wird. Dass ein Kartellrechtsverstoß vorliegt, wird einem Unternehmen in dieser Konstellation noch am ehesten bewusst sein. Der Einsatz eines Preissetzungsalgorithmus kann eine bereits begangene kartellrechtswidrige Preisabsprache nicht „heilen". Derzeit ermittelt die spanische Wettbewerbsbehörde gegen sieben Unternehmen, die im spanischen Immobiliensektor tätig sind, wegen des Verdachts, Preise durch in Software eingebettete Algorithmen vereinbart zu haben. Das Ergebnis der Ermittlungen bleibt gespannt abzuwarten.

Zweitens ist eine kartellrechtswidrige Absprache über einen Dritten denkbar (**hub and spoke**) und bereits im Fall Eturas[1] vorgekommen. Eturas, ein Online-Reisevermittler, informierte die ihm angeschlossenen Reisebüros über eine Änderung im Preissetzungsalgorithmus. Eturas habe in der Systemeinstellung Online-Rabatte auf 3 % beschränkt und hiervon könne lediglich manuell durch die Reisebüros abgewichen werden. Bereits die passive Entgegennahme dieser Information bezüglich der Rabattbegrenzung wurde hier als abgestimmte Verhaltensweise und damit als kartellrechtswidrig betrachtet, soweit jedes angeschlossene Reisebüro davon ausgehen musste, dass die Wettbewerber dieselbe Nachricht erhalten hatten und dadurch eine Koordinierung der maximalen Rabattsätze erfolgte. Die Reisebüros hätten sich entweder öffentlich vom Inhalt der Mitteilung distanzieren, die Behörden darüber unterrichten oder über ihr Marktverhalten eine deutliche Abkehr von der 3 % Obergrenze signalisieren müssen.

Auch der Fall Uber[2] stellt ein Beispiel für diese Grundkonstellation dar. Im Fall Uber, der 2016 den District Court of New York beschäftigte, ging es um Ubers Internet-Plattform, über die private Fahrer taxiähnliche Dienste anbieten können. Die Abrechnung erfolgt über die Uber App, die Fahrpreisvorschläge berechnet und z. B. zu Stoßzeiten Preiserhöhungen für sämtliche Fahrer vorschlägt. Theoretisch sei ein Abweichen von dem vorgeschlagenen Preis möglich, die App sehe jedoch praktisch – so der District Court – keine entsprechende Möglichkeit vor. Letztlich ging das Gericht davon aus, dass es sich um eine horizontal wirkende Abstimmung nach § 1 des Sherman Act handele.[3]

Ganz allgemein spielen vermittelnde Plattformen im Kartellrecht eine zentrale Rolle. Es gibt ein unzähliges Angebot an Produkten und Dienstleistungen, die über solche Plattformen angeboten und erworben werden, von Ferienwohnungen, über Versicherungen oder Getränkelieferungen. Bei manchen dieser Plattformen tritt die Plattform selbst als Anbieter gegenüber dem Kunden auf, bei anderen ist sie reiner Vermittler. In diesen Fällen, bietet der Plattformbetreiber häufig eine Vielzahl von Services und Hilfestellungen für die Anbieter an. Dazu kann u. a. auch gehören, dass die Plattform die Preise vorschlägt

[1] EuGH 21. Januar 2016, EuZW 2016, 435.

[2] U.S. District Court of the Southern District of New York 2016, Case 15 Civ. 9796, Meyer/Kalanick.

[3] U.S. District Court of the Southern District of New York 2016, Case 15 Civ. 9796, Meyer/Kalanick, Opinion and Order v. 31. März 2016, S. 17; Thomas (2016, § 19 Rn. 123) weist darauf hin, dass dass die Bewertung von Sternverträgen nach deutschem Recht der nach US-Recht zwar ähnlich, aber nicht mit dieser identisch ist.

oder sogar die Preissetzung mittels eigener Preissetzungsalgorithmen für den Anbieter übernimmt. Auch in diesen Fällen besteht je nach Ausgestaltung die Gefahr, dass solche Tools zu einer unzulässigen Preiskoordinierung führen.

Kartellrechtliche Risiken lauern also verstärkt dort, wo ein Unternehmen mit einem Dritten kooperiert oder dessen Algorithmus verwendet und dieser Dritte wiederum mit Wettbewerbern des Unternehmens ähnliche Kontaktpunkte hat. Deutlich wird vor allem, dass auch vollständige Passivität zu Kartellrechtsverstößen führen kann. Vor allem, wenn es um wettbewerblich sensible Informationen wie Preise oder Preisbestandteile geht, ist bei der Auslagerung von Entscheidungen an Dritte (Algorithmen) Vorsicht geboten. Greifen mehrere Wettbewerber auf Preisalgorithmen und Datensätze ein und desselben Drittanbieters zurück, ist dies vor allem dann kartellrechtlich problematisch, wenn die von der Software unterbreiteten Preisvorschläge nicht auf öffentlich verfügbaren Informationen beruhen, sondern auf einen Datenpool zu dem die Software anwendenden Wettbewerber die Daten geliefert haben. Dann nämlich könnte die vom EuGH im Urteil Eturas aufgestellte Vermutung greifen, dass sich die beteiligten Unternehmen aufgrund des gemeinsam genutzten IT-Systems an einer aufeinander abgestimmten Verhaltensweise beteiligt haben.[4] Es ist daher besonders wichtig für Unternehmen sich genau über die Funktionsweise und Datengrundlage für solche Anwendungen zu informieren und dies kartellrechtlich prüfen zu lassen. Insbesondere wenn Nutzer selbst eigene sensible Daten an den Algorithmus liefern sollen, ist Vorsicht und eine genaue kartellrechtliche Würdigung geboten.

Drittens besteht die Möglichkeit, dass sich unabhängig voneinander eingesetzte Algorithmen verschiedener Unternehmen selbstständig koordinieren und Preise absprechen. Fallpraxis zu diesen autonomen Entscheidungen durch Algorithmen gibt es noch nicht, die rasante KI-Entwicklung lässt diese Szenarien jedoch immer wahrscheinlicher werden (Käseberg und von Kalben 2018, S. 3). Auch der Bundeskartellamtspräsident Andreas Mundt hält kommunizierende Algorithmen, die voneinander lernen, wie man im Onlinehandel möglichst hohe Preise durchsetzt, für denkbar (Wirtschaftswoche 2019, S. 37). Die Europäische Wettbewerbskommissarin M. Vestager hat sich klar positioniert: „The challenges that automated systems create are very real. If they help companies to fix prices, they really could make our economy work less well for everyone else. […] And businesses also need to know that when they decide to use an automated system, they will be held responsible for what it does. So they had better know how that system works." (Vestager 2017) Es ist wahrscheinlich, dass auch die Wettbewerbsbehörden Entscheidungen im Zusammenhang mit Preisen, die selbstständig von Algorithmen getroffen wurden, den jeweiligen Unternehmen zurechnen werden. Daher wird es nicht möglich sein, sich hinter einem Algorithmus zu verstecken, um einem Bußgeld zu entgehen. In jeder Phase der Schaffung und Nutzung eines Algorithmus ist es erforderlich, kartellrechtliche Risiken zu erkennen und entsprechende Maßnahmen zu ergreifen. Die Preisgestaltung sollte nicht einem einmal konfigurierten und dann nicht mehr kontrollierten Algorithmus überlassen

[4] EuGH 21. Januar 2016, EuZW 2016, 435.

werden. Andernfalls müssen sich Unternehmen dieses Verhalten als eigenes zurechnen lassen – „Kartellverstoß by Design" sozusagen.

Von diesen kartellrechtlich problematischen Konstellationen abzugrenzen ist das zulässige autonome Parallelverhalten. Ein solches liegt vor, wenn Unternehmen öffentlich verfügbare Preise von Wettbewerbern beobachten und diese Preise dann bei ihrer eigenen Preissetzung berücksichtigen. Ursachen für ein Parallelverhalten sind beispielsweise eine hohe Transparenz veröffentlichter Endkundenpreise (z. B. bei Tankstellen), eine Homogenität der Herstellungskosten und eine hohe Reaktionsverbundenheit. Der Europäische Gerichtshof hat entschieden, dass ein Parallelverhalten „nur dann als Beweis für eine Abstimmung angesehen werden kann, wenn es sich nur durch die Abstimmung einleuchtend erklären lässt."[5]

Der Einsatz von Preissetzungsalgorithmen kann jedoch das eigentlich zulässige Parallelverhalten immer näher in Richtung kartellrechtswidriges „Signalling" rücken und die Grenze zwischen diesen beiden Verhaltensweisen verschwimmen lassen (OECD 2017a, Rn. 70–74). Ein solches Signalling liegt häufig vor, wenn Unternehmen öffentlich Preise ankündigen, um dadurch eine dem Wettbewerb eigentlich fremde Transparenz zu erzeugen und eine entsprechende Reaktion des Wettbewerbers erreichen zu wollen. Die Horizontalleitlinien der Kommission gehen davon aus, dass eine „echt öffentliche" einseitige Bekanntgabe von Informationen zwar grundsätzlich unbedenklich ist, im Einzelfall jedoch kritisch zu bewerten sein kann, wenn etwa der ersten Bekanntgabe korrespondierende Veröffentlichungen anderer Unternehmen folgen (Europäische Kommission 2011, Rn. 63). Zu befürchten ist, dass Algorithmen von Wettbewerbern sich gegenseitig durch (kodierte) Signale anzeigen, dass sie beabsichtigen, einen bestimmten Wettbewerbsparameter wie den Preis auf eine bestimmte Weise zu ändern. Ohne eine vorherige Ankündigung ist eine Preiserhöhung für ein bestimmtes Produkt naturgemäß kartellrechtskonform. Das Unternehmen setzt sich dem gewollten Risiko aus, dass Kunden aufgrund des erhöhten Preises zu Wettbewerbern abwandern, da die Wettbewerber nicht sofort auf die Preiserhöhung reagieren können, z. B. durch ein Anheben der eigenen Preise. Aufgrund dieser Ungewissheit der Marktreaktionen kommt es nur sehr dosiert zu entsprechenden Preisänderungen. Nutzt nun ein Unternehmen einen Preissetzungsalgorithmus und weiß zudem, dass auch seine Wettbewerber einen ähnlichen Algorithmus verwenden, kann es davon ausgehen, dass entsprechende Preisanpassungsreaktionen der Wettbewerber sehr zeitnah erfolgen werden, sodass das Risiko des Vorreiters wesentlich geringer ist (OECD 2017a, Rn. 70–74).

Im Hinblick auf die präsenter werdende Blockchain-Technologie ist zu sagen, dass es noch keine konkreten Fälle vor den Wettbewerbsbehörden gab. Wie auch ganz allgemein bei der Veröffentlichung von Informationen, müssen Unternehmen, die auf der Blockchain operieren und dort ihre Daten offenlegen, darauf achten, dass es sich bei diesen Daten nicht um wettbewerbsrelevante Daten handelt (Hoffer und Mirtchev 2019, S. 239).

[5] EuGH 31. März 1993, – 89/85, Rn. 71.

Aufgrund der Transparenz der Blockchain könnte bereits das einseitige Speichern von Daten als Kartellrechtsverstoß gewertet werden.

8.1.2 Vertikale Aspekte

Nicht nur im horizontalen Verhältnis zwischen verschiedenen Wettbewerbern, sondern auch im vertikalen Verhältnis spielt KI schon jetzt eine Rolle. Nach Art. 4 lit a. der **Verordnung (EU) Nr. 330/2010** (**Vertikal-GVO**) ist es kartellrechtskonform, wenn ein Hersteller Höchstverkaufspreise festsetzt oder Preisempfehlungen ausspricht, sofern sich diese nicht infolge der Ausübung von Druck oder der Gewährung von Anreizen tatsächlich wie Fest- oder Mindestverkaufspreise auswirken. Die Kommission weist in ihrer Sektoruntersuchung „E-Commerce" darauf hin, dass Hersteller Abweichungen beim Wiederverkaufspreis von ihren **unverbindlichen Preisempfehlungen** (**UVP**) durch eingesetzte Preissoftware fast in Echtzeit entdecken können. Hierdurch wird es ihnen ganz wesentlich erleichtert, die Einhaltung von Preisen zu überwachen und letztlich auch durchzusetzen (Europäische Kommission 2017, Rn. 13). Aus diesem Grund gilt mehr denn je, dass die Kenntnis von der Unterschreitung der UVP nicht zu einer für den Händler nachteiligen Handlung seitens des Herstellers führen darf. Je näher eine solche benachteiligende Handlung zeitlich am Unterschreiten der UVP liegt, desto eher wird eine Kartellbehörde den Grund für diese Handlung wohl (auch) in dem Unterschreiten sehen und Kartellrechtswidrigkeit annehmen. Automatisch eingestellte Belieferungsreduzierungen oder -einstellungen bei Unterschreiten der UVP sind kartellrechtswidrig. Schon bei der automatischen Erfassung der Wiederverkaufspreise der nachgeschalteten Händler, z. B. bei der Art und Weise wie diese Informationen gespeichert werden, sollten die kartellrechtlichen Bestimmungen stets im Hinterkopf behalten werden, damit bei einer möglichen späteren Untersuchung einer Kartellbehörde nicht der (berechtigte) Eindruck entsteht, dass unzulässig auf die Preisgestaltung der Händler eingewirkt worden ist. Denn schon die bloße Kontaktaufnahme zum Abnehmer, um den Weiterverkaufspreis zu beeinflussen, kann eine verbotene vertikale Preisbindung darstellen.

Zudem können Preisanpassungsalgorithmen die schädlichen Wirkungen vertikaler Preisbeschränkungen zusätzlich verstärken, wie die Verfahren bezüglich diverser Preisbindungen der Europäischen Kommission gegen Asus, Denon & Marantz, Philips und Pioneer veranschaulichen (vgl. Europäische Kommission 2018). Viele dieser Online-Einzelhändler, auch die größten, setzten Preissetzungsalgorithmen ein, welche ihre Verkaufspreise automatisch an die Preise der Wettbewerber anpassten. Aus diesem Grund wirkte die vertikale Preisbeschränkung praktisch nicht nur zwischen den Vertragsparteien, sondern hatte auch preisliche Auswirkungen auf weitere Marktteilnehmer auf der nachgeordneten Stufe.

Zurechnung

Ganz wesentlich ist die Frage, unter welchen Umständen das Verhalten eines lernenden Algorithmus einem Unternehmen zugerechnet werden kann. In der Literatur wird verein-

zelt vorgeschlagen, dieselben Maßstäbe wie bei der Mitarbeiterzurechnung zugrunde zu legen (vgl. Dohrn und Huck 2018, S. 178; Wolf 2019 S. 6; OECD 2017b, Rn. 38). Hiernach könnte die Verantwortlichkeit schon aus dem Einsatz und dem in Betrieb halten des Algorithmus folgen. Nach anderer Ansicht soll das Verhalten des Algorithmus dem Unternehmen nur zugerechnet werden, wenn es für das Unternehmen vorhersehbar hätte sein müssen (Janka und Uhsler 2018, S. 121; Salaschek und Serafimova 2018, S. 15). Auch ohne sich einer konkreten Ansicht anzuschließen wird deutlich, dass die Zurechnung wohl nur in Ausnahmefällen verneint werden wird. Hierfür sprechen auch die bereits oben erwähnten Aussagen von M. Vestager und Andreas Mundt.

Die Verantwortlichkeit für KI-Anwendungen wird auf europäischer Ebene heiß diskutiert. Hierbei geht es nicht nur darum, wann das Verhalten eines Algorithmus einem verwendenden Unternehmen zugerechnet werden kann. Die Europäische Kommission versucht derzeit vielmehr eine Lösung für die Frage, wann eine KI-Anwendung dem Entwickler, dem Benutzer oder dem Verkäufer zugerechnet werden kann, zu finden. M. Vestager sagte in diesem Zusammenhang, dass eine Tendenz bestehe, dass derjenige, der am besten in der Lage ist, Risiken anzugehen, zur Verantwortung gezogen werden soll. Je nachdem, wie die Europäische Kommission diese Frage letztlich beantworten wird, können für bestimmte Gruppen, deren Geschäftstätigkeiten Berührungspunkte mit KI-Anwendungen haben, neue kartellrechtliche Risiken entstehen.

8.2 Marktmachtmissbrauch

KI kann auch für einen kartellrechtswidrigen Marktmachtmissbrauch nach § 19 GWB und Art. 102 AEUV relevant werden. Zum einen können Algorithmen zur Marktmacht von Unternehmen beitragen (Wettbewerb um Algorithmen), was aufgrund der zentralen Bedeutung von Algorithmen für innovative Geschäftsmodelle nur plausibel ist. Der deutsche Gesetzgeber hat auf diese Entwicklung im Rahmen der 9. GWB Novelle bereits reagiert und § 18 Abs. 3a GWB geschaffen, der ein moderneres, vielseitigeres Verständnis von Marktmacht zum Ausdruck bringt. Im Einzelfall kann der Zugang zu Algorithmen sogar eine Marktzutrittsschranke darstellen. Bejaht wurde dies z. B. von der Kommission im Google Shopping Verfahren, in dem die Kommission betonte, dass die erstmalige Entwicklung und der Aufbau einer allgemeinen Suchmaschine insbesondere aufgrund der notwendigen Algorithmen erhebliche Investitionen in den Bereichen Forschung und Entwicklung sowie Ausrüstung und Personal voraussetze.[6] Zudem sollte erwähnt werden, dass die mit Algorithmen einhergehende Marktmacht ihrerseits in einem inneren Zusammenhang mit dem Zugang zu denjenigen Daten stehen kann, die vom Algorithmus analysiert und dann verarbeitet werden sollen (BKartA 2020, S. 10).[7] Im oben genannten

[6] Europäische Kommission, 27. Juni 2017, Case AT.39740, Rn. 185 und Rn. 286–291.

[7] Siehe zu Ansprüchen auf Zugang zu Daten, die gerade für den Erfolg und die Funktionsfähigkeit von KI wichtig ist Kap. 4.

Google Verfahren wies die Kommission darauf hin, dass eine allgemeine Suchmaschine eine gewisse Menge an Abfragen erhalten müsse, um wettbewerbsfähig zu sein, da nur so eine sinnvolle Relevanz der Suchergebnisse festgestellt werden kann. Auf die Bedeutung von Daten für Marktmacht in der Digitalwirtschaft sind das BKartA und die französische Wettbewerbsbehörde in einer gemeinsamen Untersuchung eingegangen (ADLC und BKartA 2016).[8] Aus Vorstehendem ergibt sich, dass Unternehmen, die Algorithmen verwenden, unter Umständen schneller als bisher als marktmächtiges Unternehmen im Sinne des Kartellrechts angesehen werden können. Hieraus folgt dann, dass ihre unternehmerische Handlungsfreiheit eingeschränkt ist. Bei ihrem Vorgehen am Markt muss verstärkt auf das Einhalten der kartellrechtlichen Vorschriften geachtet werden.

Zum anderen kann die Nutzung eines Algorithmus den Missbrauch einer bestehenden Marktmacht darstellen (Wettbewerb mit Algorithmen). Die eben erwähnte Verweigerung des Zugangs zu Algorithmen bzw. zu Informationen (siehe hierzu Kap. 4) über algorithmische Schnittstellen kann im Einzelfall auch einen Missbrauch einer marktbeherrschenden Stellung darstellen. Dies nahm die Kommission beispielsweise im Microsoft-Verfahren von 2004 an. Die Kommission hielt hier die Ermöglichung von Interoperabilität von Softwareprogrammen für erforderlich, obwohl (teilweise) gewisse Industriestandards, Möglichkeiten für sogenanntes reverse-engineering und Lizenzierungsmöglichkeiten existierten.[9]

Der Einsatz von Preissetzungsalgorithmen kann zudem einen Marktmachtmissbrauch darstellen. Für eine nähere Betrachtung sind in einem ersten Schritt die dynamische und die individualisierte Preisbildung zu unterscheiden. Dynamische Preisbildung bedeutet, dass ein Preis aufgrund von Veränderungen der Marktlage, insbesondere durch Angebot und Nachfrage, gebildet wird. Der Preis ist hierbei aber für alle Kunden gleich. Wie bereits oben erläutert, findet aufgrund der Digitalisierung eine immer weiter ansteigende Beschleunigung dieser Anpassungsprozesse statt. Individualisierte Preisbildung bedeutet, dass der jeweilige Preis von objektiven Kriterien (z. B. Endgerät, Browser oder Betriebssystem) oder subjektiven Kriterien (z. B. Alter, Geschlecht, Herkunft, Wohnort oder vorausgehendes Kauf- und Nutzungsverhalten) abhängt. Beide Preisbildungsmechanismen können wettbewerbstheoretisch durchaus begrüßenswert sein und eine gesteigerte Konsumentenwohlfahrt zur Folge haben (Zander-Hayar et al. 2016, S. 405).

Auch die gegenteilige Wirkung kann jedoch eintreten und ein Marktmachtmissbrauch vorliegen. Durch Algorithmen festgesetzte Preise können missbräuchlich sein, wenn ein marktbeherrschendes Unternehmen diese zur Ausbeutung seiner Nachfrager oder der Behinderung seiner Wettbewerber einsetzt. Der Anfangsverdacht eines Ausbeutungsmissbrauchs (dynamische Preisbildung) bestand z. B. im vom Bundeskartellamt betrachteten Lufthansa-Fall.[10] Im Anschluss an die Insolvenz von Air Berlin, die zu einer Monopolstellung der Lufthansa auf einigen innerdeutschen Routen und Preiserhöhungen von etwa

[8] Vgl. hierzu auch den ersten Beitrag dieser Schriftenreihe des BKartA (2017).

[9] Europäische Kommission 24. März 2004, Case COMP/C-3/37.792 Microsoft, Rn. 666–668.

[10] BKartA, 29. Mai 2018, Az.: B9-175/17.

25–30 Prozent geführt hatte, erklärte die Lufthansa, dass diese Preiserhöhungen nicht auf manuellen Änderungen, sondern den Reaktionen des Algorithmus auf Nachfrageänderungen beruhten (vgl. Busse 2017). Zu einer Prüfung der Umstände bezüglich der Preiserhöhungen kam es letztlich jedoch nicht.

Auch der Einsatz von Personalisierungsalgorithmen (individualisierte Preisbildung) kann kartellrechtlich problematisch sein. Die wettbewerblichen Auswirkungen solcher Diskriminierungen sind jedoch nicht unabhängig vom Einzelfall beurteilbar (vgl. bspw. Locher 2018). Einerseits kann eine Diskriminierung auch zu Wohlfahrtsgewinnen führen, wenn jeder den Preis zahlt, den er zu zahlen bereit und im Stande ist. Dann können mitunter einzelne Kunden(gruppen) zu günstigeren (quersubventionierten) Preisen einkaufen, als unter sonstigen Marktbedingungen. Andererseits ist die individualisierte Preissetzung auch nicht zwingend ein Zeichen von Marktmacht, da entsprechende Preissetzungen auch ein wettbewerbliches Mittel darstellen können, um Kunden trotz starker Präferenz für konkurrierende Produkte zu gewinnen (vgl. ADLC und BKartA 2016, S. 21–22). Es ist daher wichtig in jedem Einzelfall eine konkrete Bewertung der Umstände, dem Einsatz und der Funktionsweise des Algorithmus vorzunehmen.

Auch Ranking Algorithmen sind potenziell geeignet, zu einem Missbrauch einer marktbeherrschenden Stellung zu führen. Wie im Google Shopping-Verfahren geht es hier vor allem um Fälle der sogenannten Selbstbevorzugung. Im genannten Verfahren sah die Kommission ein missbräuchliches Verhalten von Google insbesondere darin, dass Google seinem eigenen Shopping-Dienst einen günstigeren Platz im Rahmen der allgemeinen Suchergebnisseiten einräumte und dadurch die Sichtbarkeit von Wettbewerbern beschränkte.[11]

Wenn keine marktbeherrschende Stellung vorliegt, dürften sowohl die dynamische, als auch die individualisierte Preisbildung gegenüber anderen Unternehmern kartellrechtlich weniger problematisch sein, da diese dann lediglich Ausdruck der unternehmerischen Handlungs- und Vertragsfreiheit sind (Ylinen 2018, S. 19). Bei einem Einsatz gegenüber einem Verbraucher stellen sich hingegen möglicherweise diskriminierungs-, datenschutz- oder lauterkeitsrechtliche Fragen (Ylinen 2018, S. 19).

Auch im Rahmen der Marktmissbrauchskontrolle gilt, dass ein Unternehmen sich durch die Nutzung von Algorithmen nicht seiner kartellrechtlichen Verantwortung entziehen kann. Im Lufthansa-Fall hat das Bundeskartellamt zum Ausdruck gebracht, dass der Einsatz von Preissetzungsalgorithmen die Verwender selbstverständlich nicht von ihrer Verantwortung ihres Marktverhaltens entbindet.[12] Mit der Auslagerung von (preisbezogenen) Entscheidungen an Algorithmen kann also ein hohes kartellrechtliches Risiko verbunden sein, da ebenjene Entscheidungen nicht mehr (vollständig) beeinflussbar sind, dem Unternehmen aber (vollständig) zugerechnet werden. Zugleich ist es bei Entscheidungsfindungsprozessen durch Algorithmen eher weniger möglich oder nicht gewollt, einzelne Entscheidungsfindungsphasen zu überwachen und bei kartellrechtlich problematischen Abläufen frühzeitig genug entsprechende Abhilfemaßnahmen zu ergreifen. Aus

[11] Europäische Kommission, 27. Juni 2017, Case AT.39740, Rn. 341.

[12] BKartA, 29. Mai 2018, Az.: B9-175/17.

diesem Grund sollte schon vor der Implementierung eines Algorithmus – vor allem, wenn es sich um ein marktbeherrschendes Unternehmen handelt – eine umfangreiche kartellrechtliche Prüfung erfolgen.

8.3 Compliance

Weil Kartellrecht in besonderer Weise „verletzungsgeneigt" ist und die Entdeckungswahrscheinlichkeit von Kartellrechtsverletzungen hoch ist und stetig zunimmt, ist es seit langer Zeit das zentrale Thema im Rahmen von Compliance Maßnahmen (Glöckner 2017, S. 905). Ziel von kartellrechtlichen Compliance-Programmen ist es, auf systematische Weise ein Bewusstsein für die rechtliche Situation und das Risikomanagement zu schaffen. Kartellrechtswidriges Verhalten soll so entdeckt und beseitigt oder am besten von Anfang an vermieden werden. Die Verwendung von KI verstärkt die Verletzungsgeneigtheit noch weiter. Aus diesem Grund muss das Thema KI, wenn entsprechende Compliance Maßnahmen und Schulungen gewissenhaft und vollständig sein sollen, berücksichtigt werden. Dass das Thema KI im Rahmen der kartellrechtlichen Compliance eine große Rolle spielt, zeigt auch die Diskussion um eine Pflicht zur Implementierung einer einprogrammierten Compliance-Software für Algorithmen (Paal 2019, S. 43). Die stetig fortschreitende Digitalisierung und der zunehmende Onlinehandel haben letztlich zur Folge, dass „Digital Antitrust" als wesentlicher Baustein kartellrechtlicher Compliance integriert werden muss (Ritz und Marx 2018, S. 421).

▶ **Praxistipp** Insbesondere das bisher zu den Themen Kartellverbot und Marktmachtmissbrauch Erläuterte ist im Rahmen von Compliance-Maßnahmen zu berücksichtigen. Unabhängig vom Einzelfall sind beim Einsatz von Preissetzungsalgorithmen in jedem Fall folgende Grundregeln zu beachten:

- Tauschen Sie sich unter keinen Umständen mit Ihren Wettbewerbern über verwendete Preissetzungsalgorithmen oder ähnliche Themen aus – auch nicht mittelbar über IT-Dienstleister (Ritz und Marx 2018, S. 421).
- Unterwerfen Sie Ihre internen und externen IT-Dienstleister strikten Compliance-Regeln im Hinblick auf Entwicklung und Verwendung von Preissetzungsalgorithmen (Compliance by Design) (Ritz und Marx 2018, S. 421).
- Lassen Sie Ihre internen IT-Dienstleister Compliance-Schulungen absolvieren (Ritz und Marx 2018, S. 421).
- Informieren Sie sich regelmäßig bei den IT-Kollegen über geplante Entwicklungen und Einsätze von Preisalgorithmen (Ritz und Marx 2018, S. 421).
- Halten Sie die Entwicklung des Kartellrechts im Hinblick auf KI im Auge.

Darüber hinaus kann KI aber auch bei der Durchsetzung von Compliance-Maßnahmen erheblich helfen. Zum einen wird KI bereits von Unternehmen bei internen Untersuchun-

gen und von Kartellbehörden bei Kartellverfahren eingesetzt, um nach Kartellverstößen zu suchen. Dabei werden umfangreiche Datensätze von relevanten Mitarbeitern und Unternehmensteilen ausgewertet und nach auffälligen Kommunikations-, Bewegungs- und Verhaltensmustern gesucht, um Kartell- (und andere Compliance-)Verstöße zu ermitteln.

8.4 Fusionskontrolle

Im Rahmen der Fusionskontrolle spielt das Thema KI bisher nur eine untergeordnete Rolle. Wie aus dem oben Erläuterten hervorgeht, kann der Besitz von Software, die KI beinhaltet, zur Marktmacht von Unternehmen beitragen. Hieraus folgt, dass eben diese Software bei der Beurteilung der Marktverhältnisse vor und auch nach dem angestrebten Zusammenschluss eine gewichtige Rolle spielen kann. Ein Fokus der fusionskontrollrechtlichen Prüfung durch die Kartellbehörden könnte also in Zukunft auf den vorhandenen Technologien, die KI beinhalten, liegen. Dass sich der Fokus dahingehend verschiebt, deutet bereits die Schaffung des § 35 Abs. 1 lit. a GWB an. Dieser begründet, vereinfacht gesagt, trotz eigentlich zu geringer Umsätze der an der Fusion Beteiligten eine Anmeldepflicht, wenn der Kaufpreis des Zielunternehmens mehr als 400 Millionen Euro beträgt. Hierdurch wird vor allem anerkannt, dass wettbewerbsrechtlich bedenkliche Marktmacht nicht ausgeschlossen ist, wenn die gesetzlichen Umsatzschwellenwerte noch nicht erreicht sind. Vor allem die großen Technologie Konzerne erwerben immer häufiger (kleine) Unternehmen, die sich mit KI beschäftigen, sodass das Thema KI wohl in Zukunft auch im Rahmen der Fusionskontrolle an Bedeutung gewinnen wird. Für konkrete Handlungsanweisungen oder Empfehlungen müssen jedoch die Umstände des konkreten Zusammenschlussvorhabens betrachtet werden. Spannend ist auch, dass die herkömmliche Methodik zur Abgrenzung von Märkten anhand des SSNIP-Tests beeinflusst werden könnte, wenn algorithmische individualisierte Preisbildung verhindert, dass sich ein einheitlicher Marktpreis für eine größere Gruppe von Abnehmern bildet (Ylinen 2018, S. 19). Auch insoweit wird KI die Kartellrechtspraxis in Zukunft beeinflussen.

8.5 Fazit

Im Rahmen der bisherigen Fallpraxis zum Thema KI – vor allem Preissetzungsalgorithmen – war das derzeit kodifizierte Kartellrecht für eine sachgerechte Entscheidung (und hohe Bußgelder) ausreichend (Käseberg und von Kalben 2018, S. 3). Aufgrund der immer komplexer werdenden Algorithmen ist es vorstellbar, dass algorithmische Kollusion lange Zeit stattfindet, ohne dass eines der beteiligten Unternehmen hiervon Kenntnis hat. Dies verdeutlicht, welche hohen finanziellen Risiken mit einer kartellrechtsblinden Nutzung von KI einhergehen können. Daher sollten die Bestimmungen des Kartellrechts stets im Auge behalten werden, wenn ein Unternehmen auf KI zurückgreift. Als ganz wesentliche

Erkenntnis ist festzuhalten, dass sich ein Unternehmen durch den Einsatz von KI nicht seiner kartellrechtlichen Verantwortung entziehen kann. Ganz im Gegenteil kann der Einsatz entsprechender Algorithmen sogar zum Nachteil eines Unternehmens bei der Bußgeldbemessung im Hinblick auf die Schwere der Verletzung berücksichtigt werden.[13]

Die Europäische Kommission hat kürzlich aber auch betont, dass das bestehende Recht aufgrund der rapiden Entwicklung von KI wohl nicht alle speziellen Risiken dieser Entwicklung abdeckt. Daher besteht eine hohe Wahrscheinlichkeit, dass die Legislative im Zusammenhang mit Künstlicher Intelligenz in nicht allzu ferner Zukunft tätig werden wird. Die Europäische Wettbewerbskommissarin M. Vestager hat angekündigt, dass die Europäische Kommission in naher Zukunft Hinweise für Technologieunternehmen geben wird, die das kartellrechtskonforme Offenlegen von Daten zum Gegenstand haben.

Das Zusammenspiel von KI und Kartellrecht wird sich voraussichtlich in Zukunft noch intensivieren. Für Unternehmen ist daher wichtig das Thema Kartellrecht frühzeitig mit in den Blick zu nehmen, um sich keine ungewünschten – oder sogar unentdeckten – Risiken ins Haus zu holen.

Literatur

ADLC, BKartA (2016) Competition Law and Data. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.html?nn=3591568. Zugegriffen am 16.04.2020

BKartA (2017) Schriftenreihe „Big Data und Wettbewerb“. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.html. Zugegriffen am 16.04.2020

BKartA (2020) Algorithmen und Wettbewerb, Schriftenreihe „Wettbewerb und Verbraucherschutz in der digitalen Wirtschaft“. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_6.html?nn=3591568. Zugegriffen am 16.04.2020

Busse C (2017) Bundeskartellamt rügt Lufthansa. https://www.sueddeutsche.de/wirtschaft/nach-air-berlin-pleite-bundeskartellamt-ruegt-lufthansa-1.3806188. Zugegriffen am 16.04.2020

Dohrn D, Huck L (2018) Der Algorithmus als „Kartellgehilfe“? Der Betrieb 2018:173–178

Europäische Kommission (2011) Mitteilung der Kommission – Leitlinien zur Anwendbarkeit von Artikel 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52011XC0114%2804%29. Zugegriffen am 17.04.2020

Europäische Kommission (2017) Bericht der Kommission an den Rat und das Europäische Parlament – Abschlussbericht über die Sektoruntersuchung zum elektronischen Handel, COMP(2017) 229 final. https://op.europa.eu/en/publication-detail/-/publication/7ed6e02f-3570-11e7-a08e-01aa75ed71a1/language-de. Zugegriffen am 17.04.2020

Europäische Kommission (2018) Kartellrecht: Kommission verhängt Geldbußen gegen vier Elektronikhersteller wegen Festsetzung von Online-Wiederverkaufspreisen, 24.07.2018. https://ec.europa.eu/commission/presscorner/detail/de/IP_18_4601. Zugegriffen am 17.04.2020

Glöckner J (2017) Kartellrecht und Compliance, Institutionalisierte Rechtseinhaltung zwischen Professionalität und Potemkinschem Dorf. JuS 2017:905–913

Hoffer R, Mirtchev K (2019) Erfordert die Blockchain ein neues Kartellrecht? NZKart 2019:239–247

[13] CMA 12. August 2016, Case 50223, Rn. 6.23 c.

Janka SF, Uhsler SB (2018) Antitrust 4.0. Eur Compet Law Rev 2018:112–121
Käseberg T, von Kalben J (2018) Herausforderung der Künstlichen Intelligenz für die Wettbewerbspolitik – Preisbildung durch Algorithmen. WuW 2018:2–4
Künstner KM (2019) Preissetzung durch Algorithmen als Herausforderung des Kartellrechts. GRUR 2019:36–42
Künstner KM, Franz B (2017) Preisalgorithmen und Dynamic Pricing: Eine neue Kategorie kartellrechtswidriger Abstimmungen? K&R 2017:688–690
Locher L (2018) Verschiedene Preise für gleiche Produkte? Personalisierte Preise und Scoring aus ökonomischer Sicht. ZWeR 2018:292–293
OECD (2017a) Algorithms and Collusion – Background Note by the Secretariat, DAF/COMP(2017)4. https://one.oecd.org/document/DAF/COMP(2017)4/en/pdf. Zugegriffen am 17.04.2020
OECD (2017b) Algorithms and Collusion – Note from the European Union, 14.06.2017. https://one.oecd.org/document/DAF/COMP/WD(2017)12/en/pdf. Zugegriffen am 17.04.2020
Paal B (2019) Missbrauchstatbestand und Algorithmic Pricing, Dynamische und individualisierte Preise im virtuellen Wettbewerb. GRUR 2019:43–53
Ritz C, Marx L (2018) Algorithmen im Fokus der Monopolkommission: Digital Antitrust erfordert Anpassungen kartellrechtlicher Compliance. GRUR-Prax 2018:421–423
Salaschek U, Serafimova M (2018) Preissetzungsalgorithmen im Lichte von Art. 101 AEUV. WuW 2018:8–15
Thomas S (2016) In: Kling M, Thomas S (Hrsg) Deutsches Kartellrecht, 2. Aufl. Franz Vahlen, München
U.S. Department of Justice (2015) E-Commerce Exec and Online Retailer Charged with Price Fixing Wall Posters. https://www.justice.gov/opa/pr/e-commerce-exec-and-online-retailer-charged-price-fixing-wall-posters. Zugegriffen am 17.04.2020
Vestager M (2017) Vortrag im Rahmen der 18. Internationalen Kartellrechtskonferenz des Bundeskartellamts in Berlin am 16. März 2017
Wirtschaftswoche (2019) Wirtschaftswoche vom 29.03.2019, S. 37
Wolf M (2019) Algorithmengestützte Preissetzung im Online-Einzelhandel als abgestimmte Verhaltensweise. NZKart 2019:2–6
Ylinen J (2018) Digital Pricing und Kartellrecht. NZKart 2018:19–22
Zander-Hayar H, Reisch L, Steffen C (2016) Personalisierte Preise – Eine verbraucherpolitische Einordnung. VuR 2016:403–405

Gestaltung von Verträgen mit Bezug zu KI

9

Sabine von Oelffen

Zusammenfassung

In diesem Kapitel wird erläutert, inwieweit vertragliche Gestaltung im Rahmen von KI-Projekten notwendig ist und welche Besonderheiten zu beachten sind. Zum einen kann der Zugriff auf Maschinengenerierte Daten, mit welchen die KI „trainiert" werden soll eine vertragliche Grundlage erforderlich machen. Des Weiteren haben die Parteien, die an einer KI-Lösung beteiligt sind, grundsätzlich auch ein hohes Interesse daran, vertraglich festzulegen, wer Zugriff auf die durch die KI generierten Datensätze haben soll bzw. diese verwerten darf. Von einem Datenüberlassungsvertrag, in dem die zukünftigen Bezugsrechte von Datensätzen geregelt sind, bis hin zur Untersagung des Zugriffs auf die erhobenen Daten sind zahlreiche Gestaltungsmöglichkeiten denkbar.

Welche Arten von Verträgen in Zusammenhang mit dem Einsatz einer KI-Lösung abzuschließen sind, richtet sich insbesondere nach Einsatzzweck und technischen Besonderheiten der KI-Lösung sowie danach, wie viele und welche Stakeholder die KI-Lösung nutzen möchten. Grundsätzlich ist zwischen Verträgen über Daten, welche den Rohstoff für die Nutzung der KI-Lösung bilden und Verträgen über die KI-Lösung selbst zu unterscheiden. Verträge über Daten dienen dabei der Beschaffung von für die Nutzung der KI-Lösung benötigten Daten oder der Kommerzialisierung von durch die KI-Lösung gesammelten Daten. In diesem Kapitel[1] erhalten Sie zunächst einen Überblick über Beson-

[1] Hinweise zu Vertragsgestaltungen mit steuerrechtlichem Bezug unter Kap. 7, Abschn. 7.3.

S. von Oelffen (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: sabine.vonoelffen@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_9

derheiten der Gestaltung von Verträgen über Maschinengenerierte Daten,[2] gefolgt von Erläuterungen zu Besonderheiten der Gestaltung von Verträgen über die KI-Lösung selbst. Gegenstand von Verträgen über die KI-Lösung selbst ist hierbei typischerweise entweder die Erstellung der KI-Lösung oder die Einräumung bzw. der Erhalt von Nutzungsrechten an derselben durch Abschluss eines Lizenzvertrags.

Die Erläuterungen zu den jeweiligen Vertragstypen beziehen sich auf KI-spezifische Besonderheiten und stellen daher keine abschließende Auflistung aller Regelungsgegenstände dar, die in einen Vertrag des jeweiligen Vertragstypus aufzunehmen sind. Zusätzlich gelten daher die allgemeinen Grundsätze der Vertragsgestaltung für den jeweiligen Vertragstyp.

9.1 Verträge über Maschinengenerierte Daten

Der Abschluss eines Vertrags über Maschinengenerierte Daten kommt insbesondere in den nachfolgend genannten Fällen in Betracht:

Anwendungsfälle von Verträgen bzw. vertraglichen Regelungen über Maschinengenerierte Daten

Anwendungsfall 1: Das die KI-Lösung nutzende Unternehmen verfügt nicht über die zur Nutzung der KI-Lösung erforderlichen Maschinengenerierten Daten und kann diese auch nicht selbst erheben.

Anwendungsfall 2: Die KI-Lösung erzeugt während ihrer Nutzung Maschinengenerierte Daten. Das Anwenderunternehmen oder der Anbieter der KI-Lösung möchte diese weiter kommerzialisieren, d. h. Dritten anbieten.

Anwendungsfall 3: Die KI-Lösung erzeugt während ihrer Nutzung Maschinengenerierte Daten. Aufgrund technischer Konfiguration haben sowohl der Anbieter der KI-Lösung als auch das Anwenderunternehmen Zugriff auf die durch die KI-Lösung Maschinengenerierten Daten. Das wirtschaftliche Verwertungsrecht an diesen soll jedoch nur einer Partei zustehen.

Anwendungsfall 4: Die KI-Lösung erzeugt während ihrer Nutzung Maschinengenerierte Daten. Das Anwenderunternehmen ist technisch in der Lage, die KI-Lösung so zu konfigurieren, dass nur das Anwenderunternehmen, nicht jedoch der Anbieter der KI-Lösung unmittelbaren Zugriff auf die Maschinengenerierten Daten erhält. Der Anbieter der KI-Lösung möchte die Maschinengenerierten Daten jedoch ebenfalls für eigene Geschäftszwecke nutzen.

Da an Maschinengenerierten Daten kein Eigentum kraft Gesetzes besteht, gilt die „Herrschaft des Faktischen“. Das bedeutet, dass im Rahmen der gesetzlichen Grenzen[3] und

[2] Zu Verträgen über personenbezogene Daten siehe unter Kap. 2.

[3] Siehe hierzu unter Kap. 2.

ohne anderslautende Vereinbarungen diejenige Partei die Maschinengenerierten Daten kommerziell verwerten kann, die tatsächlichen Zugriff auf diese hat.

Sofern ausschließlich Maschinengenerierte Daten Gegenstand des Vertrags sind, findet die DS-GVO keine Anwendung.[4] Speziell auf Maschinengenerierte Daten zugeschnittene, gesetzliche Regelungen existieren derzeit nicht.

Auch wenn das Gesetz sachenrechtlich Daten nicht per se einem Eigentümer zuweist, können Maschinengenerierte Daten und ihre Überlassung dennoch Gegenstand schuldrechtlicher Verträge sein. Verträge über Maschinengenerierte Daten existieren in unterschiedlichen Erscheinungsformen: unter einem Datenüberlassungsvertrag ist die Überlassung Maschinengenerierter Daten zentraler Gegenstand des Vertrags. Der Abschluss eines Datenüberlassungsvertrags ist daher in den oben genannten Anwendungsfällen 1 und 2 Mittel der Wahl. Alternativ können die Parteien in einem Vertrag mit anderem Hauptgegenstand (z. B. einem Lizenzvertrag über die KI-Lösung) rechtliche Regelungen über Maschinengenerierte Daten als Zusatzvereinbarung treffen. Ein Beispiel hierfür ist Anwendungsfall 3, in dem eine Partei Interesse daran hat, mit der anderen Partei zu vereinbaren, dass nur sie selbst die durch die KI-Lösung erzeugten Maschinengenerierten Daten verwerten darf.

Die Aufnahme einer entsprechenden Regelung in einen Vertrag mit anderem Hauptgegenstand bietet sich zudem in Anwendungsfall 4 an, in dem der Anbieter der KI-Lösung die von dem Anwenderunternehmen während der Nutzung erzeugten Maschinengenerierten Daten ebenfalls für eigene Geschäftszwecke nutzen möchte und aufgrund technischer Konfiguration nicht ohnehin selbst unmittelbaren Zugriff auf diese Maschinengenerierten Daten hat. Hauptgegenstand des Vertrags ist auch in diesem Fall die Lizenzierung bzw. Überlassung der KI-Lösung. Das Zugriffsrecht des Anbieters der KI-Lösung auf die Maschinengenerierten Daten können die Parteien sodann als Sonderregelung im Rahmen des Lizenzvertrags vereinbaren.

► **Praxistipp** Überlegen Sie projektbezogen, ob der Abschluss eines eigenständigen Datenüberlassungsvertrags notwendig und sinnvoll ist oder ob Sie in dem Vertrag über die Entwicklung oder Lizenzierung der KI-Lösung Regelungen über Rechte an den durch diese Maschinengenerierten Daten treffen möchten.

Vertragliche Rechte an durch die KI-Lösung Maschinengenerierten Daten können sowohl positiv (Zuweisung der Rechte) als auch negativ (vertragliche Untersagung des Datenzugriffs/der Datenverwertung) formuliert sein.

9.1.1 Datenüberlassungsverträge

Datenüberlassungsverträge können sowohl als Datenkaufvertrag im Sinne von § 433 BGB in Form eines Kaufs von sonstigen Gegenständen gemäß § 453 BGB oder als Datenlieferungsvertrag, welcher Elemente des Pacht- oder des Mietrechts aufweist, geschlossen werden. Legen Sie den beabsichtigen Vertragstyp ausdrücklich in dem Vertrag fest.

[4] Siehe zu Verträgen über personenbezogene Daten unter Kap. 2.

Insbesondere aus Sicht des Datenbeziehers ist eine vertragliche Regelung, welche den beabsichtigten Vertragstyp festlegt, schon zur Reduzierung des Risikos von Streitigkeiten, welche gesetzlichen Regelungen in Bezug auf Gewährleistung (Kauf- oder Pacht- bzw. Mietrecht) in dem konkreten Fall anwendbar sind, empfehlenswert.[5]

Der Daten(ver-)kauf im Sinne des Abschlusses eines Daten(ver-)kaufvertrags im Sinne von § 433 BGB ist nur dann von Interesse, wenn der Verkäufer des Datenbestands diesen nur einem bestimmten Käufer zur Verfügung stellen und sich dauerhaft von dem Datenbestand trennen möchte. Sachenrechtlich wird in diesem Fall jedoch an dem Datenbestand kein vollwertiges, absolutes Recht im Sinne von § 929 ff. BGB eingeräumt,[6] sondern lediglich eine quasi-absolute, faktische Rechtsposition begründet, die ausschließlich zwischen den Parteien wirkt. Gegenüber Dritten, die nicht Vertragspartei sind, entfaltet diese Vereinbarung nicht die Wirkung einer eigentumsähnlichen Rechtsposition.

In den meisten Fällen dürfte ein Datenlieferungsvertrag, bei dem der Datenbestand weiterhin (auch) bei dem Datengeber verbleibt und dieser gegen Entgelt (mehreren) Nutzern Nutzungsrechte an dem Datenbestand einräumt, jedenfalls aus kommerzieller Perspektive attraktiver sein, da derselbe Datensatz mehreren Kunden gegen Entgelt angeboten werden kann. Der Datenlieferungsvertrag ist ein typengemischter Vertrag (Arning 2018, § 15 Rz. 1), der je nach Ausgestaltung Elemente des Kauf- und/oder Pacht- bzw. Mietvertrags enthalten kann.

▶ **Praxistipp** Um Streitigkeiten über die auf den Vertrag anwendbaren, zivilrechtlichen Regelungen vorzubeugen, sollten die Parteien ihren diesbezüglichen Willen hinsichtlich der vertragstypologischen Einordnung des abzuschließenden Vertrags ausdrücklich im Vertrag niederlegen.

Entscheiden Sie projektbezogen, ob Sie einen Daten(ver-)kaufvertrag oder einen Datenlieferungsvertrag abschließen möchten.

9.1.1.1 Vertragsgegenstand

Achten Sie beim Abschluss eines Datenüberlassungsvertrags insbesondere auf eine akkurate Beschreibung des geschuldeten Leistungsgegenstands in Form der bereitzustellenden Maschinengenerierten Daten. Detaillierte technische Leistungsbeschreibungen sollten dabei in eine Anlage ausgegliedert werden, um die Übersichtlichkeit des Vertrags zu wahren. Mögliche Regelungsaspekte sind insbesondere der Umfang des Datenbestandes, die Quelle der Daten, die Verfügbarkeit neuer Datensätze und – sofern zutreffend – die Definition der Daten als anonyme Daten (Arning 2018, § 15 Rz. 19–26). Bedenken Sie auch, dass eine präzise Beschreibung des Leistungsgegenstands von großer Bedeutung für eine etwaig später notwendige Geltendmachung von Gewährleistungsrechten ist, beurteilt sich doch anhand der Leistungsbeschreibung, ob die Leistung vertragsgemäß ist (Kirchner

[5] Siehe für ein Beispiel einer vertraglichen Regelung zu Gewährleistungsrechten beim Datenlieferungsvertrag: Arning 2018, § 15 Rz. 63.

[6] Siehe zum Meinungsstand in der Literatur Schefzig 2015, S. 553.

2018, S. 21). Aus Sicht des Datengebers ist demgegenüber wichtig, die Parameter und Faktoren von der Beschaffenheitsvereinbarung auszunehmen, die sich außerhalb der Einflusssphäre des Datengebers befinden und für die dieser deswegen nicht einstehen möchte (Arning 2018, § 15 Rz. 22–23).

9.1.1.2 Gewährleistungsrechte

Welche Gewährleistungsrechte dem Datenbezieher zustehen, richtet sich danach, ob die Datenüberlassung im Rahmen eines Datenkaufvertrags gem. § 433 BGB oder eines Datenlieferungsvertrags, welcher Elemente des Pacht- oder des Mietrechts aufweist, erfolgt. Modifizieren die Parteien die Gewährleistungsrechte nicht vertraglich, so gelten (ausschließlich) die jeweiligen gesetzlichen Regelungen.

Bei einem Datenkaufvertrag stehen dem Datenbezieher grundsätzlich die Rechte aus § 437 BGB zu (Wilhelmi 2019, Rn. 154). Demgegenüber stehen dem Datenbezieher unter einem Datenlieferungsvertrag die Rechte aus § 581 Abs. 2 BGB in Verbindung mit §§ 536 f. BGB zu (Kirchner 2018, S. 22), sofern dieser keine abweichenden vertraglichen Regelungen enthält.

Naturgemäß haben Datenbezieher und Datengeber jedenfalls teilweise gegenläufige Zielvorstellungen im Hinblick auf die Inhalte der Gewährleistungsregelung.

Der Datenbezieher kann je nach Einzelfall insbesondere Interesse an den nachfolgend genannten Modifikationen der gesetzlichen Gewährleistungsrechte haben:

Werden unter dem Vertrag ausschließlich Maschinengenerierte Daten überlassen, so ist empfehlenswert, eine Regelung aufzunehmen, wonach der Datengeber gewährleistet, dass die überlassenen Daten keine personenbezogenen Daten sind.[7] Darüber hinaus ist es für den Datenbezieher ratsam, sich vom Datengeber versichern zu lassen, dass die Daten frei von Rechten Dritter sind (Hackenberg 2019, Teil 16.7 Rn. 38). Maschinengenerierte Daten könnten beispielsweise den wesentlichen Teil einer nach §§ 87a ff. UrhG geschützten Datenbank, an welcher ein Dritter Rechte hält, darstellen (Kraus 2015, S. 546). Auf semantischer Ebene können Daten auch anderweitig, sogar strafrechtlich, geschützt sein. So könnte es sich bei ihnen um Geschäftsgeheimnisse handeln (Kraus 2015, S. 546; Hackenberg 2019, Teil 16.7 Rn. 38), die den Vorschriften des **Geschäftsgeheimnisgesetzes** (**GeschGehG**) unterliegen. Der Datenbezieher sollte daher eine Gewährleistung des Datengebers, dass es sich bei den Daten nicht um Geschäftsgeheimnisse handelt, anstreben. Wünschenswert aus Sicht des Datenbeziehers kann zudem eine Gewährleistung des Datengebers für die Richtigkeit der Maschinengenerierten Daten und/oder deren Aussagegehalt sein (Kraus 2015, S. 546). Ob derartige Regelungen sinnvoll sind und der Datenbezieher diese in den Vertragsverhandlungen durchsetzen kann, hängt von der Art der zu überlassenden Maschinengenerierten Daten und deren Verwendungszweck, den berechtigten Interessen des Datengebers und letztlich auch von der Verhandlungsmacht des Datenbeziehers ab. Anderes gilt freilich in Fällen, in denen nicht nur Maschinengenerierte Daten überlassen werden. So ist es im Interesse beider Parteien, von der Vereinbarung

[7] Siehe allgemein zu dieser Thematik Arning 2018, § 15 Rz. 63–74.

einer Gewährleistung für die Richtigkeit der Daten abzusehen, wenn die Verifizierung der Richtigkeit eine Rückverfolgung auf ursprünglich personenbezogene und später anonymisierte Daten notwendig macht (Arning 2018, § 15 Rz. 23). Ist dies jedoch von vornherein ausgeschlossen, da ausschließlich Maschinengenerierte Daten überlassen werden, kann eine Gewährleistung für die Richtigkeit dieser demgegenüber aus Sicht des Datenbeziehers erstrebenswert sein.

Wann die Maschinengenerierten Daten mangelhaft sind, richtet sich nach den vertraglichen Vereinbarungen und (ggf. ergänzend) nach den gesetzlichen Regelungen. Daher ist eine (ausführliche) vertragliche Vereinbarung über den Vertragsgegenstand einschließlich von den Parteien festzulegender Parameter, welche die Maschinengenerierten Daten erfüllen müssen sowie des angestrebten Verwendungszwecks essenziell.[8] Ein Mangel der Maschinengenerierten Daten dürfte jedenfalls dann vorliegen, wenn Datensätze fehlerhaft übertragen wurden (Arning 2018, § 15 Rz. 67) oder unvollständig sind. Die Behebung eines Mangels eines überlassenen Datensatzes wird in der Praxis in der Regel durch Bereitstellung eines mangelfreien Datensatzes erfolgen. Bei einem pachtvertraglich ausgestalteten Datenlieferungsvertrag hat der Datenbezieher zudem gem. § 581 Abs. 2 BGB in Verbindung mit § 536 Abs. 1 BGB ein Recht auf Minderung des Pachtzinses für die Zeit, in der die geschuldeten Maschinengenerierten Daten nicht mangelfrei zur Verfügung stehen.

Aus Sicht des Datengebers können demgegenüber insbesondere die nachfolgend genannten Modifikationen der gesetzlichen Gewährleistungsrechte sinnvoll sein:

Aus Sicht des Datengebers ist es vorteilhaft, die gesetzlich geltenden Regelungen zu Gewährleistung und Haftung im Datenüberlassungsvertrag (ggf. unter Beachtung der §§ 305 ff. BGB) einzuschränken, da ansonsten dem Datenbezieher abhängig von der vertragstypologischen Einordnung des Datenüberlassungsvertrags sämtliche gesetzlichen Rechte nach §§ 437 ff. BGB bzw. § 581 Abs. 2 BGB in Verbindung mit §§ 536 f. BGB zustehen.

▶ **Praxistipp** Modifizieren und ergänzen Sie die gesetzlichen Gewährleistungsrechte durch vertragliche Vereinbarungen, die den Besonderheiten des Datenüberlassungsvertrags Rechnung tragen.

Im Übrigen, d. h., soweit die gesetzlichen Rechte nicht durch den Datenüberlassungsvertrag modifiziert oder ausdrücklich ausgeschlossen werden, sollten im Regelfall die gesetzlichen Rechte (nachrangig) Anwendung finden und somit nicht vollständig ausgeschlossen werden.

9.1.1.3 Sicherung der Exklusivität?

Abhängig von der Art des Datenbestands und angestrebtem Nutzungszweck kann der Datenbezieher ein Interesse daran haben, ein ausschließliches Nutzungsrecht an dem Datenbestand zu erhalten. Dies kommt beispielsweise dann in Betracht, wenn sich der

[8] Ein Beispiel für eine entsprechende Regelung enthält Arning 2018, § 15 Rz. 18.

Datenbezieher durch die Aus- und Verwertung des Datenbestands einen Wettbewerbsvorsprung am Markt verschaffen möchte. Je nach Einzelfall kann die Vereinbarung einer eingeschränkten Exklusivität, die nur im Hinblick auf die Wettbewerber des Datenbeziehers gilt, ausreichend sein (Schefzig 2015, S. 561). Vertraglich kann ein ausschließliches Nutzungsrecht an Daten entweder durch Abschluss eines Daten(ver-)kaufvertrags oder durch Einräumung ausschließlicher Nutzungsrechte unter einem Datenlieferungsvertrag vereinbart werden. Ggf. kann die Exklusivität zusätzlich durch eine Vertragsstrafe oder Gewinnabschöpfungsklausel (Riehm 2019, S. 716) abgesichert werden.[9]

9.1.1.4 Zukünftiges Bezugsrecht

Datenbezieher können sich vertraglich ein Bezugsrecht für weitere Datensätze in der Zukunft einräumen lassen. Anderenfalls besteht beispielsweise kein Anspruch auf eine Erhöhung der zu liefernden Datenmenge oder auf Lieferung neuer Datensätze, welche über den ursprünglich vertraglich geschuldeten Umfang hinausgehen. Auf diese Weise lassen sich zeitaufwendige und teure Neuverhandlungen vermeiden und die KI-Lösung erhält schnell und flexibel die zusätzlich benötigten Maschinengenerierten Daten. Als Datenbezieher vereinbaren Sie idealerweise zudem Preisstabilität für einen zeitlich näher zu bestimmenden Zeitraum.

9.1.2 Regelung von Zugriffsrechten in dem Vertrag über die KI-Lösung

Hauptgegenstand der unter Abschn. 9.1.1 erläuterten Datenüberlassungsverträge ist die Zurverfügungstellung Maschinengenerierter Daten, welche in die KI-Lösung zur weiteren Nutzung eingespeist werden (z. B. zum Zwecke des „Trainings“ derselben). Rechte an Maschinengenerierten Daten, welche die KI-Lösung selbst erzeugt, können die Parteien hingegen (auch) als Sonderregelung in dem Vertrag über die Zurverfügungstellung der KI-Lösung vereinbaren. Sowohl Anbieter von KI-Lösungen als auch Hersteller von Produkten, die KI-basierte Software enthalten als auch (kommerzielle) Endnutzer dieser Produkte können Interesse haben, durch die KI-Lösung generierte, Maschinengenerierte Daten zu erhalten.

Wünscht – wie beispielsweise in Anwendungsfall 4 (Abschn. 9.1) der jeweilige Anbieter der KI-Lösung oder der Hersteller oder Endnutzer eines KI-basierten Produkts den Zugriff auf die bzw. eine Übermittlung der entsprechenden Maschinengenerierten Daten, sollte er sich dieses Recht vertraglich einräumen lassen. Der Anbieter der KI-Lösung bzw. Hersteller eines KI-basierten Produkts kann zwar die technischen Voraussetzungen für einen Zugriff bzw. eine Übermittlung der Maschinengenerierten Daten schaffen, sollte sich jedoch zusätzlich vertraglich davor schützen, dass der Nutzer der KI-Lösung und/

[9] Die für Vertragsstrafen und Gewinnabschöpfungsklauseln geltenden Grenzen der §§ 305 ff. BGB sind ggf. zu beachten (Riehm 2019, S. 716).

oder des Produkts die Datenübermittlung durch von diesem vorgenommene, technische Einstellungen faktisch verhindert. Der Anbieter der KI-Lösung bzw. der Hersteller sollte unter technischen Gesichtspunkten entscheiden, ob er sich lediglich ein vertragliches Recht auf Zugriff (z. B. über eine Schnittstelle) oder ein weitergehendes Recht auf Übermittlung der Maschinengenerierten Daten an ihn einräumen lassen möchte. Der Datengeber schuldet in beiden Fällen die Übermittlung der Maschinengenerierten Daten bis zum vereinbarten Übergabepunkt.

▶ **Praxistipp** Prüfen Sie, welche Stakeholder (Anbieter der KI-Lösung, Hersteller eines Produkts, das die KI-Lösung eines anderen Anbieters einbettet, Anwenderunternehmen, Endnutzer) technisch Zugriff auf die durch die KI-Lösung Maschinengenerierten Daten haben bzw. eine Datenübermittlung wünschen.

Im Einzelnen ist zwischen verschiedenen Fallkonstellationen zu differenzieren:

9.1.2.1 Vertragliches Recht des Anbieters auf Datenübermittlung

Solange die KI-Lösung ausschließlich Maschinengenerierte (und keine personenbezogenen Daten) erzeugt, kann der Anbieter der KI-Lösung dieselbe schlicht so konfigurieren, dass er faktische Zugriffsmöglichkeiten auf die durch das Anwenderunternehmen erzeugten Maschinengenerierten Daten erhält. Weder der Hersteller eines KI-basierten Produkts noch die Anwenderunternehmen sind in diesem Fall ohne ausdrückliche Zustimmung des Anbieters berechtigt, die Software so zu verändern, dass der Anbieter die Zugriffsmöglichkeiten auf die Maschinengenerierten Daten verliert. Urheberrechtlich ist die Vornahme von nicht von dem Urheber autorisierten, technischen Veränderungen an der Software, die dazu führen, dass der Urheber die Zugriffsmöglichkeiten auf die durch diese Maschinengenerierten Daten verliert, außer in eng begrenzten Ausnahmefällen nicht zulässig. Eine zusätzliche, vertragliche Regelung, die dem Vertragspartner technische Gestaltungen, durch die ein Zugriff auf die bzw. eine Übermittlung der Maschinengenerierten Daten faktisch unmöglich wird, untersagt, ist dennoch sinnvoll. Vertragliche Ansprüche sind aus rechtlicher Sicht vorteilhafter als gesetzliche Ansprüche. Zudem wäre ein etwaiger urheberrechtlicher Unterlassungsanspruch nur auf die Unterlassung entsprechender Veränderungen an der Software gerichtet, nicht aber auf aktive Übermittlung der durch die KI-Lösung erzeugten Maschinengenerierten Daten. Wird die KI-Lösung in ein Produkt eines anderen Herstellers implementiert, ist zudem nicht auszuschließen, dass eine Datenübermittlung durch die Konfiguration des Produkts (und nicht durch Veränderungen an der KI-Lösung selbst) verhindert wird.

Der Anbieter der KI-Lösung sollte sich daher ungeachtet seiner etwaigen urheberrechtlichen Ansprüche ein vertragliches Recht auf Zugriff auf die bzw. Übermittlung der gewünschten Maschinengenerierten Daten einräumen lassen. Unterscheiden Sie auch hier verschiedene Fallkonstellationen: Vermarktet der Anbieter die KI-Lösung zur unmittelbaren Nutzung an Anwenderunternehmen (**B2B**) oder Verbraucher (**B2C**), so kann ein entsprechendes Recht in die für die KI-Lösung geltenden Lizenzbedingungen aufgenom-

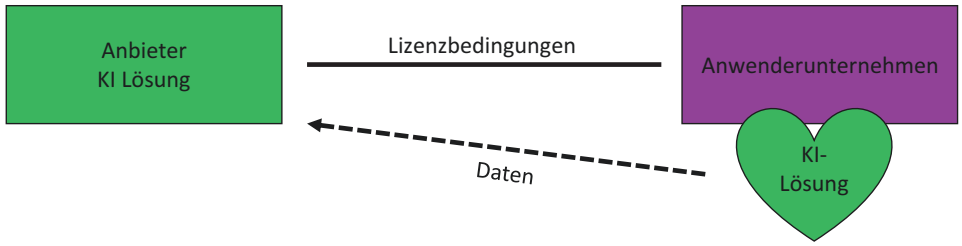

Abb. 9.1 Vertragliches Recht des Anbieters auf Datenübermittlung I

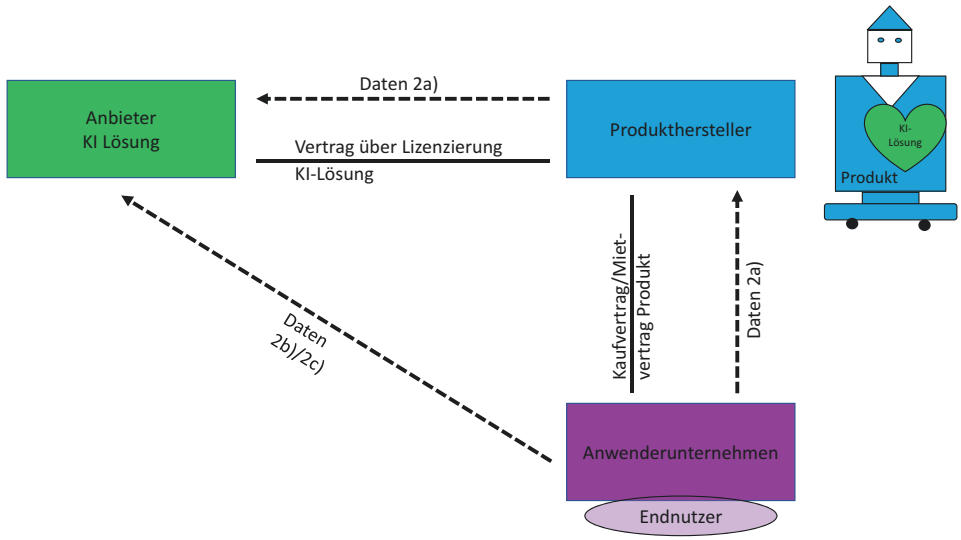

Abb. 9.2 Vertragliches Recht des Anbieters auf Datenübermittlung II

men werden. Sofern die entsprechende Regelung in den Lizenzbedingungen nicht individuell verhandelt wird, sind die durch §§ 305 ff. BGB gezogenen Grenzen für allgemeine Geschäftsbedingungen zu beachten (Abb. 9.1).

Eine andere Fallkonstellation ist gegeben, wenn die KI-Lösung in ein Produkt eines anderen Herstellers implementiert wird, welcher das KI-basierte Produkt dann weitervermarktet (Abb. 9.2). Möchte der Anbieter der KI-Lösung während der Nutzung des Produkts durch das Anwenderunternehmen Maschinengenerierte Daten erhalten, so sollte er dem Produkthersteller in dem Vertrag über die Lizenzierung der in das Produkt implementierten KI-Lösung folgende Verpflichtungen auferlegen:

(1) Technische Gestaltung des Produkts in einer Art und Weise, die eine Übermittlung der Maschinengenerierten Daten an den Anbieter der KI-Lösung ermöglicht und entweder
(2a) Verpflichtung des Produktherstellers, in den mit dem Anwenderunternehmen abzuschließenden Kauf- oder Mietvertrag über das KI-basierte Produkt eine Verpflich-

tung zur Übermittlung der Maschinengenerierten Daten an den Produkthersteller aufzunehmen und Verpflichtung des Produktherstellers zur Übermittlung der Maschinengenerierten Daten an den Anbieter der KI-Lösung
oder

(2b) Verpflichtung des Produktherstellers, in den mit dem Anwenderunternehmen abzuschließenden Kauf- oder Mietvertrag über das KI-basierte Produkt eine Verpflichtung des Endkunden zur direkten Übermittlung der Maschinengenerierten Daten an den Anbieter der KI-Lösung aufzunehmen
oder

(2c) Verpflichtung des Anwenderunternehmens zur Datenübermittlung in den Endnutzer-Lizenzbedingungen des Anbieters für die KI-Lösung und Verpflichtung des Produktherstellers zur Durchreichung dieser Endnutzer-Lizenzbedingungen an das Anwenderunternehmen. Die Datenübermittlung erfolgt in diesem Fall auch direkt an den Anbieter der KI-Lösung (siehe 2b).

9.1.2.2 Vertragliches Recht des Herstellers KI-basierter Produkte auf Datenübermittlung

Auch der Hersteller eines KI-basierten Produkts kann ein Interesse daran haben, sich ein vertragliches Recht auf Übermittlung Maschinengenerierter Daten, die bei der Nutzung des Produkts erzeugt werden, einräumen zu lassen (Abb. 9.3). Werden die Maschinengenerierten Daten durch eine in das Produkt implementierte KI-Lösung eines anderen Anbieters erzeugt, so sollte der Produkthersteller in den mit dem Anbieter zu schließenden Vertrag über die KI-Lösung eine Regelung aufnehmen, die den Anbieter verpflichtet, den Endnutzern in seinen Lizenzbedingungen eine entsprechende Verpflichtung zur Daten-

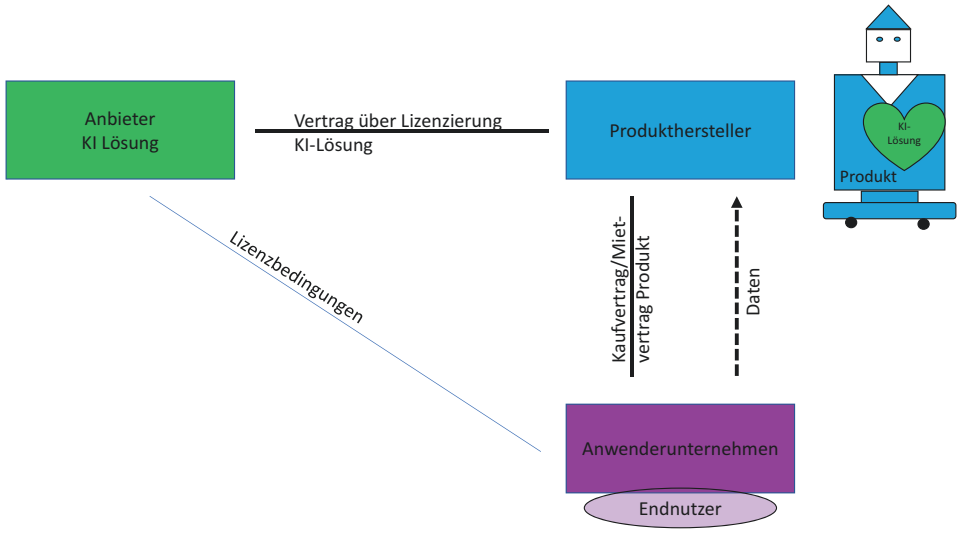

Abb. 9.3 Vertragliches Recht des Herstellers KI-basierter Produkte auf Datenübermittlung

übermittlung aufzuerlegen. Alternativ kann sich der Produkthersteller in dem mit dem Anwenderunternehmen zu schließenden Kauf- oder Mietvertrag ein Recht auf Übermittlung der Maschinengenerierten Daten durch das Anwenderunternehmen einräumen lassen.

9.1.2.3 Vertragliches Recht des Endnutzers KI-basierter Produkte auf Datenübermittlung?

Auch der Endnutzer eines KI-basierten Produkts kann ein Interesse an der Übermittlung von während der Nutzung des Produkts Maschinengenerierten Daten haben. Die Entscheidung, ob der Endnutzer faktisch Zugriff auf die gewünschten Maschinengenerierten Daten erhält, treffen jedoch typischerweise der Anbieter der KI-Lösung und/oder Produkthersteller, da diese durch die technische Konfiguration festlegen können, ob – und wenn ja – auf welche Maschinengenerierten Daten der Endnutzer Zugriff erhält. Je nach Einzelfall erhält der Endnutzer unter Umständen lediglich Informationen über die mittels Maschinengenerierter Daten durch die KI-Lösung erzeugten Ergebnisse, nicht aber Zugriff auf die Maschinengenerierten Daten in Reinform. Ist ein Zugriff auf die Maschinengenerierten Daten durch den Endnutzer nicht per Voreinstellung vorgesehen, hängt es von der Verhandlungsmacht ab, ob der Endnutzer ein vertragliches Recht zum Zugriff auf alle Maschinengenerierten Daten erhält. Im Einzelfall kann der Endnutzer auch einen gesonderten Datenüberlassungsvertrag schließen. Interesse am Erhalt der durch KI-Lösungen Maschinengenerierten Daten haben beispielsweise Landwirte im Bereich des *Smart Farming*, also der durch vernetzte IT-Lösungen unterstützten Landwirtschaft. Nutzt ein Landwirt mehrere KI-gestützte Landmaschinen, wobei jede Maschine für den landwirtschaftlichen Betrieb relevante Daten sammelt, so dürfte der Landwirt Interesse daran haben, diese zu erhalten, um sie für sich auszuwerten und darauf basierend betriebliche Entscheidungen zu treffen. Beispielsweise sammelt eine die Felder überfliegende Drohne Informationen über den Pflanzenzustand (Schädlingsbefall, etc.) und ein Schlepper während der Arbeit auf dem Feld Daten zur Bodenbeschaffenheit. Erhält der Landwirt von den jeweiligen Maschinen nicht nur aggregierte Ergebnisse, sondern die Daten in Reinform, so kann er diese (ggf. mittels weiterer Spezialsoftware) insgesamt auswerten und Bewässerung, Schädlingsbekämpfung und Düngung optimal dem aktuellen Zustand der Böden und Pflanzen anpassen.

9.1.2.4 Ausgestaltung eines vertraglichen Rechts auf Zugriff bzw. Übermittlung

Eine vertragliche Regelung, durch die sich eine Partei ein Recht auf Gewährleistung des Zugriffs auf die bzw. Übermittlung der Maschinengenerierten Daten einräumen lassen möchte, sollte insbesondere folgende Aspekte abdecken:

- **Eckpunkte einer vertraglichen Regelung auf Zugriff auf bzw. Übermittlung Maschinengenerierter Daten**
  - Unterlassung technischer Gestaltungen, durch die ein Zugriff auf bzw. eine Übermittlung der Maschinengenerierten Daten faktisch unmöglich wird;

- Ggf. Schaffung der technischen Voraussetzungen, durch die ein Zugriff auf bzw. eine Übermittlung der Maschinengenerierten Daten ermöglicht wird;
- Beschreibung der Art der zu übermittelnden Maschinengenerierten Daten;
- Ggf. Untersagung, Dritten ebenfalls Zugriff auf die Daten zu gewähren (Grund: Ausschöpfung des wirtschaftlichen Werts der Daten durch den Datengeber selbst);
- Ggf. Regelung der zu zahlenden Vergütung.

▶ **Praxistipp** Teilweise versuchen Softwareanbieter, für die Nutzung mittels ihrer Software erzeugter Daten durch Dritte separate Lizenzgebühren zu verlangen. Anknüpfungspunkt für die Forderung entsprechender Lizenzgebühren ist in diesen Fällen der Export der Maschinengenerierten Daten in das System des Dritten. Inwieweit derartige Forderungen zusätzlicher Lizenzgebühren berechtigt sein können, ist aus rechtlicher Sicht umstritten und letztlich für jeden Einzelfall gesondert zu beurteilen. Schützen Sie sich vor überraschenden Forderungen, indem Sie die Lizenzbedingungen prüfen und ggf. eine ausdrückliche Regelung in den Vertrag aufnehmen, wonach der Export der mittels der KI-Lösung erzeugten Daten an ggf. näher zu benennende Parteien und/oder Dritte keine zusätzlichen Lizenzgebühren auslöst!

9.1.3 Vertragliche Untersagung des Zugriffs

Der Anbieter einer KI-Lösung bzw. eines KI-basierten Produkts hat unter Umständen ein wirtschaftlich motiviertes Interesse daran, dass nur er selbst Zugriff auf bestimmte, von der KI-Lösung bzw. dem KI-basierten Produkt erhobene Daten erhält und somit deren wirtschaftlichen Wert voll ausschöpfen kann. Im Rahmen der durch das Urheberrecht gesetzten (engen) Grenzen kann der Anbieter einer KI-Lösung seinen Vertragspartnern vertraglich den Einsatz technischer Maßnahmen zur Umgehung der von ihm implementierten Schutzmaßnahmen untersagen. Sofern eine derartige Regelung Teil allgemeiner Geschäftsbedingungen ist, sind die §§ 305 ff. BGB zu beachten. Im Sinne einer effizienten Wirkung der vertraglichen Vereinbarung kann in Individualverträgen zudem eine Vertragsstrafe vereinbart werden.

9.2 Verträge über die KI-Lösung

Anwenderunternehmen, die eine KI-Lösung benötigen und diese nicht selbst entwickeln wollen, können entweder einen Dienstleister beauftragen, eine KI-Lösung individuell zu entwickeln (Entwicklung von Individualsoftware) oder eine für viele Anwenderunternehmen konzipierte, standardisierte KI-Lösung lizenzieren (Lizenzierung von Standardsoftware). Beauftragt ein Kundenunternehmen die individuelle Entwicklung einer KI-Lösung

für seine eigenen Zwecke, richtet sich der Vertragsinhalt zunächst nach den allgemein für Verträge über die Entwicklung von Individualsoftware geltenden Grundsätzen. Dementsprechend ist ein Vertrag über die individuelle Entwicklung einer KI-Lösung Werkvertrag, Dienstvertrag oder gemischt-typischer Vertrag mit Elementen des Dienst- und Werkvertragsrechts. Demgegenüber bilden das Urheberrechtsgesetz sowie allgemeine Grundsätze des IT-Vertragsrechts den rechtlichen Rahmen für die Einräumung bzw. den Erhalt von Nutzungsrechten durch Abschluss eines Lizenzvertrags über eine standardisierte KI-Lösung. Je nach Art der Lizenzierung findet dann Kauf- oder Mietrecht Anwendung. Nachfolgend erhalten Sie daher einen Überblick über diejenigen Aspekte, die über die allgemeinen vertragsrechtlichen Grundlagen hinausgehend in Bezug auf KI-Lösungen von besonderer Bedeutung sind. Insgesamt sollten die vertraglichen Regelungen dabei die Tatsache, dass eine KI-Lösung Vertragsgegenstand ist sowie sich daraus ergebende Besonderheiten und Rechtsfolgen deutlich widerspiegeln. Die genaue Ausgestaltung der vertraglichen Regelungen wird freilich auch dadurch geprägt, ob der Vertrag insgesamt überwiegend auftraggeberfreundlich oder auftragnehmerfreundlich ist oder den Interessen beider Parteien ausgewogen Rechnung tragen soll. Neben den KI-spezifischen Besonderheiten sollten Verträge über die Entwicklung bzw. Lizenzierung einer KI-Lösung alle Themen adressieren, die üblicherweise in IT-Verträgen des jeweiligen Vertragstypus enthalten sind.

► **Praxistipp** Entscheiden Sie, welcher Vertragstyp (Werkvertrag, Dienstvertrag, gemischt-typischer Vertrag mit Elementen des Dienst- und Werkvertragsrechts) oder Lizenzvertrag (kaufrechtlich oder mietrechtlich ausgestaltet) in dem konkreten Fall vorteilhaft ist.

9.2.1 Präambel

Die Präambel bildet als Einleitung die Interpretationsleitlinie für die folgenden Regelungen des Vertrags und bietet den Parteien die Möglichkeit, die Ausgangs- und Zielsituation im Hinblick auf die dem Vertrag zugrunde liegenden Umstände zu beschreiben (Thalhofer und Żdanowiecki 2019, § 19 Rn. 59). Zu Beginn der Präambel werden die den Vertrag unterzeichnenden Parteien beschrieben (Schmidt 2019a, Kap. 6.1, Rn. 10). Beauftragt ein Unternehmen einen Dienstleister mit der Entwicklung einer KI-Lösung und/oder schließt einen Lizenzvertrag über eine solche ab, so ist es aus Auftraggebersicht vorteilhaft, die Expertenstellung des Dienstleisters gerade für die Entwicklung und/oder Bereitstellung von KI-Lösungen hervorzuheben. Anbieter der KI-Lösungen versuchen demgegenüber vielfach, eine vertragliche Expertenstellung zu vermeiden, da diese (besonders) hohe Anforderungen hinsichtlich der Qualität der KI-Lösung begründet. Sodann gilt es, den Hintergrund des Vertrags zu schildern. Setzt das Unternehmen erstmalig eine KI-Lösung ein oder dient diese zur Ergänzung bereits bestehender Produkte? Soll die KI-Lösung für unternehmenseigene Zwecke (z. B. in der Produktion oder im Rahmen von Predictive

Maintenance) eingesetzt werden oder kommt die KI-Lösung gegenüber Endkunden zum Einsatz? Welche (allgemeinen) Erwartungen und Ziele werden mit der KI-Lösung verfolgt? Da die Präambel regelmäßig von Gerichten zur Auslegung des gesamten Vertrags herangezogen wird[10] (Schmidt 2019a, Kap. 6.1, Rn. 10), ist eine auf den konkreten Vertragszweck und die jeweilige KI-Lösung individuell zugeschnittene Präambel empfehlenswert.

9.2.2 Vertragsgegenstand/Anlage: Leistungsbeschreibung

Vertragsgegenstand und Leistungsbeschreibung kommt stets herausragende Bedeutung zu, bilden doch diese Regelungen den Maßstab, ob die Leistungen die „vereinbarte Beschaffenheit" aufweisen oder ob ggf. ein Mangel vorliegt (Conrad und Witzel 2019, § 18 Rn. 24–26). Da Vertragsgegenstand und Leistungsbeschreibung stets eine juristische und eine technische Komponente haben, sollten Sie diese aus juristischer und technischer Perspektive prüfen. Je nach Einsatzfeld der KI-Lösung können zudem ethische Aspekte von großer Bedeutung und somit in der Leistungsbeschreibung festzuhalten sein. Dies gilt umso mehr, als die EU einen besonderen Fokus auf ethische Aspekte des Einsatzes von KI legt. Die von der Unabhängigen Hochrangigen Expertengruppe für Künstliche Intelligenz (HEG-KI) entwickelte „Bewertungsliste für vertrauenswürdige KI" (HEG-KI 2019, S. 32–41) enthält eine aussagekräftige Zusammenstellung von Kriterien, die eine aus ethischer Sicht vertrauenswürdige KI-Lösung erfüllen sollte. Es ist empfehlenswert, in der Leistungsbeschreibung darzustellen, durch welche technischen Verfahren die KI-Lösung die Kriterien für vertrauenswürdige KI erfüllt.

Bei KI-Lösungen sind häufig sowohl die durch die KI Lösung getroffenen „Entscheidungen" als auch die algorithmische Logik hinter der Entscheidungsfindung im Detail nicht nachvollziehbar (sog. **Black-Box-Phänomen**). Diese Besonderheit und daraus ggf. resultierende Unwägbarkeiten im Hinblick auf die durch die KI-Lösung zu erzeugenden Ergebnisse sollten im Vertrag reflektiert sein. Um Fehlinvestitionen zu vermeiden und Rechtsstreitigkeiten vorzubeugen, sollten beide Parteien im Zuge der Verhandlungen eine realistische Vorstellung von Möglichkeiten und Grenzen der KI-Lösung entwickeln und diese vertraglich verankern. Eine lückenlose, schlüssige, präzise und transparente Beschreibung von Eigenschaften und Funktionsweise der KI-Lösung ist geeignet, insoweit größtmögliche Rechtssicherheit zu schaffen. Diese sollte auch festlegen, welcher Grad an Präzision seitens der KI-Lösung erforderlich ist.[11] Ergänzend können Sie Produktpräsentationen des Dienstleisters im Vorfeld des Vertragsschlusses als Anlage zum Vertrag aufnehmen und so dessen werblichen Aussagen rechtsverbindlichen Charakter verleihen. Ab-

[10] BGH 01. Februar 2012, NJW 2012, 1718, Rn. 26.

[11] Das Kriterium der „Präzision" findet sich auch in den Leitlinien für Vertrauenswürdige KI (HEG-KI 2019, S. 35).

runden sollten Sie die Leistungsbeschreibung durch eine klare Festlegung der Leistungen, die „out-of-scope", d. h. nicht unter dem Vertrag geschuldet, sind.

Checkliste Vertragsgegenstand/Leistungsbeschreibung einer KI-Lösung

Ist die Funktionsweise der KI-Lösung lückenlos, schlüssig, präzise und transparent beschrieben?
Handelt es sich um sog. Black-Box Szenarien? Wenn ja, spiegelt sich dies in der Leistungsbeschreibung wieder?
Reflektiert die Leistungsbeschreibung das gemeinsame Verständnis der Parteien hinsichtlich Möglichkeiten und Grenzen der KI-Lösung?
Berührt die KI-Lösung ethische Aspekte? Wenn ja, trifft die Leistungsbeschreibung Aussagen dazu, wie ethischen Aspekten Rechnung getragen wird?
Ist beschrieben, welche Leistungsbestandteile „out-of-scope" sind bzw. was nicht von der KI-Lösung erwartet werden kann?

▶ **Praxistipps** Produktpräsentationen im Vorfeld ebenfalls als Anlage zum Vertrag aufnehmen!

Leitlinien für vertrauenswürdige KI der HEG-KI können Orientierung bei der Erstellung bzw. Prüfung der Leistungsbeschreibung bieten.

9.2.3 Definitionen

Die Definition und einheitliche Verwendung der für den Vertrag zentralen Begrifflichkeiten zählt zu den Standardanforderungen jeder Vertragsgestaltung (Thalhofer und Żdanowiecki 2019, § 19 Rn. 61; Lütcke und Bähr 2001, S. 84). Bei Verträgen über KI-Lösungen sollten Sie neben den üblicherweise aus juristischer Sicht erforderlichen Standarddefinitionen die wesentlichen Begrifflichkeiten in Zusammenhang mit der KI-Lösung aussagekräftig und präzise definieren. Dies ist essenziell, da KI-spezifische Begrifflichkeiten nicht gesetzlich definiert sind und aufgrund der Neuheit und ständiger Weiterentwicklung der Materie in den wenigsten Fällen existierende Rechtsprechung zur Auslegung bestimmter Begrifflichkeiten herangezogen werden kann.

9.2.4 Vereinbarung von Zielen, die durch den Einsatz der KI-Lösungen erreicht werden sollen

Sofern Sie durch den Einsatz der KI-Lösung bestimmte Ziele, wie beispielsweise einen bestimmten Grad an Prozessautomatisierung, Einsparungen o. ä. erreichen möchten, ist die Festlegung entsprechender Meilensteine bzw. Ziele im Vertrag empfehlenswert. Meilensteine sind definierte Zeitpunkte, zu denen bestimmte Arbeitsergebnisse vorliegen oder

definierte Ziele erreicht sein müssen (Pruß und Sarre 2019, Technisches Glossar). Soll die KI-Lösung beispielsweise einen bisher durch Menschen ausgeführten Prozess übernehmen, kann durch Meilensteine ausgedrückt werden, bis zu welchem Zeitpunkt die KI-Lösung einen bestimmten Prozentsatz der im Rahmen des Prozesses anfallenden Aufgaben ohne menschliches Zutun erledigen können muss. An die Nichterreichung der Meilensteine sollte der Vertrag Rechtsfolgen, wie Kündigungsmöglichkeiten und Vertragsstrafen bzw. Gutschriften knüpfen (Thalhofer und Żdanowiecki 2019, § 19 Rn. 181).

9.2.5 Verarbeitung von und Rechte an Daten

Da Daten den Rohstoff für die Nutzung einer KI-Lösung bilden, ist im Vertrag festzulegen, ob und in welchem Umfang die KI-Lösung personenbezogene Daten und/oder bereits existierende Maschinengenerierte Daten verarbeitet und/oder inwieweit die KI-Lösung selbst Daten erzeugt.[12] Da die DS-GVO nur für personenbezogene Daten gilt, sind in Bezug auf Maschinengenerierte Daten vertragliche Regelungen zu den technischen Gegebenheiten der Datenübertragung (beispielsweise in Bezug auf Verschlüsselung) zu treffen. Sofern zur Gewährleistung der korrekten Funktionsweise der KI-Lösung eine bestimmte Datenqualität erforderlich ist, sollte der Vertrag entsprechende Anforderungen an die Datenqualität festlegen und definieren, welche Partei für die Gewährleistung der Datenqualität und die Qualitätskontrolle verantwortlich ist.

Da das deutsche Recht kein Eigentum an Maschinengenerierten Daten kennt,[13] ist eine vertragliche Regelung der Rechte an Maschinengenerierten Daten sinnvoll (siehe hierzu Abschn. 9.1.2). Beispielsweise kann der Anbieter der KI-Lösung vertraglich dazu verpflichtet werden, die Maschinengenerierten Daten, auf die die KI-Lösung während des Betriebs Zugriff nimmt, nicht anderweitig zu nutzen. Freilich ist stets zu prüfen, ob dies im Einzelfall technisch möglich und wirtschaftlich sinnvoll ist. Sofern die KI-Lösung selbst Maschinengenerierte Daten erzeugt, kann aus Auftraggebersicht eine vertragliche Zuordnung auch solcher Daten zum Anwenderunternehmen wünschenswert sein, da das Anwenderunternehmen diese nach ihrem Inhalt und dem Bezug zu der bezogenen Leistung wirtschaftlich als „seine“ Daten betrachtet (Thalhofer und Żdanowiecki 2019, § 19 Rn. 99, bezogen auf Rechte an Daten beim Outsourcing). In wiederum anders gelagerten Fällen dürften kommerzielle und technische Erwägungen zu der Entscheidung führen, dass Anwenderunternehmen und Anbieter der KI-Lösung Nutzungsrechte an durch die KI-Lösung erzeugten Maschinengenerierten Daten erhalten. Anbieterseitig wird vielfach ein hohes Interesse an einer derartigen Lösung bestehen, da für die kontinuierliche Weiterentwicklung der KI-Lösungen große Mengen an Daten erforderlich sind.

[12] Zu den besonderen Anforderungen für die Verarbeitung personenbezogener Daten siehe Kap. 2.

[13] Siehe zum aktuellen Stand der Diskussion Kap. 5.

Checkliste zur Verarbeitung von und Rechten an Daten

Verarbeitet die KI-Lösung personenbezogene Daten und wenn ja, welche?
Verarbeitet die KI-Lösung bereits existierende Maschinengenerierte Daten?
Erzeugt die KI-Lösung selbst Maschinengenerierte Daten?
Welche Partei(en) sollen Rechte an Maschinengenerierten Daten erhalten?
Welche Anforderungen gelten hinsichtlich der Qualität der durch die KI-Lösung genutzten Daten?

9.2.6 Verantwortungsbereiche der Parteien

Um Rechtsstreitigkeiten vorzubeugen, sollten die Verantwortungsbereiche beider Parteien vertraglich klar voneinander abgegrenzt sein (Kötz 2018, S. 1; Thalhofer und Żdanowiecki 2019, § 19 Rn. 181). Ist das Anwenderunternehmen für die Bereitstellung der für die Nutzung der KI-Lösung erforderlichen Daten und das entsprechende Qualitätsmanagement verantwortlich, sollten Sie dies explizit im Vertrag festlegen. Aus Anbietersicht sind in derartig gelagerten Fällen Regelungen wünschenswert, die das Haftungsrisiko für Ansprüche Dritter wegen Verletzung ihrer Rechte aufgrund der durch die KI-Lösung verarbeiteten Maschinengenerierten Daten ausschließlich dem Anwenderunternehmen zuweisen. Anbieter können für den Fall, dass Dritte gegen sie diesbezügliche Ansprüche geltend machen, jedenfalls individualvertraglich einen Freistellungsanspruch gegen das Anwenderunternehmen vereinbaren.[14]

Zudem sollte vertraglich festgelegt werden, welche Partei die Kontrollverantwortung für die KI-Lösung und die durch diese getroffenen Entscheidungen trägt. Die von der EU eingesetzte HEG-KI nennt in den Leitlinien für vertrauenswürdige KI den Vorrang menschlichen Handelns und menschliche Kontrolle zu Recht als ein maßgebendes Kriterium für vertrauenswürdige KI (HEG-KI 2019, S. 32–33). Sofern die KI-Lösung Entscheidungen trifft, die Auswirkungen auf Menschen haben, sollte einer Partei die Verantwortung dafür zugewiesen werden, dass die KI-Lösung diskriminierungsfrei arbeitet.

9.2.7 Gewährleistungsrechte

Welche Gewährleistungsrechte dem Anwenderunternehmen bei Mängeln der KI-Lösung zustehen, richtet sich nach den vertraglichen und/oder gesetzlichen Regelungen. Welche gesetzlichen Regelungen gelten, hängt davon ab, welchem Vertragstypus die mangelbehaftete Leistung zuzuordnen ist. Sofern ein gemischt-typischer Vertrag mit Elementen mehrerer Vertragstypen vorliegt, richten sich (sofern keine vorrangigen vertraglichen Re-

[14] In allgemeinen Geschäftsbedingungen im Sinne der §§ 305 ff. BGB dürften derartige Freistellungsverpflichtungen demgegenüber häufig unwirksam sein.

gelungen getroffen wurden) die Rechte in Bezug auf die mangelbehaftete Leistung nach den gesetzlichen Regelungen des für den jeweiligen Leistungsteil einschlägigen Vertragstyps (Wicker 2012, S. 784). Zunächst gelten insoweit die allgemeinen, von Rechtsprechung und Literatur entwickelten Grundsätze. Demnach gilt für KI-Lösungen, für die eine Lizenzierung OnPremise[15] vorgesehen ist, grundsätzlich das kaufrechtliche Gewährleistungsregime, während Cloud-Lösungen häufig mietvertraglich (Wicker 2012, S. 785; Pohle und Ammann 2009, S. 275), gelegentlich aber auch dienstvertraglich (Strittmatter 2019, § 22 Rn. 36.) ausgestaltet sind. In IT-Verträgen vereinbaren die Parteien üblicherweise von den gesetzlichen Gewährleistungsrechten abweichende bzw. diese ergänzende, vertragliche Regelungen, um den IT-spezifischen Besonderheiten Rechnung zu tragen. Berücksichtigen Sie daher die KI-spezifischen Besonderheiten bei der Vereinbarung von Gewährleistungsrechten für eine KI-Lösung. KI-Lösungen unterscheiden sich von tradierten Softwarelösungen insbesondere dadurch, dass KI-Lösungen kontinuierlich „lernen". Oft wird sich erst während des „Trainings" der KI-Lösung zeigen, ob diese den Erwartungen des Anwenderunternehmens entspricht. Wie sich diese Besonderheit bei der Ausgestaltung von Gewährleistungsrechten auswirkt, hängt davon ab, ob das Lizenzmodell kaufrechtlich, werkvertraglich, dienstvertraglich und/oder mietrechtlich geprägt ist.

9.2.7.1 Kaufvertraglich ausgestaltete Gewährleistungsregelung

Bei einem kaufvertraglich ausgestalteten Lizenzmodell ist für die Frage, ob die KI-Lösung einen Sach- oder Rechtsmangel aufweist, der Zeitpunkt des Gefahrübergangs entscheidend. Nach allgemeinen Rechtsgrundsätzen erfolgt der Gefahrübergang, soweit nicht abweichend vereinbart, mit Übergabe. Für die Frage, ob ein Sach- oder Rechtsmangel vorliegt, ist dementsprechend maßgeblich, ob die KI-Lösung im Zeitpunkt des Gefahrübergangs mangelhaft ist. Gem. § 434 Abs. 1 Satz 1 BGB ist für die Frage, ob ein Sachmangel vorliegt, vorrangig entscheidend, ob die KI-Lösung bei Gefahrübergang die vereinbarte Beschaffenheit aufweist. Wurde keine Beschaffenheit vereinbart, ist gem. § 434 Abs. 1 Satz 2 BGB maßgeblich, ob sich die KI-Lösung für die nach dem Vertrag vorausgesetzte Verwendung eignet (§ 434 Abs. 1 Satz 2 Nr. 1 BGB) oder ob sie sich für die gewöhnliche Verwendung eignet und eine Beschaffenheit aufweist, die bei „Sachen"[16] der gleichen Art üblich ist und die der Käufer nach der Art der Sache erwarten kann (§ 434 Abs. 1 Satz 2 Nr. 2 BGB). Eine detaillierte Leistungsbeschreibung einschließlich der Festlegung des angestrebten Nutzungszwecks der KI-Lösung ist daher essenziell für die Geltendmachung von Gewährleistungsrechten.

Mit Gefahrübergang beginnt auch die Gewährleistungsfrist zu laufen. Aus Anwendersicht kann es daher vorteilhaft sein, den Beginn der Gewährleistungsfrist vertraglich hi-

[15] Bei einer Lizenzierung On-Premise wird die Software in eigener Verantwortung des Anwenderunternehmens auf einer bei diesem vorhandenen Hardware betrieben.

[16] Nach herrschender Meinung weist Software keine Sacheigenschaft im Sinne des § 90 BGB auf, da ihr „die für den Sachbegriff kennzeichnende abgrenzbare Körperlichkeit fehlt" (Stresemann 2018, § 90 Rn. 25). Gemäß § 453 BGB ist das Kaufrecht dennoch anwendbar.

nauszuschieben und beispielsweise an den (erfolgreichen) Abschluss eines zwischen den Parteien vereinbarten, ersten Trainingszeitraums der KI-Lösung zu knüpfen.

9.2.7.2 Mietvertraglich ausgestaltete Gewährleistungsregelung

Wird die KI-Lösung in einer Cloud bereitgestellt, wird der Vertrag häufig mietvertraglich ausgestaltet. Gem. § 535 Abs. 1 Satz 2 BGB hat der Anbieter die KI-Lösung in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu überlassen und sie während der Mietzeit in diesem Zustand zu erhalten. Gesetzliche Mängelrechte knüpfen daran an, ob die KI-Lösung zur Zeit der Überlassung oder während der Mietzeit einen Mangel hat, der ihre Tauglichkeit zum vertragsgemäßen Gebrauch aufhebt oder mindert. Auch bei mietvertraglich ausgestalteten Verträgen über KI-Lösungen kommt einer detaillierten Leistungsbeschreibung einschließlich der Festlegung des angestrebten Nutzungszwecks daher überragende Bedeutung für die Geltendmachung von Gewährleistungsrechten zu. Im Übrigen gelten bei Cloud-basierten KI-Lösungen die allgemeinen Grundsätze für die Gestaltung von Cloud-Verträgen.[17] Flankiert werden mietvertraglich ausgestaltete Gewährleistungsregelungen üblicherweise durch Service Level Vereinbarungen, nach welchen das Anwenderunternehmen bei Nichtverfügbarkeit der KI-Lösung Service Level Gutschriften erhält.

9.2.7.3 Werkvertraglich ausgestaltete Gewährleistungsregelung

Wird eine KI-Lösung individuell für das Anwenderunternehmen entwickelt, wird der Vertrag vielfach werkvertraglich ausgestaltet. Gem. § 633 Abs. 2 Satz 1 BGB ist für die Frage, ob ein Sachmangel vorliegt, vorrangig entscheidend, ob die KI-Lösung die vereinbarte Beschaffenheit aufweist. Wurde keine Beschaffenheit vereinbart, ist gem. § 633 Abs. 2 Satz 2 BGB maßgeblich, ob sich die KI-Lösung für die nach dem Vertrag vorausgesetzte Verwendung eignet (§ 633 Abs. 2 Satz 2 Nr. 1 BGB) oder ob sie sich für die gewöhnliche Verwendung eignet und eine Beschaffenheit aufweist, die bei Werken der gleichen Art üblich ist und die der Besteller nach der Art der Sache erwarten kann (§ 633 Abs. 2 Satz 2 Nr. 2 BGB). Eine detaillierte Leistungsbeschreibung einschließlich der Festlegung des angestrebten Nutzungszwecks der KI-Lösung ist daher auch bei werkvertraglicher Ausgestaltung essenziell für die Geltendmachung von Gewährleistungsrechten. Ähnlich wie im Kaufrecht kann es im Einzelfall aus Anwendersicht wünschenswert sein, dass die Gewährleistungsfrist erst nach Abschluss eines ersten „Trainingszeitraums" für die KI-Lösung beginnt. Anders als im Kaufrecht beginnt die Gewährleistungsfrist unter einem Werkvertrag ohnehin erst mit der Abnahme. Dem der Abnahme üblicherweise vorgeschalteten Abnahmetest (Witzel 2017 S. 216; Schmidt 2019b, § 1 Rn. 344–346) kann eine „Trainingsphase" der KI vorausgehen. Die Parteien können dann vereinbaren, dass der Auftraggeber die Abnahme erst dann erklärt, wenn die bereits entsprechend „trainierte" KI-Lösung die Abnahmekriterien erfüllt.

[17] Siehe zur Ausgestaltung von Cloud Verträgen beispielsweise Boehm 2016, S. 358–386; Conrad et al. 2019 C § 22.

9.2.8 IT-Sicherheit

Bei der Nutzung von KI sind technische Robustheit und Sicherheit insbesondere zur Gewährleistung der Einhaltung der Regelungen der DS-GVO und zum Schutz der oft weitreichenden Geheimhaltungsinteressen der Parteien von herausragender Bedeutung. Der Vertrag sollte daher (ggf. als Anlage) umfassende Regelungen in Bezug auf IT-Sicherheit enthalten. Insbesondere sind die durch den Anbieter zu treffenden Maßnahmen zum Schutz gegen Angriffe auf die KI-Lösung zu beschreiben. Für den Fall der Nichteinhaltung der vertraglichen Regelungen zur IT-Sicherheit kann sich das Anwenderunternehmen ein Sonderkündigungsrecht mit sofortiger Wirkung einräumen lassen. Aus Sicht der Anwenderunternehmen ist es zudem vorteilhaft, für den Fall, dass Dritte wegen Vorfällen in Bezug auf die durch den Anbieter zu gewährleistende IT-Sicherheit Ansprüche gegen das Anwenderunternehmen geltend machen, zumindest individualvertraglich einen Freistellungsanspruch gegen den Anbieter zu vereinbaren.

9.2.9 Lizenzmetriken

Beide Parteien haben gleichermaßen großes Interesse an der Wahl einer geeigneten Lizenzmetrik, gibt doch letztlich die Lizenzmetrik vor, in welchem Umfang das Anwenderunternehmen zur Nutzung der KI-Lösung berechtigt ist und welche Vergütung hierfür zu entrichten ist. Bei der Lizenzierung von KI-Lösungen kann dabei auf bekannte Lizenzmetriken aus dem Bereich der Softwarelizenzierung zurückgegriffen werden, freilich unter Beachtung der Besonderheiten der KI-Lösung. Anbieter und Anwenderunternehmen werden dabei regelmäßig eigene Interessen verfolgen, welche bei der Wahl des Lizenzmodells Berücksichtigung finden sollten.

Den gesetzlich zwingenden Rahmen einer jeden Lizenzmetrik bilden §§ 69 c, 69 d UrhG. Gem. § 69 c Nr. 1 UrhG hat der Rechtsinhaber das ausschließliche Recht, die dauerhafte oder vorübergehende Vervielfältigung eines Computerprogramms mit jedem Mittel und in jeder Form zu gestatten. Dies gilt auch, soweit das Laden, Anzeigen, Ablaufen, Übertragen oder Speichern des Computerprogramms eine Vervielfältigung erfordert. Im Umkehrschluss bedeutet das, dass grundsätzlich jede urheberrechtlich relevante Handlung, die der Rechtsinhaber nicht ausdrücklich gestattet hat, unzulässig ist. § 69 d UrhG regelt jedoch Ausnahmen von an sich zustimmungsbedürftigen Handlungen. Relevant ist insoweit insbesondere § 69 d Abs. 1 UrhG, wonach die in § 69 c Nr. 1 und Nr. 2 UrhG genannten Handlungen, soweit keine besonderen vertraglichen Bestimmungen vorliegen, nicht der Zustimmung des Rechtsinhabers bedürfen, wenn sie für eine bestimmungsgemäße Benutzung des Computerprogramms einschließlich der Fehlerberichtigung durch jeden zur Verwendung eines Vervielfältigungsstücks des Programms Berechtigten notwendig sind. Nach überwiegender Auffassung begründet § 69 d Abs. 1 UrhG einen zwingenden Kernbereich bestimmungsgemäßer Nutzung, der auch durch besondere

vertragliche Bestimmungen nicht wirksam abbedungen werden kann[18] (Metzger und Hoppen 2017, S. 629; Grützmacher 2019, § 69 d Rn. 40–49). Gerade weil mit Ausnahme der in § 69 d UrhG geregelten Ausnahmefälle jegliche urheberrechtlich relevanten Nutzungshandlungen nur mit ausdrücklicher Zustimmung des Rechtsinhabers zulässig sind, ist eine transparente Lizenzmetrik, die klar und verständlich Reichweite und Grenzen der Nutzungsberechtigung aufzeigt, für Anwenderunternehmen essenziell. Dies gilt umso mehr, als bei einer (auch unwissentlichen) Überschreitung der Lizenzrechte teils hohe Nachforderungen der Lizenzgeber auf Vergütung der zusätzlichen Nutzung drohen.

Welche Lizenzmetrik kommerziell attraktiv ist, hängt von den Funktionalitäten der KI-Lösung sowie der angestrebten Nutzungsweise ab. Während früher Verarbeitungsprozesse in Software typischerweise durch menschliche User veranlasst wurden, tauschen im Zuge der Digitalisierung KI-Lösungen und andere Software vielfach ohne unmittelbare Interaktion menschlicher User Daten aus. Dies resultiert in neuen Lizenzmodellen, die nicht mehr an eine urheberrechtlich relevante Nutzungshandlung der Software durch einen menschlichen User anknüpfen.

Beim Thema Lizenzmetriken sind die Interessen des Anbieters der KI-Lösung und des Anwenderunternehmens naturgemäß oft unterschiedlich. Aus Sicht des Anbieters der KI-Lösung gilt es, Lizenzmetriken zu wählen, die das geistige Eigentum des Anbieters schützen und zugleich dessen wirtschaftlichen Wert optimal ausschöpfen. Die Wahl des richtigen Lizenzmodells ist daher eine wichtige unternehmerische Entscheidung. Anwenderunternehmen legen demgegenüber insbesondere Wert auf Transparenz hinsichtlich Reichweite und Grenzen der Nutzungsrechte sowie eine gute Kalkulierbarkeit der Lizenzgebühren. Zudem sollten Sie bedenken, ob neben den aktuellen Nutzungsarten der KI-Lösung bereits jetzt neue Arten der Nutzung, welche Sie in Zukunft benötigen, absehbar sind und ggf. vertraglich vereinbaren, dass die eingeräumten Nutzungsrechte auch für zukünftige Nutzungsarten gelten.

Im Folgenden erhalten Sie ausgehend von der früher weit verbreiteten Named User Lizenz einen Überblick über unterschiedliche Arten von Lizenzmetriken, die für die Lizenzierung von KI-Lösungen verwendet werden. Da diese Lizenzmetriken jedoch nicht gesetzlich definiert sind, sind letztlich immer die Formulierungen in den jeweiligen Lizenzbedingungen maßgeblich.

9.2.9.1 Named User Lizenz

Wird eine KI-Lösung auf Basis der sog. Named User Lizenz lizenziert, so ist für jeden Nutzer der KI-Lösung eine gesonderte Lizenz erforderlich. Achten Sie bei Bezug einer Named User Lizenz darauf, ob der Begriff Named User in den Lizenzbedingungen definiert ist und ob demnach nur für menschliche Nutzer eine Lizenz bezogen werden muss oder ob auch für softwaregestützte Maschinen bzw. andere KI-Lösungen, mit denen die lizenzierte KI-Lösung Daten austauscht, eine Lizenz erforderlich ist. Bei Chatbots oder

[18] BGH 17. Juli 2013, GRUR 2014, 264, Rn. 33 und 66–68; BGH 24. Februar 2000, GRUR 2000, 866 (868).

Companion Robots ist wegen der Interaktion menschlicher Nutzer mit dem jeweiligen Chatbot oder Companion Robot eine Lizenzierung auf Basis von Named User Lizenzen durchaus denkbar. Hingegen dürfte dieser Lizenzmetrik im Bereich der KI-basierten Steuerung und Überwachung von Produktionsabläufen (z. B. Predictive Maintenance oder Predictive Analytics) geringere Bedeutung zukommen, da hier typischerweise Datenaustausch zwischen der jeweiligen KI-Lösung und anderer Software stattfindet.

Eine Variante der Named User Lizenz ist die sog. Concurrent User Lizenz, bei der eine vordefinierte Anzahl an Usern lizenziert wird, die die KI-Lösung gleichzeitig nutzen. Dieses Lizenzmodell ist dann attraktiv, wenn beispielsweise im Rahmen eines Schichtbetriebs eine begrenzte Anzahl von Usern gleichzeitig auf die KI-Lösung zugreift.

9.2.9.2 Ergebnisorientierte Lizenzmetrik

Wird die zu entrichtende Lizenzgebühr ergebnisorientiert berechnet, knüpft die Lizenzmetrik an ein bestimmtes Ergebnis, welches durch die KI-Lösung erzeugt wird, an. Denkbar ist beispielsweise eine Vergütungspflicht für jedes durch die KI-Lösung erstellte Dokument oder für jeden ohne menschliche Interaktion durch die KI-Lösung bewältigten Prozess, z. B. für die Lösung eines Problems. Ergebnisorientierte Lizenzmetriken erfreuen sich bei Softwareanbietern zunehmender Beliebtheit, da die Lizenzgebühr unabhängig davon anfällt, ob das Ergebnis das Resultat einer Interaktion zwischen einem Menschen und der KI-Lösung ist oder ob Datenaustausch zwischen der KI-Lösung und anderer Software stattfindet. Vorteil der ergebnisorientierten Lizenzmetriken ist, dass die Vergütungspflicht an einen festgelegten Nutzungstatbestand (z. B. Dokumenterstellung o. ä.) geknüpft ist, was grundsätzlich im Sinne der Transparenz ist. Achten Sie jedoch darauf, ob dieser Tatbestand aus technischer und rechtlicher Sicht klar und eindeutig beschrieben ist. Bei intensiver Nutzung der KI-Lösung können ergebnisorientierte Lizenzmetriken jedoch kommerziell nachteilig sein, da eine häufige Nutzung mit entsprechend hohen Lizenzgebühren einhergeht. In diesem Fall kann es lohnend sein, eine maximale Obergrenze von durch die KI-Lösung erzeugten Ergebnissen zu vereinbaren, nach deren Erreichen weitere, durch die KI-Lösung erzeugte Ergebnisse vergütungsfrei sind oder eine ermäßigte Lizenzgebühr auslösen.

9.2.9.3 Zeitabhängige Lizenzmetrik

Bei zeitabhängigen Lizenzmetriken gestattet der Anbieter die Nutzung der KI-Lösung für einen bestimmten Zeitraum gegen Zahlung einer beispielsweise monatlich oder jährlich zu entrichtenden Subskriptionsgebühr. Gerade bei Cloud-basierten Lösungen finden sich häufig derartige Subskriptionsmodelle. Vorteilhaft ist die gute Kalkulierbarkeit der für die Nutzung entstehenden Kosten. Zudem ist das Risiko von Nachforderungen wegen Nutzungsüberschreitung geringer, da die Lizenzgebühr an einen Zeitabschnitt und nicht an die konkrete Nutzungsintensität der KI-Lösung anknüpft. Jedoch gibt es auch Lizenzmetriken, bei denen die Lizenzmetrik zeitabhängig und ergebnisorientiert ausgestaltet ist. Dies ist beispielsweise dann der Fall, wenn gegen Zahlung einer monatlichen Vergütung die Abwicklung einer maximalen Anzahl von Transaktionen durch die KI-Lösung geschuldet

ist. In diesen Fällen sollten die Parteien eine ausdrückliche Vereinbarung darüber treffen, wie das Monitoring der Einhaltung der Anzahl inkludierter Transaktionen erfolgt und welche Gebühren für darüber hinausgehende Transaktionen anfallen. Für Anwenderunternehmen ist in diesen Fällen eine vertragliche Regelung, die den Anbieter zur regelmäßigen Information über den Stand der bereits erzeugten Ergebnisse (z. B. der abgewickelten Transaktionen) verpflichtet, empfehlenswert. In der Praxis legen die Lizenzbedingungen jedoch häufig zunächst alleine dem Anwenderunternehmen die Pflicht zur Überwachung der Einhaltung der Nutzungsbeschränkungen auf. Sollte die Überwachung der Einhaltung der Nutzungsbeschränkungen aus technischer Sicht schwierig oder gar unmöglich sein, sollten Sie mit dem Anbieter der KI-Lösung individualvertraglich eine kontinuierliche Überwachungs- und zeitnahe Informationspflicht des Anbieters für den Fall der Überschreitung des gegen Zahlung der Subskriptionsgebühr inkludierten Nutzungsvolumens vereinbaren.

9.2.9.4 Umsatzbasierte Lizenzmetrik

Umsatzbasierte Lizenzmetriken knüpfen nicht an eine konkrete Nutzung der Software, sondern davon losgelöst an den Umsatz des Anwenderunternehmens an. Vorteil umsatzbasierter Lizenzmetriken ist, dass die für die Nutzung der KI-Lösung entstehenden Kosten gut kalkulierbar sind. Zudem besteht bei Vereinbarung umsatzbasierter Lizenzmetriken ein geringeres Risiko von Nachforderungen wegen unberechtigter Nutzung der KI-Lösung für eigene Unternehmenszwecke. Umsatzbasierte Lizenzmetriken werden jedoch von Softwareanbietern lediglich zurückhaltend und wenn überhaupt für Unternehmen mit entsprechend hohen Umsätzen und guter Wachstumsprognose angeboten.

Literatur

Arning M (2018) In: Moos F (Hrsg) Datenschutz- und Datennutzungsverträge, Teil 3 Datennutzungsverträge, § 15 Datenlieferungsvertrag, 2. Aufl. Otto Schmidt, Köln, S 2018

Boehm F (2016) Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten. ZEuP 2016:358–387

Conrad I, Witzel M (2019) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, Teil C. Software-, Hardware- und Providerverträge, § 18 IT-Projektmanagement, 3. Aufl. C.H. Beck, München

Conrad I, Licht S, Redeker H, Strittmatter M (2019) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, Teil C. Software-, Hardware- und Providerverträge, § 22 Cloud Computing, 3. Aufl. C.H. Beck, München

Grützmacher M (2019) In: Wandtke A-A, Bullinger W (Hrsg) Praxiskommentar Urheberrecht, Gesetz über Urheberrecht und verwandte Schutzrechte (Urgeberrechtsgesetz), Teil 1 Urheberrecht, § 69d Ausnahmen von den zustimmungsbedürftigen Handlungen, 5. Aufl. C.H. Beck, München

Hackenberg W (2019) In: Hoeren T, Sieber U, Holznagel B (Hrsg) Handbuch Multimedia-Recht, Teil 16 Datenschutz und Datensicherheit, 50. Ergänzungslieferung 2019. C.H. Beck, München

HEG-KI (2019) Ethik-Leitlinien für eine vertrauenswürdige KI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Zugegriffen am 17.01.2020

Kirchner G (2018) Big Data Management: Die Haftung des Big-Data-Anwenders für Datenfehler (Vertragsrecht – Teil 1). InTeR 2018:19–24

Kötz H (2018) Risikoverteilung im Vertragsrecht. JuS 2018:1–10
Kraus M (2015) Datenlizenzverträge. DSRITB 2015:537–551
Lütcke J, Bähr M (2001) Outsourcing-Verträge und Service Level Agreements in der IT-Branche – Gestaltungsvarianten für die Praxis. K&R 2001:82–87
Metzger A, Hoppen P (2017) Zur Zulässigkeit von Nutzungsbeschränkungen in Lizenzverträgen bei Verwendung von Drittanbietersoftware. CR 2017:625–639
Pohle J, Ammann T (2009) Über den Wolken… – Chancen und Risiken des Cloud Computing. CR 2009:273–278
Pruß M, Sarre F (2019) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, Technisches Glossar, 3. Aufl. C.H. Beck, München
Riehm T (2019) Rechte an Daten – Perspektive des Haftungsrechts. VersR 2019:714–724
Schefzig J (2015) Die Datenlizenz. DSRITB 2015:551–567
Schmidt M (2019a) In: Redeker H (Hrsg) Handbuch der IT-Verträge Band 3, Teil 6 Zusammenarbeit verschiedener Unternehmen oder Berater, Teil 6.1. Projektvertrag, 39. Lieferung 2019. Otto Schmidt, Köln
Schmidt M (2019b) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, Teil A. Technische und organisatorische Grundlagen, § 1 Erstellung und Pflege von Software, 3. Aufl. C.H. Beck, München
Stresemann C (2018) In: Säcker FJ, Rixecker R, Oetker H, Limperg B (Hrsg) Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd 1, Buch 1 Allgemeiner Teil, § 90 Begriff der Sache, 8. Aufl. C.H. Beck, München
Strittmatter M (2019) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, Teil C. Software-, Hardware- und Providerverträge, § 22 Cloud Computing, 3. Aufl. C.H. Beck, München
Thalhofer T, Żdanowiecki K (2019) In: Auer-Reinsdorff A, Conrad I (Hrsg) Handbuch IT- und Datenschutzrecht, Teil C. Software-, Hardware- und Providerverträge, § 19 Outsourcing-Verträge, 3. Aufl. C.H. Beck, München
Wicker M (2012) Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln. MMR 2012:783–788
Wilhelmi R (2019) In: Gsell B, Krüger W, Lorenz S, Reymann C (Gesamt Hrsg) beck-online. GROSSKOMMENTAR BGB, Buch 2 Recht der Schuldverhältnisse, § 453, Stand: 1. Oktober 2019. C.H. Beck, München
Witzel M (2017) Abnahme, Projektbeendigung und Schadensersatz. CR 2017:213–219

Ausblick: Vorhaben und Handlungsfelder der EU mit Bezug zu KI

10

Sabine von Oelffen

Zusammenfassung

Die EU-Kommission hat erkannt, dass KI-Technologien der Förderung bedürfen, um die EU als Wirtschaftsraum zukunftsfähig zu machen und zu erhalten. Die vielschichtigen Initiativen sind zum einen finanzieller Natur, zum anderen setzen sie sich zusammen aus Expertenberichten, Themenpapieren, Investitionsempfehlungen und Verfahren der öffentlichen Beteiligung. In diesem Kapitel wird ein Überblick über die einzelnen Veröffentlichungen und wirtschaftlichen Förderprogramme gegeben. Zwar zeichnet sich eine Zusammenfassung der Förderprogramme und Initiativen unter einzelne Dach programme wie bspw. Horizon Europe ab. Die Initiativen der EU bleiben jedoch breit gefächert und gehen das Thema KI auf vielen Ebenen und in differenzierter Weise an.

Die EU befasst sich in den letzten Jahren intensiv und im Rahmen unterschiedlichster Initiativen mit dem Themenfeld KI. Eine wichtige Säule der EU-Initiativen im Bereich KI bilden Fördergelder für KI-Projekte. Beispielsweise stehen seit Juli 2019 35 Millionen Euro für Prävention, Vorhersage und Behandlung der häufigsten Krebsarten mithilfe von KI-Lösungen für diagnostische Bildanalysen zum Abruf bereit (Europäische Kommission 2019a). Ebenfalls seit Juli 2019 abrufbar sind 50 Millionen Euro für den Aufbau eines dynamischen europäischen Netzwerks von Exzellenzzentren für KI (Europäische Kommission 2019b). Die Fördermaßnahme dient der Verbesserung der Zusammenarbeit innerhalb der europäischen Forschungsgemeinschaft für künstliche Intelligenz und der

S. von Oelffen (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: sabine.vonoelffen@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_10

Verbesserung des technologischen Fortschritts im Bereich KI (Europäische Kommission 2019b). Weitere 20 Millionen Euro investiert die EU in AI4EU, eine europäische Online-Plattform für den Austausch von KI-Tools und –Ressourcen (Project AI4EU o. J.). Neben monetär geprägten Initiativen zur Förderung von KI stehen zahlreiche Initiativen, die auf die Evaluierung und Schaffung eines Rechtsrahmens für KI ausgerichtet sind. Im Folgenden erhalten Sie einen Überblick über zentrale monetäre und rechtlich geprägte Initiativen der EU, die auf die stetige (Fort-)Entwicklung einer EU-weiten KI-Strategie abzielen. Die Fülle der Initiativen und rechtlichen Regelungen auf EU-Ebene mit Bezug zu KI lässt sich dabei unterteilen in solche Initiativen und Regelungen, deren Kernelement KI ist Abschn. 10.1 und solche, die zwar nicht KI-spezifisch sind, jedoch aufgrund ihres Inhalts große Bedeutung für die Entwicklung, Vermarktung und Nutzung von KI-Lösungen entfalten Abschn. 10.2.

10.1 KI-spezifische Initiativen

Thematisch zielen die aktuellen Initiativen der EU auf die Bildung einer einheitlichen, EU-weiten Strategie in Bezug auf KI, die Bildung von Kooperationen und die Förderung von KI-Projekten in den Mitgliedstaaten ab. Zudem evaluiert die EU aktuell, inwieweit ein europäischer Rechtsrahmen speziell für KI erforderlich ist. Konkrete Richtlinien- und Verordnungsvorschläge existieren derzeit jedoch noch nicht. Während einige der Initiativen Absichtserklärungen für Maßnahmen darstellen, die die EU in Bezug auf KI ergreifen möchte, befassen sich andere Initiativen mit inhaltlichen Einzelaspekten der Entwicklung und Nutzung von KI. Letztere berühren dabei durchaus eine Vielzahl rechtlicher Themen. Einen verbindlichen Rechtsrahmen schaffen diese Initiativen für sich genommen jedoch nicht, da sie keinen legislativen Charakter in Form einer EU-Richtlinie oder EU-Verordnung haben. Im Folgenden erhalten Sie einen Überblick über KI-spezifische Initiativen in Form von grundlegenden Absichtserklärungen und inhaltlich geprägten Initiativen für praktische Maßnahmen.

10.1.1 Allgemeine Maßnahmenplanung der EU mit Bezug zu KI

10.1.1.1 Erklärung über die Kooperation in Bezug auf KI

Anlässlich des „Digital Days 2018“ am 10. April 2018 unterzeichneten die Mitgliedstaaten eine Erklärung über eine Kooperation in Bezug auf KI (**Kooperationserklärung**). In dieser vereinbarten die Mitgliedstaaten insbesondere, die Entwicklung von KI in der EU voranzutreiben, besseren Zugang zu Daten des öffentlichen Sektors zu gewähren, mit KI in Zusammenhang stehende sozio-ökonomische Herausforderungen zu meistern und einen rechtlichen und ethischen Rahmen für KI zu schaffen (Mitgliedstaaten 2018, S. 1). Im Fokus der Kooperation stehen dabei insbesondere monetäre Investitionen in KI-spezifische Forschung und Entwicklung, die Förderung und Nutzung von KI im öffentlichen Sektor sowie die Förderung von Zukunftsfähigkeit und Vertrauenswürdigkeit von KI (Mitgliedstaaten 2018, S. 2). Bereits an dieser Stelle betonen die Mitgliedstaaten, dass der Mensch

die letztinstanzliche Kontrolle über KI ausüben muss (Mitgliedstaaten 2018, S. 3). Alle in dieser Kooperationserklärung enthaltenen Themen finden sich in zahlreichen, zeitlich späteren EU-Initiativen wieder und werden dort weiter konkretisiert.

10.1.1.2 Koordinierter Plan für KI

Als Folgemaßnahme zu der Kooperationserklärung der Mitgliedstaaten und der am 25. April 2018 Seitens der Kommission veröffentlichten Strategie für KI (**Strategie für Künstliche Intelligenz**) (Europäische Kommission 2018a) legte die Kommission am 7. Dezember 2018 einen gemeinsam mit den Mitgliedstaaten ausgearbeiteten koordinierten Plan für KI (**Koordinierter Plan für KI**) vor (Europäische Kommission 2018b). Der Koordinierte Plan für KI zielt darauf ab, eine größtmögliche Wirkung der Investitionen zu erreichen, Synergien, Austausch und eine intensive Zusammenarbeit im Bereich der KI zu fördern und das weitere Vorgehen gemeinsam abzustimmen (Europäische Kommission 2018b, S. 2). Hierzu stellt der Koordinierte Plan für KI einen Maßnahmenkatalog auf, welcher Strategien für eine effektive Zusammenarbeit mit den Mitgliedstaaten und eine Maximierung der Investitionen aufsetzt, Maßnahmen zum Ausbau von Spitzenforschung und digitalen Innovationszentren enthält und Berufsbildung im Bereich KI fördert (Europäische Kommission 2018b, S. 4 ff.). Zudem betont die Europäische Kommission die Wichtigkeit der Schaffung eines gemeinsamen europäischen Datenraums für die Förderung von KI, wobei sie der Bereitstellung von Daten und KI für Bereiche von öffentlichem Interesse besondere Bedeutung beimisst (Europäische Kommission 2018b, S. 15 ff.). Des Weiteren weist die Kommission darauf hin, dass integrierte Ethik und ein angemessener regulatorischer Rahmen für die Akzeptanz von KI bei Verbrauchern, aber auch für die Herstellung der Seitens der Unternehmen benötigten Investitionssicherheit von entscheidender Bedeutung sind (Europäische Kommission 2018b, S. 20 ff.). Der Koordinierte Plan für KI schließt mit einem Maßnahmenpaket in Bezug auf KI für den öffentlichen Sektor ab (Europäische Kommission 2018b, S. 22 ff.).

10.1.1.3 Artificial Intelligence – A European Perspective

2018 veröffentlichte die Kommission einen umfassenden Bericht mit dem Titel „Artificial Intelligence – A European Perspective“ (Craglia et al. 2018), welcher die europäische Sichtweise in Bezug auf KI darstellt. Grundlage des Berichts sind Forschungs- und Analyseergebnisse der **Gemeinsamen Forschungsstelle der Europäischen Kommission** (**GFS**).[1] Der Bericht ist in zwei Teile unterteilt. Der erste Teil führt den Leser hinsichtlich des zeitlichen Kontexts und aktuellen Entwicklungen in die Thematik „KI“ ein. Sodann wird aufgezeigt, wie die EU im Bereich „KI“ in der globalen Wettbewerbslandschaft aufgestellt ist. Teil 1 schließt mit einer Darstellung der KI-Entwicklung in den USA und China. In Teil 2 wird KI aus verschiedensten Blickwinkeln beleuchtet, darunter aus recht-

[1] **GFS** – Bei der Gemeinsamen Forschungsstelle der Europäischen Kommission handelt es sich um eine Generaldirektion der Europäischen Kommission. Als wissenschaftlicher Dienst der Europäischen Kommission unterstützt sie die Europäische Kommission mit technischen und wissenschaftlichen Dienstleistungen.

licher, ökonomischer sowie ethischer und sozialer Perspektive. Auch Fragen der Cybersicherheit sowie Fragen der Bedeutung von Daten für KI werden behandelt.

In Anbetracht der starken internationalen Konkurrenz möchte die EU die Chancen und das Potenzial, welches KI mit sich bringt, nicht ungenutzt verstreichen lassen. Die Kommission sieht USA und China derzeit an der Spitze der KI-Entwicklung. Bis 2030 soll jedoch China die aus Sicht der Kommission momentan führenden USA im Bereich der KI überholt haben (Craglia et al. 2018, S. 31). Aus ethischer und sozialer Sicht sind die im Bericht beleuchteten Fragen in Bezug auf die Auswirkungen von KI auf einzelne Personen oder Personengruppen interessant. Freilich spielen dabei auch Fragen des Datenschutzes eine wichtige Rolle (Craglia et al. 2018, S. 55–62). Aber auch technische Fragen werden beleuchtet. So wird unter anderem der erhebliche Stromverbrauch in Bezug auf den stetig steigenden Verarbeitungs- und Speicherbedarf der digitalen Wirtschaft behandelt (Craglia et al. 2018, S. 95–102). Aus ökonomischer Sicht werden die potenziellen Auswirkungen von KI auf Arbeitsplätze, insbesondere das Thema des Verlustes von Arbeitsplätzen und Einkommensungleichheiten diskutiert. Aber auch die Vorteile, die KI auf das Produktionswachstum haben kann, werden aufgegriffen (Craglia et al. 2018, S. 77 bis 86). Hinsichtlich der rechtlichen Implikationen von KI werden Fragen bezüglich der Vereinbarkeit von KI mit europäischem Recht sowie Eigentum an Daten, Zugang zu diesen und Teilen derselben dargestellt (Craglia et al. 2018, S. 63–70).

Etliche der in dem Bericht aus 2018 angesprochenen Aufgabenstellungen in Bezug auf KI wurden in den Folgejahren bereits weiter ausgearbeitet. So wird die Absicht, die Entwicklung von KI zu fördern, auch in Erwägungsgrund 3 der **Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors** (**Richtlinie 2019/1024/EU**) explizit geäußert. Ferner dürfte die **Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU** (**Verordnung 2018/1807/EU**) ein Weg in die richtige Richtung sein, um die Verfügbarkeit von Daten grenzübergreifend zu ermöglichen. Auch dem Schutz des Verbrauchers im „digitalen Zeitalter" wurde mit der **Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen** (**Richtlinie 2019/770/EU**) ein rechtlicher Rahmen gesetzt.[2]

10.1.2 Themenpapiere und Schwerpunktinitiativen der EU zum Thema KI

Insbesondere seit 2017 wurden Seitens der EU zahlreiche Initiativen ins Leben gerufen, die einzelne Aspekte der Entwicklung und Nutzung von KI in der EU beleuchten, Handlungsbedarf ausloten und Maßnahmenpakete vorschlagen. Der inhaltliche Schwerpunkt der Initiativen liegt auf ethischen Themen, Rechts- und Haftungsfragen, Forschung und Investitionen.

[2] Richtlinie 2019/770/EU.

10.1.2.1 Entschließung zu zivilrechtlichen Regelungen im Bereich Robotik

Das Europäische Parlament hat am 16. Februar 2017 eine Entschließung mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (**Entschließung Zivilrechtliche Regelungen im Bereich Robotik**) abgegeben (Europäische Parlament 2017). In seiner Entschließung Zivilrechtliche Regelungen im Bereich Robotik fordert das Europäische Parlament insbesondere die Einführung eines EU-weiten Registrierungssystems für Roboter (Europäische Parlament 2017, Rz. 2). Inhaltlich evaluiert das Europäische Parlament Handlungsbedarf hinsichtlich des Einsatzes von autonomen Verkehrsmitteln (autonome Fahrzeuge und Drohnen) (Europäische Parlament 2017, Rz. 24 ff.), Pflegerobotern (Europäische Parlament 2017, Rz. 31 ff.), medizinischen Robotern (Europäische Parlament 2017, Rz. 31 ff., 33 ff.) und hinsichtlich des Einsatzes von Robotik in Zusammenhang mit geschädigten Organen des Menschen (Europäische Parlament 2017, Rz. 36 ff.). Das Europäische Parlament sieht keine Notwendigkeit spezieller Schutzrechte des geistigen Eigentums für den Bereich Robotik; vielmehr sieht es einen horizontalen, branchenübergreifenden Ansatz zum Schutz des geistigen Eigentums für die Bereiche, in denen Robotik zum Einsatz kommen könnte, als vorzugswürdig an (Europäische Parlament 2017, Rz. 18).

10.1.2.2 Initiativen der gemeinsamen Forschungsstelle der Europäischen Kommission

Die GFS befasst sich in den letzten Jahren intensiv mit dem Einfluss von KI auf die verschiedensten Sektoren. Die folgende Auflistung gibt einen Überblick über zentrale Initiativen und Ergebnisse der GFS in Bezug auf KI:

10.1.2.2.1 Bedarfsfeststellung in Bezug auf KI

Am 23. Mai 2018 führte die GFS mit einem ersten, internen Workshop eine Bedarfsfeststellung in Bezug auf KI durch. Ziel dieses Workshops war der Austausch zwischen den Spezialisten der Forschungsstelle, um die derzeitigen wissenschaftlichen Anwendungsbereiche von KI sowie Möglichkeiten für die Erfüllung der Anforderungen der Europäischen Kommission an KI zu ermitteln und die Zusammenarbeit der Arbeitsgruppen innerhalb der gemeinsamen Forschungsstelle zu verbessern (Nativi and Gómez Losada 2019, S. 6). Die Ergebnisse dieses Workshops sind in dem Bericht „Künstliche Intelligenz bei der GFS“ (Nativi and Gómez Losada 2019) einzusehen. Die Experten betonten, dass KI den Fragen zur Untrennbarkeit von Ethik und Recht eine neue Dimension verleihe und dass üblicherweise der Grad der Möglichkeiten und der Automatisierung von KI unterschätzt werde (Nativi and Gómez Losada 2019, S. 35). Ein Blick auf die anderen Initiativen der EU, beispielsweise auf die KI-Ethikleitlinien und auf die Politik- und Investitionsempfehlungen zeigt in der Tat, dass den Themenbereichen „Ethik“ und „Recht“ sowie einer Verzahnung derselben in den nächsten Jahren überragende Bedeutung zukommen dürfte.

10.1.2.2.2 Lernen, Lehre, Bildung

Die Untersuchung des Einflusses von KI auf den Bildungssektor stellt einen weiteren Forschungsschwerpunkt der GFS dar. Die GFS veröffentlichte 2018 einen Bericht über den Einfluss von KI auf Lernen, Lehre und Bildung (Tuomi 2018). Zweck dieses Berichts ist, Pädagogen und politischen Entscheidungsträgern die technische Entwicklung von KI näher zu bringen (Tuomi 2018, S. 3). Dabei wird vor allem auf die Chancen für den Bildungssektor hingewiesen. So könnten durch den Einsatz von KI völlig neue Wege des Lernens und Lehrens entstehen (Tuomi 2018, S. 2). Dafür sei jedoch eine breite Zugriffsmöglichkeit auf große Datensätze für die Entwicklung dieser KI-Systeme notwendig (Tuomi 2018, S. 36). Gleichzeitig wird auch vor ethischen und rechtlichen Problemen gewarnt, die besonders im Bildungssektor relevant seien (Tuomi 2018, S. 36). Dies gelte zum Beispiel für das Kontrollieren von Schülerinnen und Schülern durch intelligente Videoverarbeitung oder bezüglich der Gefahr, dass KI, wenn diese im Rahmen der Bewertung von Leistungen eingesetzt wird, verzerrte und unausgewogene Ergebnisse produziert (Tuomi 2018, S. 4).

10.1.2.2.3 Autonomes Fahren, M-Health, Text und Datamining

Außerdem analysierte die GFS 2019 in Zusammenarbeit mit dem Europäischen Institut für Innovation und Technologie im Rahmen eines Forschungsprojekts die rechtlichen Implikationen von KI. Der Fokus lag dabei auf drei verschiedenen Sektoren: Autonomem Fahren, M-Health[3] und Text- und Data Mining. Dazu veranstaltete die GFS einen Workshop, der in einem Bericht zusammengefasst und veröffentlicht wurde (Holder et al. 2019). Ziel dieses Projekts war, bestehende Initiativen zu ermitteln sowie Aufmerksamkeit herzustellen für rechtliche Herausforderungen, die sich der Gesellschaft und insbesondere auch Start-Up-Unternehmen[4] bei dem Einsatz dieser Technologien stellen. Im Zentrum des Interesses standen Herausforderungen im Bereich Haftung und Versicherungen (Holder et al. 2019, S. 15), Datenschutz, vor allem im Konflikt mit dem sozio-ökonomischen Nutzen von Daten (Holder et al. 2019, S. 15) sowie gewerbliche Schutzrechte (Holder et al. 2019, S. 15, 22, 28). Das Fazit der Analyse lautete, dass die derzeitige Rechts- und Gesetzeslage von dem technischen Fortschritt überholt wurde und nun sektorbezogen analysiert und bearbeitet werden müsse. Um bei der Gesetzgebung Innovationen zu fördern und zu unterstützen, wird eine Zusammenarbeit mit Industrie-Experten angestrebt (Holder et al. 2019, S. 33). Die Ergebnisse des Berichts der GFS sind jedoch weder verbindlich noch stellen sie die politische Position der Europäischen Kommission dar (Holder et al. 2019, S. 2).

[3] **M-Health** bedeutet „Mobile Health". Dies „steht für die Unterstützung von medizinischen Verfahren und Maßnahmen der Gesundheitsfürsorge durch Geräte wie Smartphones, Tablets, digitale Assistenzsysteme sowie durch Lifestyle- und Gesundheitsapplikationen" (Katzenmeier 2019, S. 264).

[4] Im Rahmen dieses Projekts wurden zehn Start-Up Unternehmen über Herausforderungen befragt, denen sie in Bezug auf den Einsatz von KI begegnen.

10.1.2.2.4 Geistiges Eigentum

KI hat eine Sphäre des Einfallsreichtums und der Kreativität erreicht. Bilder werden erzeugt, Musik wird komponiert, sogar Medikamente werden maschinell entdeckt (Iglesias et al. 2019 S. 3). Rechtlich gesehen gibt es daher eine Vielzahl von Berührungspunkten zum Recht des geistigen Eigentums. Aus diesem Grund hat sich die GFS mit dem Einfluss künstlicher Intelligenz auf das geistige Eigentum befasst und die Diskussion, ob der gegenwärtige Rechtsrahmen für KI geeignet ist, in einem Bericht zusammengefasst (Iglesias et al. 2019). Die GFS konzentrierte sich auf das geistige Eigentum an KI-Lösungen selbst (Iglesias et al. 2019, S. 6–9), an Daten, mit denen die KI „gefüttert" wird (Iglesias et al. 2019, S. 10–11) an Ergebnissen, die durch den Einsatz der KI generiert werden (Iglesias et al. 2019, S. 12–19) sowie auf das Zwischenspiel von geistigen Eigentum und Transparenz und Erklärbarkeit von KI (Iglesias et al. 2019, S. 20–21). Dabei stellte die GFS Lücken bei der Zuweisung und Anerkennung von Urheber- und Patentrechten fest (Iglesias et al. 2019, S. 22). Viele Urheberrechte der EU-Mitgliedstaaten fokussieren sich auf den Menschen[5] (Iglesias et al. 2019, S. 14). Daher sei vor allem die Frage des geistigen Eigentums an KI-generierten Vermögenswerten problematisch (Iglesias et al. 2019, S. 22). Zudem stelle sich die Frage, ob ein Schutzrecht überhaupt notwendig und wünschenswert sei (Iglesias et al. 2019, S. 14–16). Bevor man jedoch zu einer bestimmten Lösung dieser Probleme komme, seien weitere wirtschaftliche und rechtliche Studien und Untersuchungen vorzunehmen (Iglesias et al. 2019, S. 22).

10.1.2.2.5 Themenpapiere der Hochrangigen Expertengruppe für KI

In Umsetzung ihrer in dem Koordinierten Plan für KI und den dazugehörigen Mitteilungen dargelegten Vision in Bezug auf KI hat die Europäische Kommission im Juni 2018 eine **hochrangige Expertengruppe für KI** (**HEG-KI**) eingesetzt und diese damit beauftragt, **KI-Ethikleitlinien** (HEG-KI 2019a) und **KI-Politik- und Investitionsempfehlungen** (HEG-KI 2019b) zu erarbeiten. Beide Dokumente sind für Anbieter von KI-Lösungen wie für Anwender bzw. Endnutzer gleichermaßen interessant. Anbieter von KI-Lösungen können sich bei der technischen Ausgestaltung ihrer Produkte an den KI-Ethikleitlinien orientieren. Zudem bieten die KI-Politik- und Investitionsempfehlungen für Unternehmen, die kurz- und mittelfristig in KI investieren möchten, einen Überblick, in welchen Bereichen die EU voraussichtlich Fördermaßnahmen und Investitionen tätigen wird. Als Anwender bzw. Endnutzer von KI-Lösungen erhalten Sie demgegenüber einen Einblick in wichtige ethische Fragestellungen, die sich bei der Nutzung von KI unweigerlich stellen.

10.1.2.2.5.1 KI-Ethikleitlinien

Ausgehend von Grundrechten als moralischer und rechtlicher Eckpfeiler von KI (HEG-KI 2019a, Kapitel I), hat die HEG-KI Anforderungen an eine vertrauenswürdige KI sowie damit einhergehende technische und nicht-technische Methoden zur Schaffung einer vertrauenswürdigen KI entwickelt (HEG-KI 2019a, Kap. II). Abgerundet werden die

[5] So auch das deutsche Urheberrecht (Thum 2019, § 7 Rn. 13–15).

KI-Ethikleitlinien durch eine Bewertungsliste für vertrauenswürdige KI (HEG-KI 2019a, Kap. III). Vertrauenswürdige KI zeichnet sich demnach durch Rechtmäßigkeit, Einhaltung ethischer Grundsätze und Robustheit in technischer und sozialer Hinsicht aus (HEG-KI 2019a, S. 6). Ausgehend von diesen drei Komponenten entwickelte die HEG-KI eine nicht-abschließende Liste mit sieben Anforderungen an eine vertrauenswürdige KI, die während des gesamten Lebenszyklus Berücksichtigung finden sollen (HEG-KI 2019a, S. 17). Die KI-Ethikleitlinien können allen an der Entwicklung und Nutzung von KI beteiligten Stakeholdern wichtige Impulse geben und dürften gerade auch für die Entwicklung von KI interessant sein. Sie entfalten jedoch keine Verbindlichkeit im Rechtssinne, da sie unverbindliche Leitlinien und eben gerade keine förmliche Verordnung oder Richtlinie darstellen.

Anforderungen an vertrauenswürdige KI

- Vorrang menschlichen Handelns und menschlicher Aufsicht
- Technische Robustheit und Sicherheit
- Schutz der Privatsphäre und Datenqualitätsmanagement
- Transparenz
- Vielfalt, Nichtdiskriminierung und Fairness
- Gesellschaftliches und ökonomisches Wohlergehen
- Rechenschaftspflicht

Die von der HEG-KI aufgestellten Anforderungen an vertrauenswürdige KI sind nach jetzigem Stand nur in Teilaspekten in europäischen oder deutschen Rechtsakten reflektiert. So ist beispielsweise der Vorrang menschlichen Handelns in Teilen in Art. 22 DS-GVO verankert (HEG-KI 2019a, S. 6), wonach jede Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu sein. In jedem Fall bilden die Anforderungen an vertrauenswürdige KI eine praxisnahe Leitlinie für Unternehmen, die den Anspruch haben, ethischen Aspekten bei der Entwicklung und Nutzung von KI einen besonders hohen Stellenwert einzuräumen.

10.1.2.2.5.2 Politik- und Investitionsempfehlungen für eine vertrauenswürdige KI

Zusätzlich zu den KI-Ethikleitlinien hat die HEG-KI am 26. Juni 2019 KI-Politik- und Investitionsempfehlungen (HEG-KI 2019b) veröffentlicht. Das Dokument ist in zwei Kapitel aufgeteilt und enthält 33 Empfehlungen für die Umsetzung einer vertrauenswürdigen KI.

Im ersten Kapitel befasst sich die HEG-KI mit Strategien zur Nutzung vertrauenswürdiger KI, um positive Auswirkungen in Europa zu erzielen (HEG-KI 2019b, S. 9–25). Insoweit empfiehlt die HEG-KI, den Menschen in das Zentrum der Arbeit mit KI zu stellen. KI-Lösungen, die der Menschheit nützlich sind, sind zu fördern; zugleich ist die Gesellschaft jedoch vor möglichen negativen Auswirkungen von KI-Lösungen zu schützen

(HEG-KI 2019b, S. 10–14). Ferner werden Empfehlungen in Bezug auf den privaten und öffentlichen Sektor ausgesprochen. Im privaten Sektor wird unter anderem die Einführung von KI-Technologien und -Dienstleistungen in allen Sektoren in Europa empfohlen (HEG-KI 2019b, S. 15–16). Für den öffentlichen Sektor empfiehlt die HEG-KI unter anderem menschenzentrierte, KI-basierte Dienstleistungen für Einzelpersonen (HEG-KI 2019b, S. 18–19). Das erste Kapitel schließt mit Empfehlungen hinsichtlich der Frage, wie die EU im Bereich der KI-Forschung eine Weltklasse-Stellung erlangen könne (HEG-KI 2019b, S. 21–24).

Kapitel II befasst sich sodann mit den verschiedenen Voraussetzungen, die nach Auffassung der HEG-KI erfüllt sein sollten, um vertrauenswürdige KI zu fördern, beziehungsweise zu ermöglichen (HEG-KI 2019b, S. 26–46). Darunter fallen neben der Unterstützung von KI-Infrastrukturen in den Mitgliedstaaten (HEG-KI 2019b, S. 27) auch Initiativen zum rechtskonformen und ethisch korrekten Datenaustausch (HEG-KI 2019b, S. 28–30). Ferner empfiehlt die HEG-KI den Aufbau von KI-spezifischem Wissen von der Grundschule bis hin zu Weiterbildungsprogrammen für Erwachsene (HEG-KI 2019b, S. 31–37). Hohe Bedeutung kommt auch einem angemessenen Steuerungs- und Regulierungsrahmen zu (HEG-KI 2019b, S. 37–43). Kap. II schließt mit der grundsätzlichen Empfehlung, Finanzierungen und Investitionen im Bereich der KI zu erhöhen (HEG-KI 2019b, S. 43–46).

Die 33 KI-Politik- und Investitionsempfehlungen ergänzen die KI-Ethikleitlinien (HEG-KI 2019a) insoweit, als sie einen eher praktischen Ansatz zur Realisierung vertrauenswürdiger KI verfolgen. Die KI-Politik- und Investitionsempfehlungen verdeutlichen, dass aus Sicht der HEG-KI noch Handlungsbedarf hinsichtlich der Schaffung einer „vertrauenswürdigen KI“ besteht. Dabei stehen nicht nur Themen der Schaffung von Strukturen rechtlicher, technischer sowie finanzieller Art im Fokus der Diskussion; auch der Mensch und die Gesellschaft sollen hinter dem Einsatz von KI nicht zurückstehen.

10.1.2.2.6 Europäische Investitionen und Förderprogramme im Bereich KI

In den KI-Politik- und Investitionsempfehlungen stellt die HEG-KI fest, dass Europa die Datenwirtschaft im Binnenmarkt fördern und in diese investieren solle (HEG-KI 2019b, S. 48), weil die bisherigen Investitionen aus den europäischen Investitionsfonds nicht ausreichen, um die EU zu einem wichtigen Akteur in Bezug auf das Investitionsvolumen zu machen (HEG-KI 2019b, S. 43). Die EU solle demnach eine angemessene Finanzierung für die in dem Dokument ausgesprochenen Empfehlungen gewährleisten, die Investitionsherausforderungen des Marktes angehen und ein offenes und lukrativeres Investitionsklima schaffen, welches vertrauenswürdige KI belohnt (HEG-KI 2019b, S. 43–46).

Um eine verständliche Übersicht über das Engagement der EU zu geben, erhalten Sie zunächst Informationen zu wichtigen Finanzierungsinstrumenten bzw. Investitionsgebern (Woher kommen die Mittel?) und sodann in einem weiteren Schritt Informationen zu einzelnen Programmen (Wofür werden diese Mittel eingesetzt?).

10.1.2.2.6.1 Investitionsgeber

Im Folgenden werden der **Europäische Fond für strategische Investitionen** (**EFSI**), **die Europäische Investitionsbank** (**EIB**) und der **Europäische Investitionsfonds** (**EIF**) als Akteure im Bereich „Investitionen" kurz erläutert.

Hintergrund für die Schaffung des EFSI ist das Absinken des Investitionsniveaus in Folge der Finanz- und Wirtschaftskrise.[6] Der EFSI verfolgt das Ziel, die Wettbewerbsfähigkeit der EU zu verbessern und Investitionsanreize innerhalb der EU zu schaffen.[7] Gem. Art. 3 der **Verordnung über den Europäischen Fonds für strategische Investitionen, die europäische Plattform für Investitionsberatung und das europäische Investitionsvorhabenportal sowie zur Änderung der Verordnungen (EU) Nr. 1291/2013 und (EU) Nr. 1316/2013 – der Europäische Fonds für strategische Investitionen** (**Verordnung 2015/1017/EU**) liegt der Zweck des EFSI darin, „Investitionen"[8] und „einen besseren Zugang zu Finanzmitteln für Unternehmen, die bis zu 3000 Mitarbeiter beschäftigen", zu fördern. Dies geschieht durch die „Bereitstellung von Risikoübernahmekapazität" an die EIB[9] als Bank der EU.

Ferner regelt die Verordnung die Voraussetzungen für den „Einsatz der EU-Garantie".[10] Diese kann für von dem Investitionsausschuss genehmigte EIB-Finanzierungen und -Investitionen gewährt werden. Gleiches gilt für Finanzmittel oder Garantien, die die EIF für EIB-Finanzierungen und –Investitionen von der EIB erhält.[11] Die Finanzierungs- und Investitionsvorhaben müssen mit der Politik der EU im Einklang stehen und eines der in Art. 9 Abs. 2 S. 2 Verordnung 2015/1017/EU genannten Ziele unterstützen. Falls Ihr Unternehmen für potenzielle Finanzierungsmöglichkeiten und Förderprogramme in Betracht kommt, ist es empfehlenswert, die Entwicklungen in diesem Bereich zu beobachten.

Der EIF ist Teil der EIB-Gruppe und spezialisiert auf Risikofinanzierung für **kleine und mittlere Unternehmen** (**KMU**s). Anteilseigner der EIF sind unter anderem die EIB und die EU, vertreten durch die EU-Kommission (Europäischer Investitionsfond o. J.). Sollten Sie ein kleines, mittleres oder Midcap-Unternehmen führen, so können Sie sich direkt an die EIF wenden, wenn Sie im Rahmen der EFSI ein Darlehen oder Eigenkapital beantragen wollen. Die EIB stellt Informationen bezüglich der Finanzierungsmöglichkeiten aus dem EFSI auf ihrer Webseite bereit (Europäische Investitionsbank o. J.). Diese beinhaltet auch eine ausführliche Erläuterung der Kriterien nach denen Antragsteller für Finanzierungen qualifiziert sind (Europäische Investitionsbank o. J.).

---

[6] Vgl. ErwG Nr. 1 und 2 Verordnung 2015/1017/EU.

[7] Vgl. ErwG Nr. 2 Verordnung 2015/1017/EU.

[8] Vgl. Art. 3 lit. a Verordnung 2015/1017/EU.

[9] Vgl. Art. 3 Verordnung 2015/1017/EU.

[10] Vgl. Art. 9 Verordnung 2015/1017/EU.

[11] Vgl. Art. 9 Abs. 2 Verordnung 2015/1017/EU.

10.1.2.2.6.2 Förderprogramme

Zweck der im Folgenden dargestellten Förderprogramme für KI-Entwicklung und -Implementierung ist die Stärkung der Wettbewerbsfähigkeit der EU und ihrer wirtschaftlichen Situation. Die EU-Kommission stellt fest, dass in den Bereichen digitaler Infrastruktur und Netzwerke EU-weit eine jährliche Investitionslücke von 65 Milliarden Euro besteht (Europäische Kommission 2020b S. 4). Möglich sei eine Steigerung des GDP um 14 % bis 2030, wenn die richtigen Investitionen und Reformen eingeleitet würden. Wenn in den zitierten Papieren und Mitteilungen der Kommission und anderer Institutionen von „finanzieller Förderung" die Rede ist, dann bezieht sich dies zumeist auf die hier genannten Programme und Haushaltsposten.

Digital Europe Programme: Das **Digital Europe Programme** (**DEP**) soll nach dem Vorschlag der Kommission Teil des neuen, mehrjährigen Finanzierungsrahmens werden. Vorgesehen sind insgesamt 9,2 Mrd. Euro. Neben 2,7 Mrd. Euro für den Bereich Supercomputing sind auch 2,5 Mrd. Euro für den Bereich KI vorgesehen. In dem Fact Sheet zum DEP werden die Investitionen in und die Erleichterung der Nutzung von KI durch Unternehmen und Behörden, die Erleichterung sicheren Zugangs und Speicherung von großen Datenmengen und Algorithmen sowie die Unterstützung von existierenden KI-Test- und Forschungszentren in bspw. Gesundheits- und Mobilitätswesen als Wege der Förderung aufgezeigt. Weitere 2 Mrd. Euro sollen in den Bereich Cybersecurity und 1,3 Mrd. in die Bereitstellung und Verbesserung von digitalen Strukturen für die Verwendung von KI investiert werden (Europäische Kommission o. J.-a).

Mehrjähriger Finanzierungsrahmen: Der **mehrjährige Finanzierungsrahmen** (**MFF**) ist das Budget der EU, welches von Rat, Parlament und Kommission für einen längerfristigen Rahmen festgesetzt wird (Europäische Kommission o. J.-e). Die Europäische Kommission beabsichtigt, vorbehaltlich der endgültigen Einigung über den MFF eine erhebliche Aufstockung des Budgets zur Unterstützung innovativer KI-Entwicklung. Dies soll über InvestEU (s.u.) geschehen (Europäische Kommission 2020a, S. 7).

Horizon 2020: Unter dem Projektnamen Horizon 2020 hat die EU ein Rahmenprogramm für Forschung und Innovationen der EU geschaffen, welches 2014 begann und am 31. Dezember 2020 endet (Nationale Kontaktstelle IKT o. J.; Europäische Kommission o. J.-b).

Horizon Europe: Parallel zu dem derzeit aktiven Horizon 2020 laufen die Vorbereitungen für das Nachfolgerprogramm Horizon Europe auf Hochtouren. Laut Vorschlag der Kommission soll es einen Umfang von 100 Mrd. Euro haben. Das Programm ist in drei Säulen eingeteilt. Teil der dritten Säule „Innovative Europe" ist auch der **Europäische Innovationsrat** (**EIC**). Der EIC soll innovativen Unternehmen im Sinne eines One Stop Shop ermöglichen, flexible Zuschüsse und Mischfinanzierungen zu erhalten. Horizon Europe soll voraussichtlich am 01. Januar 2021 starten und bis zum 31. Dezember 2027 laufen (Europäische Kommission o. J.-c).

InvestEU: Das Invest EU-Programm, welches auf dem EFSI aufbaut und den Juncker-Plan ablöst, stellt indirekte Finanzierungsinstrumente zusammen. Dies geschieht zum einen durch die Mobilisierung von öffentlichen und privaten Geldern, indem aus dem MFF

Garantien bereitgestellt werden, zum anderen durch die Hilfestellung in Finanzierungsfragen für ausgewählte Projekte sowie durch Vermittlungsdienstleistungen zwischen Investoren und Projekten (Europäische Kommission o. J.-d.).

10.1.2.3 White Paper der EU-Kommission „Artificial Intelligence – A European approach to excellence and trust"

Am 19. Februar 2020 hat die EU-Kommission ein White Paper zu KI mit der Bezeichnung „**Artificial Intelligence – A European Approach to excellence and trust**" (**White Paper KI**) herausgebracht (Europäische Kommission 2020a). White Paper sind Dokumente, die Vorschläge für ein Aktivwerden der EU in einem speziellen Bereich ausarbeiten. Sinn und Zweck eines White Papers ist, eine Debatte anzustoßen, an der die Öffentlichkeit sowie verschiedene EU-Institutionen teilnehmen und einen politischen Konsens erzielen. Zu Beginn werden in dem White Paper KI insgesamt sechs Aktionsschritte vorgestellt: (1.) Eine überarbeitete Version des Koordinierten Plans soll bis Ende 2020 vorangebracht werden (Europäische Kommission 2020a, S. 5). (2.) Die Errichtung von Exzellenz- und Testzentren, die bei der Zusammenführung zwischen europäischen, nationalen und privaten Investitionen helfen sollen, soll erleichtert werden (Europäische Kommission 2020a, S. 3, 6). (3.) Durch die ausgeprägte Bildungssäule im Digital Europe Programme sollen im akademischen Bereich weltweit Experten gewonnen und eine weltweit konkurrenzfähige Ausbildung gewährleistet werden (Europäische Kommission 2020a, S. 7). (4.) Es soll mindestens ein digitales Innovationszentrum pro Mitgliedstaat geschaffen werden, welches sich in hohem Maße auf Künstliche Intelligenz spezialisiert (Europäische Kommission 2020a, S. 7). (5.) Im Rahmen von Horizon Europe soll eine neue öffentlich-private Partnerschaft in den Bereichen KI, Daten und Robotik geschaffen werden. Diese soll mit anderen Einrichtungen und Private Public Partnerships unter der Horizon Europe Initiative zusammenarbeiten (Europäische Kommission 2020a, S. 7). (6.) Die Kommission will offene und transparente Sektorendialoge durchführen, die in den Bereichen Gesundheitswesen, ländliche Verwaltung und Öffentlicher Dienstleistungssektor dazu beitragen, Aktionspläne zur Entwicklung und Anpassung zu schaffen (Europäische Kommission 2020a, S. 8). Grundlage aller Vorschläge, die das White Paper KI aufführt, sind auf finanzierender Seite das Horizon Europe Programme, der Nachfolger von Horizon 2020, sowie das Digital Europe Programme. Zusätzlich zu Horizon Europe hat die Kommission das Digital Europe Programme initiiert, welches die bereits angestoßenen Initiativen mit einem Budget von 9,2 Milliarden Euro in den Jahren 2021 bis 2027 flankiert (Europäische Kommission o. J.-a). Letzteres Programm ist ein Teil des neuen, mehrjährigen Finanzrahmens der EU.

Neben Zusammenfassungen der Vorschläge zu einem neuen Haftungsregime für KI fokussiert das White Paper KI sich auch auf eine nachhaltige Entwicklung von KI insbesondere dahingehend, dass im Rahmen des neuen „Green New Deals" KI-Technologien nicht nur ressourcenschonend entwickelt und eingesetzt werden sollen, sondern unter Umständen sogar selbst in der Lage sein müssen, nachhaltige Entscheidungen zu treffen und kritische Selbstanalysen unter den Aspekten Nachhaltigkeit und Ressour-

censchonung durchzuführen (Europäische Kommission 2020a, S. 3, 6). Ein weiterer Schwerpunkt liegt auf der Zugänglichmachung und nicht übermäßigen Belastung von kleinen und mittelgroßen Unternehmen. Einen ähnlichen Fokus verfolgt die Europäische Kommission auch in Ihrer Mitteilung „Shaping Europe's digital future" (Europäische Kommission 2020b, S. 1).

Des Weiteren werden die internationale Zusammenarbeit, insbesondere Im Rahmen der OECD, der G20, WTO sowie das europäische Engagement im Rahmen von UN-Verfahren zum Thema KI thematisiert (Europäische Kommission 2020a, S. 8).

Das White Paper KI macht zudem Vorschläge in Bezug auf KI-spezifische, legislative Handlungspositionen in den nächsten Jahren. Im Vordergrund steht dabei eine risikobasierte Vorgehensweise. Demnach soll die Regulierungsintensität in allen legislativen Vorhaben von den zwei Faktoren „Risikointensität des Sektors" und „Risikointensität des konkreten Einsatzes der KI" abhängen (Europäische Kommission 2020a, S. 18, 19).

Der letzte Teil des White Paper KI vertieft die Anforderungen an die Entwicklung und Nutzung von KI, die schon in den KI-Ethikleitlinien aufgegriffen wurden und spricht sich für verbindliche Vorgaben aus.

Im Einzelnen benennt das White Paper KI folgende Anforderungen für die Entwicklung und Nutzung von KI

(1) Nutzung vollständiger, repräsentativer und diskriminierungsfreier Datensätze für das Training der KI (Europäische Kommission 2020a, S. 20);
(2) Protokollierungspflichten bezüglich der Art und Weise des Einsatzes der KI (Europäische Kommission 2020a, S. 20);
(3) Informationspflichten hinsichtlich Funktionstüchtigkeit und Fehlerresistenz (Europäische Kommission 2020a, S. 20);
(4) (End-)kontrolle (je nach Risikofaktor verschieden ausgestaltet) in menschlichen Händen (Europäische Kommission 2020a, S. 21);
(5) Spezifische Anforderungen an besondere Arten von KI (insbesondere die automatische, biometrische Identifizierung wird hier als regulierungsbedürftige Technologie aufgeführt) (Europäische Kommission 2020a, S. 21–22).

Auch das White Paper KI hebt einige Hauptprobleme der KI-Regulierung durch Gesetze hervor. So besteht eine zentrale Herausforderung darin, den richtigen Adressatenkreis herauszuarbeiten. Da die Kontrollmöglichkeiten sich verlagern (so kann der Entwickler der KI-Lösung Risiken in der Entwicklungsphase und der Betreiber die Risiken bei der Nutzung besser kontrollieren), könne es nicht bei einer Produzentenhaftung bleiben. Zudem sieht es die EU-Kommission als wichtig an, die geografische Reichweite einer potenziellen KI-Gesetzgebung losgelöst vom Unternehmenssitz zu definieren. Jeder Anbieter von KI-Lösungen in der EU sollte an diese gebunden sein (Europäische Kommission 2020a, S. 23–25).

Als Maßnahme abseits klassischer Regulierung schlägt das White Paper KI ein freiwilliges Label für risikoarme KI vor. Unternehmen, die dieses Label nutzen möchten, müssten die verminderte Risikointensität ihrer KI zwar beständig nachweisen, könnten durch das Label jedoch das Vertrauen in KI erhöhen (Europäische Kommission, S. 25).

Zu guter Letzt kündigt die EU in ihrem White Paper KI an, im Juni 2020 eine überarbeitete Version der Ethik-Leitlinien für eine vertrauenswürdige KI vorlegen zu wollen, in die bis dahin das Feedback von bis zu 350 Organisationen eingearbeitet werden soll.

10.2 Allgemeine Initiativen und Regelungen von besonderer Bedeutung für KI

Die nachfolgend genannten Verordnungen und Richtlinien sind in ihrem Anwendungsbereich nicht auf KI beschränkt, dürften jedoch häufig für Entwicklung und/oder Nutzung von KI-Lösungen Anwendung finden. Beachten Sie, dass der Regelungsgehalt von EU-Richtlinien grundsätzlich für den Adressaten erst dann rechtsverbindlich wird, wenn die Mitgliedstaaten die Richtlinie in nationales Gesetzesrecht umgesetzt haben. Sie erhalten unten stehend daher auch Informationen zu den für die jeweiligen Richtlinien geltenden Umsetzungsfristen. EU-Verordnungen entfalten demgegenüber unmittelbar mit Inkrafttreten Anwendung für die Adressaten und sind somit zu diesem Zeitpunkt schon rechtsverbindlich.

10.2.1 Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU

Die **Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU** (**Verordnung 2018/1807/EU**) bezweckt die Schaffung rechtlicher Voraussetzungen für den freien Verkehr nicht-personenbezogener Daten in der EU. Zu diesem Zweck regelt die Verordnung 2018/1807/EU die weitest gehende Aufhebung von Datenlokalisierungsauflagen, die Verfügbarkeit von Daten für zuständige Behörden und die Übertragung von Daten für berufliche Nutzer.[12] Die Verordnung gilt seit dem 28. Mai 2019. Mitgliedstaaten dürfen somit Unternehmen nicht länger verpflichten, Daten an einem Standort innerhalb ihrer Grenzen zu speichern oder zu verarbeiten, wenn nicht Gründe der öffentlichen Sicherheit unter Achtung des Grundsatzes der Verhältnismäßigkeit eine Datenlokalisierungsauflage rechtfertigen.[13]

Die Verordnung 2018/1807/EU fordert die Mitgliedstaaten auf, bis zum 30. Mai 2021 „alle bestehenden Datenlokalisierungsauflagen, die durch allgemeine Rechts- und Ver-

[12] Vgl. Art. 1 Verordnung 2018/1807/EU.

[13] Vgl. Art. 4 Abs. 1 Verordnung 2018/1807/EU.

waltungsvorschriften geregelt sind“ aufzuheben.[14] Für die Mitgliedstaaten besteht jedoch die Möglichkeit, gegenüber der EU-Kommission zu begründen, warum eine bestehende Datenlokalisierungsauflage aufrechterhalten werden soll, wenn sie der Ansicht sind, die betroffene Datenlokalisierungsauflage sei mit den Voraussetzungen dieser Verordnung vereinbar. Letztendlich wird wohl erst nach Ablauf des 30. Mai 2021 Klarheit über den rechtlichen Rahmen für die Datenmobilität bestehen.

Neben die Datenlokalisierungsauflagen der Mitgliedstaaten treten „private Beschränkungen“, also nicht-staatliche Beschränkungen, der Mobilität von Daten. Diese können zum Beispiel vertraglicher oder technischer Natur sein. Solche Beschränkungen können Nutzern von Datenverarbeitungssystemen die Übertragung ihrer Daten zu einem anderen Dienstanbieter erschweren oder gar unmöglich machen.[15] Diesen Umstand adressiert Art. 6 (Übertragung von Daten) der Verordnung 2018/1807/EU. Zum Zwecke der Selbstregulierung fördert die EU-Kommission die Entwicklung von „Verhaltensregeln“.[16] Bei der Entwicklung dieser Verhaltensregeln sollen alle „relevanten Interessensträger“, darunter auch Verbände für kleine und mittlere Unternehmen sowie Start-ups, einbezogen werden.[17] Berücksichtigt werden sollen dabei auch „bewährte Verfahren zur Erleichterung des Wechsels des Diensteanbieters und der Übertragung von Daten in einem strukturierten, gängigen und maschinenlesbaren Format“.[18]

Die Verordnung 2018/1807/EU definiert „Daten“[19] als „keine personenbezogenen Daten“ im Sinne des Art. 4 Nr. 1 DS-GVO. Damit werden in rechtlicher Hinsicht Überlappungen mit der DS-GVO vermieden. Die Abgrenzung von personenbezogenen und nicht-personenbezogenen Daten kann jedoch in der Praxis im Einzelfall schwierig sein. Aus anonymisierten Daten, also nicht-personenbezogenen Daten, können beispielsweise wieder personenbezogene Daten entstehen, wenn die Daten später doch re-identifiziert werden. Auch kann ein Datum, das für sich alleine kein personenbezogenes Datum darstellt, durch die Zusammenführung mit anderen Daten einen Personenbezug erhalten.[20] Interessant ist daher die Frage, welche Regeln für gemischte Datensätze gelten, bei denen personenbezogene und nicht-personenbezogene Daten nicht ohne Aufwand getrennt werden können. Dieses Problem greift Art. 2 Abs. 2 Satz 2 der Verordnung 2018/1807/EU auf und regelt, dass die Verordnung 2018/1807/EU bei einer untrennbaren Verbindung personenbezogener und nicht-personenbezogener Daten in einem Datensatz nicht die DS-GVO berührt. Die Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union stellen dementsprechend noch einmal klar, dass, „falls die nicht-personenbezogenen Daten und die personenbezogenen

[14] Vgl. Art. 4 Abs. 3 S. 1 Verordnung 2018/1807/EU.

[15] Vgl. ErwG Nr. 5 Verordnung 2018/1807/EU.

[16] Vgl. Art. 6 Abs. 1 Verordnung 2018/1807/EU.

[17] Vgl. Art. 6 Abs. 1 Verordnung 2018/1807/EU.

[18] Vgl. Art. 6 Abs. 1 lit. a Verordnung 2018/1807/EU.

[19] Vgl. Art. 3 Nr. 1 Verordnung 2018/1807/EU.

[20] Siehe dazu die Beispiele in Klar und Kühling 2018, Art. 4 Nr. 1 Rn. 36.

Daten „untrennbar miteinander verbunden“ sind, die Datenschutzrechte und -pflichten aus der Datenschutz-Grundverordnung in vollem Umfang für den gesamten gemischten Datensatz gelten, und zwar auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen“ (Europäische Kommission 2018c, S. 9). Sollten hingegen die personenbezogenen und die nicht-personenbezogenen Daten eines Datensatzes voneinander trennbar sein, gilt für personenbezogene Daten die DS-GVO und für nicht-personenbezogene Daten die Verordnung 2018/1807/EU (Europäische Kommission 2018c, S. 9).

Die Befugnisse der zuständigen Behörden, Zugang zu Daten zu verlangen oder zu erhalten, lässt die Verordnung 2018/1807/EU unberührt, um die Erfüllbarkeit der Amtspflichten zuständiger Behörden weiterhin zu gewährleisten.[21] Begründet wird dies unter anderem damit, dass Datenlokalisierungsauflagen häufig eine Folge „mangelnden Vertrauens in eine grenzüberschreitende Datenverarbeitung“ seien, weil angenommen werde, dass zuständigen Behörden die Daten zur Ausführung von Überprüfungszwecken und Audits nicht zugänglich seien. Der Zugang zu den Daten darf daher nicht mit der Begründung verweigert werden, dass die verlangten Daten in einem anderen Mitgliedstaat verarbeitet werden und somit den zuständigen Behörden nicht zur Verfügung stünden.[22]

Da Daten der „Rohstoff“ für jedwede Nutzung von KI sind, dürfte sich die Verordnung 2018/1807/EU positiv auf die grenzüberschreitende Nutzung und Entwicklung von KI in den Mitgliedstaaten auswirken.

10.2.2 Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen

Die **Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen** („**Richtlinie 2019/770/EU**“) verfolgt das Ziel, ein hohes Verbraucherschutzniveau herzustellen, indem sie Anforderungen für Verträge zwischen Verbrauchern und Unternehmern über die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen festlegt.[23] Die Richtlinie ist dabei in ihrem Anwendungsbereich auf den B2C-Bereich beschränkt (Spindler und Sein 2019a, S. 416).

Die Richtlinie 2019/770/EU definiert „digitale Inhalte“ als Daten, die in „digitaler Form erstellt und bereitgestellt werden“.[24] „Digitale Dienstleistungen“ werden definiert als „Dienstleistungen, die dem Verbraucher die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen“ oder „Dienstleistungen, die die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstell-

[21] Vgl. Art. 5 Abs. 1 Verordnung 2018/1807/EU.

[22] Vgl. Art. 5 Abs. 1 und ErwG Nr. 24 Verordnung 2018/1807/EU.

[23] Vgl. Art. 1 Richtlinie 2019/770/EU.

[24] Vgl. Art. 2 Nr. 1 Richtlinie 2019/770/EU.

ten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen".[25] In den Anwendungsbereich der Richtlinie 2019/770/EU fallen daher Computerprogramme, Anwendungen, Video-, Audio und Musikdateien sowie digitale Dienstleistungen, „die die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form sowie den Zugriff auf sie ermöglichen".[26] Auch **Software-as-a-Service** (**SaaS**) ist erfasst.[27]

Soweit eine KI-Lösung entweder unter die Definition der „digitalen Inhalte" oder „digitalen Dienstleistungen" im Sinne der Richtlinie 2019/770/EU fällt und für Verbraucher verfügbar gemacht wird, gelten für die digitalen Inhalte oder Dienstleistungen die Regelungen dieser Richtlinie. Daher sollten sich Unternehmen, die im B2C-Bereich tätig sind, der Implikationen dieser Regelungen auf das eigene Geschäftsmodell bewusst sein und die nationalen rechtlichen Entwicklungen verfolgen.

Aus Anbietersicht dürften insbesondere die Regelungen der Art. 11 ff. der Richtlinie 2019/770/EU von Bedeutung sein. Diese umfassen neben der Haftung des Unternehmers auch Regeln über die Beweislast sowie über Abhilfemaßnahmen seitens des Unternehmers gegenüber Verbrauchern bei nicht erfolgter Bereitstellung des Dienstes oder Inhalts oder Vertragswidrigkeit.

Art. 11 Abs. 1 Richtlinie 2019/770/EU regelt die Haftung des Unternehmers für jede nicht in Übereinstimmung mit Art. 5 Richtlinie 2019/770/EU erfolgte Bereitstellung. Art. 5 Richtlinie 2019/770/EU trägt die Überschrift „Bereitstellung der digitalen Inhalte oder digitaler Dienstleistungen" und gibt sowohl das „Wann" als auch das „Wie" der Bereitstellung vor.[28] So muss ein Unternehmer, die digitalen Inhalte oder digitalen Dienstleistungen nach Abschluss des Vertrages unverzüglich bereitstellen, sofern nichts Abweichendes vereinbart ist.[29] Dabei dürfte unter „unverzüglich" „ohne schuldhaftes Zögern" zu verstehen sein (Spindler und Sein 2019a, S. 419). Der Unternehmer haftet daher im Falle einer verspäteten, nicht erfolgten oder nicht vertragskonformen Bereitstellung der digitalen Inhalte bzw. Dienstleistungen. Die Absätze 2 und 3 des Art. 11 Richtlinie 2019/770/EU unterscheiden sodann hinsichtlich der Haftung des Unternehmers danach, ob der Vertrag eine einmalige (oder eine Reihe einzelner Bereitstellungen) oder fortlaufende Bereitstellung vorsieht: Bei einzelnen Bereitstellungen digitaler Inhalte oder digitaler Dienstleistungen haftet der Unternehmer für jede Vertragswidrigkeit, die zum Zeitpunkt der Bereitstellung besteht, für mindestens zwei Jahre, „mit der Möglichkeit für Mitgliedstaaten darüber hinaus zu gehen" (Spindler und Sein 2019b, S. 491). Bei einer fortlaufenden Bereitstellung besteht die Gewährleistung für die Dauer der Vertragslaufzeit.

Art. 12 Richtlinie 2019/770/EU regelt die Beweislastverteilung. Gem. Abs. 1 der Norm trägt grundsätzlich der Unternehmer die Beweislast dafür, dass digitale Inhalte oder digitale Dienstleistungen entsprechend Art. 5 Richtlinie 2019/770/EU bereitgestellt wurden.

[25] Vgl. Art. 2 Nr. 2 lit. a und b Richtlinie 2019/770/EU.

[26] Vgl. ErwG 19 Richtlinie 2019/770/EU.

[27] Vgl. ErwG 19 Richtlinie 2019/770/EU.

[28] Siehe ferner bezüglich Ort, Zeit und Wirkung der Erfüllung Spindler und Sein 2019, S. 419.

[29] Vgl. Art. 5 Abs. 1 S. 2 Richtlinie 2019/770/EU.

Unternehmer müssen also beweisen, dass sie die digitalen Inhalte oder Dienstleistungen vertragsgemäß bereitgestellt haben. Achten Sie daher darauf, bei der Vertragsgestaltung die Hauptleistungspflichten in Bezug auf Ort, Zeit und Art der Leistung klar zu formulieren. Zudem können Sie Prozesse einführen, mittels derer sie im Streitfall eine pflichtgemäße Bereitstellung nachweisen können. Die Absätze 2 und 3 des Art. 12 Richtlinie 2019/770/EU regeln hingegen die Beweislast in Fällen einer Haftung des Unternehmers. Bei der einzelnen Bereitstellung digitaler Inhalte oder Dienstleistungen trägt der Unternehmer für ein (1) Jahr ab der Bereitstellung die Beweislast dafür, dass die Leistung zu dem Zeitpunkt der Bereitstellung im vertragsgemäßen Zustand war. Bei einer fortlaufenden Bereitstellung gilt diese Beweislast für den Zeitraum der Laufzeit des Vertrages.

Auch die Richtlinie 2019/770/EU differenziert in Teilen ausdrücklich zwischen nicht-personenbezogenen Daten und personenbezogenen Daten. Bezüglich letzteren regelt die Richtlinie 2019/770/EU korrekterweise, dass für Verträge, die dieser Richtlinie unterfallen, zusätzlich die DS-GVO Anwendung findet.[30]

Da eine europäische Richtlinie im Gegensatz zu europäischen Verordnungen grundsätzlich keine unmittelbare Anwendung findet, muss diese erst durch den nationalen Gesetzgeber in nationales Recht umgesetzt werden. Die Umsetzungsfrist für die Richtlinie 2019/770/EU läuft bis zum 1. Juli 2021; Anwendung finden die Vorschriften ab dem 1. Januar 2022.[31] Als Anbieter von KI-Lösungen sollten Sie die nationalen Entwicklungen in diesem Bereich verfolgen, um frühzeitig etwaige rechtliche Anpassungen (zum Beispiel von Verträgen), aber auch technische Anpassungen (beispielsweise zum Nachweis der rechtskonformen Bereitstellung der digitalen Inhalte) vornehmen zu können.

Die Richtlinie 2019/770/EU trägt dazu bei, fortschreitende, technische Entwicklungen durch Digitalisierung mit einem hohen Verbraucherschutzniveau in Einklang zu bringen. Aus Sicht der Verbraucher, welche digitale Inhalte und digitale Dienstleistungen auch im Rahmen von KI-Lösungen nutzen, ist zu begrüßen, dass Verbraucherrechte für die digitale Wirtschaft und somit ein Plus an Rechtssicherheit in diesem zukunftsträchtigen Bereich geschaffen werden. Wie die nationale Umsetzung der Richtlinie 2019/770/EU im Ergebnis aussehen wird, bleibt zum jetzigen Zeitpunkt jedoch abzuwarten.

10.2.3 Richtlinie über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG

Auch die neue Urheberrechtsrichtlinie mit der Bezeichnung „**Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG**“ (**Richtlinie 2019/790/EU**) entfaltet große

[30] Vgl. Art. 3 Abs. 8 Richtlinie 2019/770/EU.

[31] Vgl. Art. 24 Abs. 1 Richtlinie 2019/770/EU.

Bedeutung für die Entwicklung, Vermarktung und Nutzung von KI-Lösungen. Gem. Art. 26 Abs. 1 gilt die Richtlinie für Werke und sonstige Schutzgegenstände, die ab dem 7. Juni 2021 oder danach nach dem Recht der Mitgliedstaaten auf dem Gebiet des Urheberrechts geschützt sind. Sie berührt nicht Rechte und Handlungen, die vor dem 7. Juni 2021 abgeschlossen bzw. erworben wurden. Wie für alle Richtlinien ist zudem eine Umsetzung in das nationale Recht erforderlich, da Richtlinien grundsätzlich nicht unmittelbar gelten. Diese Umsetzung hat gemäß Art. 29 Abs. 1 der Richtlinie 2019/790/EU bis zum 07. Juni 2021 zu erfolgen.

In Art. 3 und 4 Richtlinie 2019/790/EU wurden neue (und gegenüber dem deutschen Recht weitergehende) Schrankenregelungen für Text und Data Mining festgelegt. Zurzeit ist Text und Data Mining in Deutschland in § 60d UrhG geregelt, welcher vorsieht, dass Text und Data Mining nur für die wissenschaftliche Forschung zulässig ist. Mit einer Bindung an den Zweck der wissenschaftlichen Forschung unterfällt das Text und Data Mining zu anderen (z. B. wirtschaftlichen) Zwecken der Zustimmung des Urhebers. Daher muss in diesem Fall eine Lizenz erworben werden. Alle Urheber der zu diesem Zwecke verwendeten Ursprungsmaterialien bzw. Daten zu ermitteln, ist jedoch im Hinblick auf die Fülle an verwendeten Daten extrem schwer. Text und Data Mining zu derartigen Zwecken würde somit oft mit einer Urheberrechtsverletzung einhergehen. Daher (und auch um die Privatwirtschaft zu Innovationen) anzuregen[32], hat der EU-Gesetzgeber die bereits bestehende Schrankenbestimmung hinsichtlich dieser Urheberrechte erweitert.

Daher sieht Art. 4 Richtlinie 2019/790/EU keine Bindung an den Zweck der wissenschaftlichen Forschung mehr vor und ermöglicht damit auch die analytische Datensammlung- und Verarbeitung zu sonstigen, auch wirtschaftlichen Zwecken (Mitterer et al. 2020, S. 4). Zudem dürfen gemäß Art. 4 Abs. 2 2019/790/EU die Vervielfältigungen so lange aufbewahrt werden, wie es für die Zwecke des Text und Data Mining notwendig ist. Art. 4 Abs. 3 Richtlinie 2019/790/EU sieht die Möglichkeit des Rechteinhabers vor, die Werke und sonstigen Schutzgegenstände mit einem Nutzungsvorbehalt zu versehen. Durch einen Vorbehalt schafft der Rechteinhaber eine Barriere für die Nutzung der Daten und kann sie dadurch kommerzialisieren. Dieser ist gemäß Art. 4 Abs. 3 Richtlinie 2019/790/EU nur wirksam, wenn er maschinenlesbar erklärt wird. Dies ist auch aus praktischen Gründen sinnvoll. Schließlich muss der Nutzungsvorbehalt im Rahmen automatisierter Prozesse wie auch bei der Nutzung einer KI-Lösung auch von einer Software erkannt werden können (Steinbrecher 2019, S. 640). Gleichzeitig bedeutet die Möglichkeit der Erklärung eines Nutzungsvorbehalts, dass eine pauschale Vergütung, wie sie zurzeit noch in § 60h UrhG geregelt ist, in Zukunft nicht mehr geleistet werden muss (Steinbrecher 2019, S. 640–641), sollte die pauschale Vergütung doch einen Ausgleich dafür schaffen, dass die erlaubte Nutzung nach § 60d UrhG nicht durch Vertragsbestimmungen unterlaufen werden durfte (Hagemeier 2019, § 60d, Rn. 11). Mit der Möglichkeit eines Nutzungsvorbehalts ist dies nicht mehr notwendig. Die Richtlinie 2019/790/EU ermöglicht damit einen

[32] Vgl. Erwägungsgrund 18 Richtlinie 2019/790/EU.

einfachen Ausbau von KI, „die auf Auswertung und Analyse großer Datenmengen ohne urheberrechtliche Hemmnisse angewiesen ist“ (Mitterer et al. 2020, S. 4).

10.2.4 Datenschutzgrundverordnung (DS-GVO)

Wann immer eine KI-Lösung personenbezogene Daten verarbeitet, ist der Anwendungsbereich der DS-GVO eröffnet. Informationen zu den rechtlichen Implikationen der DS-GVO finden Sie unter Kap. 2.

10.2.5 Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors

Die Richtlinie über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors („**Richtlinie 2019/1024/EU**“) stellt nicht nur eine Abänderung, sondern aufgrund der Vielzahl der Änderungen sogar eine Neufassung der bisherigen **Richtlinie vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors** („**Richtlinie 2003/98/EG**“) dar.[33] Durch die Neufassung der Richtlinie 2019/1024/EU möchte die Kommission den rechtlichen Rahmen an den Stand der Technik anpassen und digitale Innovationen „insbesondere im Hinblick auf künstliche Intelligenz“[34] fördern.

Der Anwendungsbereich der Richtlinie beschränkt sich dabei auf „öffentliche Stellen“ und „öffentliche Unternehmen“.[35] „Öffentliche Stellen“ im Sinne dieser Richtlinie 2019/1024/EU sind unter anderem der Staat oder Gebietskörperschaften.[36] Unter „öffentlichen Unternehmen“ im Sinne dieser Richtlinie 2019/1024/EU werden diejenigen Unternehmen verstanden, auf welche „öffentliche Stellen aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Bestimmungen unmittelbar oder mittelbar einen beherrschenden Einfluss ausüben können“; ferner müssen diese Unternehmen in den in Art. 1 Abs. 1 lit. b Richtlinie 2019/1024/EU genannten Bereichen tätig sein.[37] Private Unternehmen sind somit nicht Adressaten dieser Richtlinie.

Die Richtlinie 2019/1024/EU regelt insbesondere, welche Daten und Dokumente Dritten zwecks Weiterverwendung bereitgestellt werden sollen und auf welche Art dies geschehen soll. Ein „Dritter“ im Sinne der Richtlinie 2019/1024/EU ist „jede natürliche oder juristische Person außer der öffentlichen Stelle oder dem öffentlichen Unternehmen, die/

[33] Vgl. ErwG Nr. 1 Richtlinie 2019/1024/EU.

[34] Vgl. ErwG Nr. 3 Richtlinie 2019/1024/EU.

[35] Vgl. Art. 1 lit. a und b Richtlinie 2019/1024/EU.

[36] Vgl. Art. 2 Nr. 1 Richtlinie 2019/1024/EU.

[37] Vgl. Art. 2 Nr. 3 Richtlinie 2019/1024/EU.

das im Besitz der Daten ist".[38] Somit kommen die Regelungen auch privaten Unternehmen zu Gute.

Art. 1 Abs. 7 Richtlinie 2019/1024/EU legt fest, dass mit dieser Richtlinie die „Weiterverwendung vorhandener Dokumente" geregelt werden soll, die sich im Besitz öffentlicher Stellen und öffentlicher Unternehmen der Mitgliedstaaten befinden. Eingeschlossen sind auch Dokumente, auf welche die **Richtlinie zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE)** (**Richtlinie 2007/2/EG**) Anwendung findet.[39]

Art. 1 Abs. 1 Richtlinie 2019/1024/EU ist zu entnehmen, dass die Verwendung „offener Daten" gefördert werden soll. Deswegen formuliert die Richtlinie Mindestvorschriften für die Weiterverwendung und die praktischen Modalitäten zur Erleichterung der Weiterverwendung vorhandener Dokumente im Besitz öffentlicher Stellen der Mitgliedstaaten und öffentlicher Unternehmen.[40] Auch Forschungsdaten sind (unter den in Art. 10 Richtlinie 2019/1024/EU festgelegten Bedingungen) umfasst.[41] Die Richtlinie definiert „offene Daten" zwar nicht, in Erwägungsgrund Nr. 16 der Richtlinie 2019/1024/EU findet sich jedoch Folgendes: „Das Konzept „offene Daten" (**Open Data**) bezeichnet nach dem allgemeinen Verständnis Daten in einem offenen Format, die von Allen zu jedem Zweck frei verwendet, weiterverwendet und weitergegeben werden können."

Welche Dokumente nicht vom Anwendungsbereich umfasst sind, wird in Art. 1 Abs. 2 Richtlinie 2019/1024/EU festgelegt. In der zwölf Dokumentenarten umfassenden Liste der Dokumente, die nicht vom Anwendungsbereich der Richtlinie 2019/1024/EU erfasst sind, sind unter anderem „Dokumente, die das geistige Eigentum Dritter betreffen", „sensible Daten, die nach den Zugangsregelungen der Mitgliedstaaten nicht zugänglich sind," oder „Logos, Wappen und Insignien" genannt. Bezüglich der sogenannten „hochwertigen Datensätze" sei auf die besonderen Regelungen in Art. 13 und 14 Richtlinie 2019/1024/EU hingewiesen. Diese erfahren eine besondere Behandlung in dieser Richtlinie, da sie aufgrund ihrer Bedeutung für die Gesellschaft, die Umwelt und die Wirtschaft eine besondere Stellung einnehmen.[42]

Beachten Sie, dass die Richtlinie 2019/1024/EU in ihrem Anwendungsbereich auf Fragen der Weiterverwendung vorhandener Daten beschränkt ist. Für Anbieter von KI-Lösungen ist jedoch nicht nur ein Anspruch auf Weiterverwendung vorhandener Daten von Bedeutung, sondern auch die Frage, ob ein Anspruch auf Zugang zu den von der Richtlinie erfassten Dokumenten besteht. Zu trennen ist also die Frage nach dem „Ob" der Gestattung einer Weiterverarbeitung von Dokumenten, die sich im „Besitz öffentlicher Stellen und Unternehmen befinden" von der Frage des „Ob" des Zugangs zu diesen.

---

[38] Vgl. Art. 2 Nr. 17 Richtlinie 2019/1024/EU.

[39] Vgl. Art. 1 Abs. 7 Richtlinie 2019/1024/EU.

[40] Vgl. Art. 1 Abs. 1 lit. c Richtlinie 2019/1024/EU.

[41] Vgl. Art. 1 Abs. 1 Richtlinie 2019/1024/EU.

[42] Vgl. die Definition von „hochwertige Datensätze" in Art. 2 Nr. 10 Richtlinie 2019/1024/EU.

Zugangsrechte lassen sich sowohl aus der bisherigen Richtlinie 2003/98/EG als auch aus ihrer aktuellen Neufassung, Richtlinie 2019/1024/EU, nicht ableiten. Beide Richtlinien regeln lediglich die Weiterverwendung[43] von Dokumenten (Buchholz 2019, S. 200). Die Richtlinie 2019/1024/EU findet aber dann Anwendung, wenn Zugangsregelungen der Union oder solche der Mitgliedstaaten ein Zugangsrecht begründen.[44] In Deutschland leitet sich zum Beispiel ein Zugangsrecht zu amtlichen Informationen aus dem **Informationsfreiheitsgesetz** (**IFG**)[45] ab. Das Zugangsrecht kann jedoch eingeschränkt oder ausgeschlossen sein, wenn ein Fall der §§ 3 bis 6 IFG vorliegt. Exemplarisch für einen solchen Fall seien der „Schutz personenbezogener Daten“[46] und der „Schutz des geistigen Eigentums und von Betriebs- oder Geschäftsgeheimnissen“[47] genannt. Weitere Zugangsrechte können sich aus Informationsfreiheitsgesetzen der Länder oder Informationsfreiheitssatzungen auf kommunaler Ebene ergeben (Buchholz 2019, S. 199).

Wenn ein Zugangsrecht besteht, muss in der Folge die Frage nach einer etwaigen Gestattung der Weiterverwendung geklärt werden. Gem. Art. 3 Abs. 1 Richtlinie 2019/1024/EU haben die Mitgliedstaaten grundsätzlich dafür Sorge zu tragen, dass dieser Richtlinie unterfallende Dokumente für kommerzielle sowie nicht kommerzielle Zwecke weiterverwendet werden können. Die Richtlinie nimmt dabei solche Dokumente aus, „an denen Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archiven Rechte des geistigen Eigentums innehaben“ sowie „Dokumente im Besitz öffentlicher Unternehmen“. Falls diese die Weiterverwendung erlauben, sollen die Mitgliedstaaten eine Verwendung der Dokumente für kommerzielle und nicht kommerzielle Zwecke sicherstellen.[48] Für öffentliche Unternehmen soll zudem keine „allgemeine Verpflichtung zur Gestattung der Weiterverwendung“ für selbst erstellte Dokumente bestehen.[49] In jedem Fall der Weitergabe von Dokumenten im Sinne des Art. 3 Richtlinie 2019/1024/EU sind die Kapitel III und IV einzuhalten.[50] Diese Kapitel beinhalten unter anderem Regelungen in Bezug auf verfügbare Formate, Gebühren und Entgelte, Transparenz, Standardlizenzen, die Nichtdiskriminierung und das Verbot von Ausschließlichkeitsvereinbarungen.

Aber auch im Hinblick auf öffentliche Stellen dürfte sich aus Richtlinie 2019/1024/EU kein uneingeschränkter Anspruch auf Weiterverwendung von Dokumenten und Daten ergeben. Vielmehr regelt Art. 4 Richtlinie 2019/1024/EU ein Verfahren, in dem ein Antrag auf Weiterverwendung zu stellen ist. Dieser kann freilich auch negativ beschieden werden. In diesem Fall soll die Ablehnung dem Antragsteller gegenüber begründet werden.[51] Die-

[43] Siehe zur Definition von Weiterverwendung Art. 2 Nr. 11 lit. a und b Richtlinie 2019/1024/EU.

[44] Vgl. Art. 1 Abs. 3 Richtlinie 2019/1024/EU.

[45] Vgl. § 1 Abs. 1 IFG.

[46] Vgl. § 5 IFG.

[47] Vgl. § 6 IFG.

[48] Vgl. Art. 3 Abs. 2 Richtlinie 2019/1024/EU.

[49] ErwG 26 Richtlinie 2019/1024/EU.

[50] Vgl. Art. 3 Richtlinie 2019/1024/EU.

[51] Art. 4 Abs. 3 Richtlinie 2019/1024/EU.

ser Begründungspflicht und den anderen Vorgaben über die Bearbeitung von Anträgen auf Weiterverwendung des Art. 4 Richtlinie 2019/1024/EU müssen öffentliche Unternehmen sowie „Bildungseinrichtungen, Forschungseinrichtungen und Forschungsförderungseinrichtungen“ nicht entsprechen.[52] Interessant ist in diesem Zusammenhang die Frage, welche Entscheidungspraxis sich in den Mitgliedstaaten in Bezug auf Kriterien für eine positive oder negative Bescheidung eines Antrags auf Weiterverarbeitung im Verhältnis zu bestehenden Zugangsrechten etabliert.

Die Bearbeitung eines Antrages umfasst auch Fragen bezüglich etwaiger Lizenzen, darunter die Frist zur endgültigen Unterbreitung eines Lizenzangebotes.[53] Welche Regeln hinsichtlich Anträgen auf Weitergabe für öffentliche Unternehmen gelten ist offen (Buchholz 2019, S. 200).

Auch sollen Daten von öffentlichen Stellen bereits „konzeptionell und standardmäßig offen (open by design and by default)“[54] erstellt und zur Verfügung gestellt werden. Zwar wird in der Richtlinie auch die Möglichkeit der Weiterverwendung ohne bestimmte Bedingungen in Bezug auf Dokumente erwähnt, ein Lizenzmodell wird in bestimmten Fällen jedoch nicht ausgeschlossen. Lizenzbedingungen können unter anderem für die Haftung des Lizenznehmers bei Weiterverwendung von Dokumenten oder den Schutz von personenbezogenen Daten denkbar sein.[55] Art. 8 der Richtlinie 2019/1024/EU regelt sogenannte „Standardlizenzen“ und setzt Regeln für ihre Ausgestaltung fest. Wie solche Lizenzen in Zukunft konkret ausgestaltet werden, ist aktuell jedoch noch offen.

Ferner wird geregelt, ob für die Weiterverwendung von Dokumenten Gebühren oder Entgelte bezahlt werden müssen. Grundsätzlich soll die Weiterverwendung von Dokumenten kostenfrei sein.[56] Dieser Grundsatz hat den Hintergrund, dass Start-ups und kleine und mittlere Unternehmen ansonsten einer nicht unerheblichen Markteintrittsschranke unterliegen würden, sollten solche erhoben werden.[57] Davon unberührt bleibt jedoch eine Erstattung von Grenzkosten, die zum Beispiel durch die Bereitstellung von Dokumenten oder durch das Anonymisieren von personenbezogenen Daten in Dokumenten entstehen können.[58]

Unter bestimmten Voraussetzungen können jedoch öffentlichen Unternehmen, Bibliotheken (einschließlich Hochschulbibliotheken), Museen und Archive sowie öffentliche Stellen, deren Auftrag das Erzielen von Einnahmen erfordert, um einen wesentlichen Teil ihrer Kosten im Zusammenhang mit der Erfüllung ihrer öffentlichen Aufträge zu decken, eine Erstattung der Gesamtkosten verlangen.[59] Es obliegt den jeweiligen Mitgliedstaaten,

[52] Art. 4 Abs. 6 Richtlinie 2019/1024/EU.

[53] Art. 4 Abs. 1 und 2 Richtlinie 2019/1024/EU.

[54] Vgl. Art. 5 Abs. 2 Richtlinie 2019/1024/EU.

[55] Vgl. ErwG 44 Richtlinie 2019/1024/EU.

[56] Vgl. Art. 6 Abs. 1 Richtlinie 2019/1024/EU.

[57] Vgl. ErwG 36 Richtlinie 2019/1024/EU.

[58] Vgl. Art. 6 Abs. 1 Richtlinie 2019/1024/EU.

[59] Vgl. Art. 6 Abs. 2 lit. a, b und c Richtlinie 2019/1024/EU.

Kriterien für die Berechnung der „Gesamtkosten“ festzulegen; insoweit gibt die Richtlinie 2019/1024/EU hinsichtlich der Höhe der Gesamteinnahmen einen Rahmen vor, wobei auch eine „angemessene Gewinnspanne“ erfasst sein darf.[60]

Da eine europäische Richtlinie im Gegensatz zu einer europäischen Verordnung keine unmittelbare Anwendung findet, müssen die in der Richtlinie festgelegten Ziele erst durch den nationalen Gesetzgeber in nationales Recht umgesetzt werden. Die Umsetzungsfrist für die Richtlinie 2019/1024/EU läuft bis zum 17. Juli 2021.[61]

Auch wenn durch die Richtlinie 2019/1024/EU keine originären Zugangsrechte zu Daten geschaffen werden, ist dennoch eine positive Auswirkung auf den Markt für KI-Lösungen zu erwarten, da die Ansprüche auf Weiterverwendung – ein Zugangsrecht vorausgesetzt – den Weg für das „Training“ der KI-Lösung mit bereits vorhandenen und kostengünstigen Daten ermöglichen.

Literatur

AI4EU (o. J.). https://www.ai4eu.eu/. Zugegriffen am 07.01.2020

Buchholz W (2019) Die neue PSI-Richtlinie – Wieviel Datenhoheit verbleibt den öffentlichen Unternehmen? IR 2019:197–201

Craglia M (ed), Annoni A, Benczur P, Bertoldi P, Delipetrev P, De Prato G, Feijoo C, Fernandez Macias E, Gomez E, Iglesias M, Junklewitz H, López Cobo M, Martens B, Nascimento S, Nativi S, Polvora A, Sanchez I, Tolan S, Tuomi I, Vesnic Alujevic L (2018) Artificial Intelligence – a European perspective. https://publications.jrc.ec.europa.eu/repository/handle/JRC113826. Zugegriffen am 15.01.2020

Europäische Investitionsbank (o. J.) Wer kann Finanzierungen aus dem EFSI beantragen? https://www.eib.org/de/efsi/how-does-a-project-get-efsi-financing/index.htm. Zugegriffen am 26.03.2020

Europäische Kommission (2018a) Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Künstliche Intelligenz für Europa (COM(2018)137 final). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=COM%3A2018%3A237%3AFIN. Zugegriffen am 08.01.2020

Europäische Kommission (2018b) ANHANG der Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence. Zugegriffen am 10.01.2020

Europäische Kommission (2018c) Mitteilung der Kommission an das Europäische Parlament und den Rat – Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nichtpersonenbezogener Daten in der Europäischen Union (COM(2019) 250 final). https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52019DC0250&from=EN. Zugegriffen am 06.04.2020

Europäische Kommission (2019a) EU investiert 35 Millionen Euro in KI-Anwendungen zur Krebsprävention und -behandlung. https://ec.europa.eu/commission/presscorner/detail/en/MEX_19_3970. Zugegriffen am 07.01.2020

[60] Vgl. Art. 6 Abs. 4 Richtlinie 2019/1024/EU.

[61] Vgl. Art. 17 Richtlinie 2019/1024/EU.

Europäische Kommission (2019b) EU investiert 50 Millionen Euro in Exzellenzzentren für künstliche Intelligenz. https://ec.europa.eu/commission/presscorner/detail/en/MEX_19_4069. Zugegriffen am 07.01.2020

Europäische Kommission (2020a) White paper on Artificial Intelligence – a European approach to excellence and trust. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. Zugegriffen am 26.03.2020

Europäische Kommission (2020b) Mitteilung der Kommission „Shaping Europe's digital future". https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf. Zugegriffen am 26.03.2020

Europäische Kommission (o. J.-a) Factsheet Digital Europe Programme. https://ec.europa.eu/digital-single-market/en/news/digital-europe-programme-proposed-eu92-billion-funding-2021-2027. Zugegriffen am 26.03.2020

Europäische Kommission (o. J.-b) What is Horizon 2020? https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020. Zugegriffen am 26.03.2020

Europäische Kommission (o. J.-c) Factsheet Horizon Europe. https://ec.europa.eu/info/sites/info/files/research_and_innovation/knowledge_publications_tools_and_data/documents/ec_rtd_factsheet-horizon-europe_2019.pdf. Zugegriffen am 26.03.2020

Europäische Kommission (o. J.-d) The InvestEU programme – legal texts and factsheets. https://ec.europa.eu/commission/publications/investeu-programme_en. Zugegriffen am 26.03.2020

Europäische Kommission (o. J.-e) Multiannual financial framework: shaping EU expenditure. https://www.consilium.europa.eu/en/policies/eu-budgetary-system/multiannual-financial-framework/. Zugegriffen am 26.03.2020

Europäische Parlament (2017) Entschließung mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL), 2018 C 252/25). http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_DE.html. Zugegriffen am 29.01.2020

Europäischer Investitionsfond (o. J.) Who we are. https://www.eif.org/who_we_are/index.htm. Zugegriffen am 21.01.2020

Hagemeier S (2019) In: Ahlberg H, Götting H-P (Hrsg) Beck OK Urheberrecht, Teil 1 Urheberrecht, § 69d Ausnahmen von den zustimmungsbedürftigen Handlungen. C.H. Beck, München, S 26

HEG-KI (2019a) Ethik-Leitlinien für eine vertrauenswürdige KI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Zugegriffen am 17.01.2020

HEG-KI (2019b) KI-Politik- und Investitionsempfehlungen. https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence. Zugegriffen am 17.01.2020

Holder C (ed), Iglesias M (ed), Triaille J-P, Van Gysegnem J-M (2019) Legal and regulatory implications of Artificial Intelligence. The case of autonomous vehicles, m-health and data mining. https://publications.jrc.ec.europa.eu/repository/handle/JRC116235. Zugegriffen am 14.01.2020

Iglesias M, Shamuilia S, Anderberg A (2019) Intellectual property and Artificial Intelligence – a literature review. https://publications.jrc.ec.europa.eu/repository/handle/JRC119102. Zugegriffen am 21.01.2020

Katzenmeier C (2019) Digitalisierung des Gesundheitswesens – Herausforderung des Rechts. MedR 2019:259–271

Klar M, Kühling J (2018) In: Kühling J, Buchner B (Hrsg) Datenschutz-Grundverordnung/BDSG 2, Art. 4 Nr. 1 personenbezogene Daten (inkl. Betroffene Person). C.H. Beck, München

Mitgliedstaaten (2018) Erklärung über die Kooperation in Bezug auf KI. https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence. Zugegriffen am 08.01.2020

Mitterer K, Wiedemann M, Thress K (2020) BB-Gesetzgebungs- und Rechtsprechungsreport zu Industrie 4.0 und Digitalisierung 2019. BB 2020:3–20

Nationale Kontaktstelle IKT (o. J.) Horizont 2020. https://www.nks-ikt.de/de/Horizont-2020.php. Zugegriffen am 21.01.2020

Nativi S, Gómez Losada A (2019) Artificial Intelligence at the JRC. https://publications.jrc.ec.europa.eu/repository/handle/JRC117232. Zugegriffen am 06.04.2020

Spindler G, Sein K (2019a) Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen – Anwendungsbereich und grundsätzliche Ansätze. MMR 2019:415–420

Spindler G, Sein K (2019b) Die Richtlinie über Verträge über digitale Inhalte – Gewährleistung, Haftung und Änderungen. MMR 2019:488–493

Steinbrecher J (2019) Die EU-Urheberrechtsrichtlinie aus Sicht der Digitalwirtschaft – Zeit für Augenmaß und faktenbasierte Gesetzgebung. MMR 2019:639–643

Thum D (2019) In: Wandtke A-A, Bullinger W (Hrsg) Praxiskommentar Urheberrecht, Gesetz über Urheberrecht und verwandte Schutzrechte (Urgeberrechtsgesetz), Teil 1 Urheberrecht, § 7 Urheber, 5. Aufl. C.H. Beck, München

Tuomi I (2018) The impact of Artificial Intelligence on learning, teaching, and education – policies for the future. https://ec.europa.eu/jrc/en/publication/impact-artificial-intelligence-learning-teaching-and-education. Zugegriffen am 06.04.2020

Bericht der Expertengruppe „Liability and New Technologies“ zu Haftungsfragen in Bezug auf KI

11

Johannes Graf Ballestrem

Zusammenfassung

In diesem Kapitel wird der Expertenbericht der Expert Group on Liability and New Technologies vorgestellt. In diesem, 2019 erschienenen Paper bezieht die Expertengruppe Stellung zu Haftungs- und Regulierungskonzepten von KI, die in der Wissenschaft teilweise bereits diskutiert wurden und stellt eigens entwickelte Konzepte vor. Einer Analyse der sich eröffnenden rechtlichen und tatsächlichen Problemfelder folgt eine Anzahl konkreter Regelungsvorschläge wie bspw. die Einführung einer Beweislastumkehr zu Gunsten der Endnutzer einer KI-Anwendung oder die Etablierung von Gefährdungshaftungsregimen.

Einen Ausblick, in welche Richtung sich das Haftungsregime in Bezug auf KI auf europäischer Ebene zukünftig entwickeln könnte, gibt der Bericht der Expertengruppe „Liability and New Technologies“ zu Haftungsfragen in Bezug auf KI. Die „**Expert Group on Liability and New Technologies**“ (**NTF**) berät die EU-Kommission bezüglich der Anwendbarkeit der Produkthaftungsrichtlinie auf traditionelle Produkte, neue Technologien und neue gesellschaftliche Herausforderungen und unterstützt sie bei der Entwicklung von Grundsätzen, die als Leitlinien für mögliche Anpassungen der geltenden Gesetze dienen können.[1] Ursprung ist eine Resolution des EU-Parlaments (2017), mit der die Kommission

[1] P8_TA(2017)0051.

J. G. Ballestrem (✉)
Osborne Clarke, Köln, Deutschland
E-Mail: johannes.ballestrem@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_11

aufgefordert wurde, konkrete Vorschläge zur Regulierung der Haftung für den Einsatz von KI zu machen. Die Expertengruppe hat sich mit der Aufgabenstellung auseinandergesetzt, „ob und in welchem Umfang bestehende Haftungsregime an die entstehenden Marktgegebenheiten, die aus der Entwicklung von Künstlicher Intelligenz, fortgeschrittener Robotertechnik, dem Internet of Things sowie Problemen der Cybersecurity folgen, angepasst sind“. Dabei war die Expertengruppe aufgefordert, wo notwendig, Vorschläge zu Änderungen und Anpassungen zu machen (NTF 2019, S. 13; Europäische Kommission 2018, S. 4– 6). Die wesentlichen Ergebnisse des Berichts zur Liability for Artificial Intelligence: Auf EU-Ebene ist derzeit nur die Produkthaftung als Gefährdungshaftungsregime harmonisiert. Zugleich liegt das Einsatzfeld von KI regelmäßig (auch) im Anwendungsbereich der Produkthaftungsrichtlinie. Nationale Haftungsregime spielen insoweit eine eher untergeordnete Rolle und werden im Bericht entsprechend generalisierend behandelt. Die Expertenkommission stellt eine Reihe von Vorschlägen auf, die sie für notwendig erachtet, um den wachsenden Herausforderungen des Einsatzes aufstrebender digitaler Technologien wie KI haftungsrechtlich zu genügen. Soweit die folgenden Abschnitte deutsches Recht behandeln, erfolgt dies durch die Verfasser, da die Expertengruppe keine einzelnen Rechtsordnungen hervorhebt.

11.1 Die wichtigsten Erkenntnisse der Expertengruppe

11.1.1 Keine eigene Rechtspersönlichkeit

Die Expertengruppe erachtet es nicht als notwendig, dass KI mit einer Rechtspersönlichkeit ausgestattet wird. Dies sei für Fragen der Haftung nicht notwendig und eröffne nur eine Vielzahl an legislativ zu regelnden Problematiken, ohne sich als effektivere Maßnahme, verglichen mit einer Erweiterung der Zurechnung jeglichen Verhaltens zu den derzeit bestehenden rechtlichen Personenformen, zu erweisen. Dies gelte ausdrücklich jedoch nur für den untersuchten Bereich der Haftung und nicht für Rechtsgebiete wie das Vertragsrecht (NTF 2019, S. 37–38).

11.1.2 Gefährdungshaftung des Betreibers

Für neue digitale Technologien schlägt die Expertenkommission vor, dass deren Anwender einer Gefährdungshaftung unterliegen sollten, sofern die Technologien typischerweise als risikoreich eingestuft und in öffentlichen Räumen eingesetzt werden. Damit löst sie sich bewusst von den gängigen Erscheinungsformen der Gefährdungshaftung, die entweder den Eigentümer, den Benutzer, oder auch den Produzenten treffen kann und entwickelt einen sogenannten „Betreiberbegriff“. Betreiber soll sein, wer die Kontrolle über die Risiken der Verwendung einer Technologie ausübt und wer von deren Verwendung profitiert. Unterschieden wird dabei zwischen „backend“ und „frontend“ Betreiber. „Frontend“

Betreiber soll sein, wer hauptsächlich über den Einsatz einer Technologie entscheidet und von dieser profitiert. „Backend“ Betreiber, wer durchgehend dafür verantwortlich ist, die Funktionen und Eigenschaften einer Technologie zu entwickeln und im Hintergrund den Support übernimmt. Letzterer wird sich mit dem bekannten Produzentenbegriff schneiden. Da das Kriterium des Profits schwer festzustellen sein wird, soll im Fall mehrerer Betreiber denjenigen eine Gefährdungshaftung treffen, der die größere Kontrolle über die Risiken der Technologie hält. Wenn die bestehenden Gefährdungshaftungsregime in den Mitgliedsstaaten auf den Einsatz von KI oder neuen digitalen Technologien angewandt werden, so empfiehlt die Expertengruppe explizit, dass die bisher gegebenen Verteidigungsmöglichkeiten des Haftungssubjekts daraufhin überdacht werden, dass sie originär für menschliche Akteure entwickelt wurden und somit nicht zwingend auch auf KI-Lösungen anwendbar sind. Gemeint sind beispielsweise die Ausnahmen eines unabwendbaren Ereignisses im Straßenverkehr im deutschen Recht, bzw. die Haftungsausnahme für den Fall, dass ein, mit entsprechenden Fähigkeiten ausgestatteter Idealfahrer[2] den Verkehrsunfall ebenfalls nicht hätte verhindern können (NTF 2019, S. 39–42).

11.1.3 Gefährdungshaftung des Produzenten

Die Expertenkommission sieht die Produkthaftung als zentrales Element bei der Kompensation durch digitale Produkte verursachter Schäden. Sie erachtet es für notwendig, dass der Produzent auch dann haftet, wenn ein Defekt erst auftritt, nachdem das Produkt in den Verkehr gebracht wurde, solange er noch über Updates oder Upgrades die Technologie kontrolliert.[3] Dahinter steht die Erwägung, dass viele moderne (physische) Produkte nur mit einwandfreier, ständig angepasster, moderner Software funktionieren und ein Defekt der geupdateten oder geupgradeten Software einem Defekt des Produkts gleichkommt. Zudem soll die Berufung darauf, dass das Produkt zum Zeitpunkt des Inverkehrbringens dem Stand der Wissenschaft und Technik entsprach, nicht möglich sein.[4] Grundsätzlich steht dahinter die Annahme, dass die Rolle, die physische Produkte zum Zeitpunkt des Erlasses der Produkthaftungsrichtlinie spielten, mittlerweile durch digitale Produkte eingenommen wird. Zusätzlich sieht sie eine Beweislastumkehr hinsichtlich des Nachweises eines Fehlers/Defekts in Fällen vor, in denen es unverhältnismäßig aufwändig und kostenintensiv wäre, dem Produzenten nachweisen zu müssen, an welche Standards er sich hätte halten müssen, bzw. dass er dies nicht getan hat (NTF 2019, S. 42–44).

---

[2] So wird sich durch den Einsatz von KI der Teil der Definition, der ein Ereignis verlangt, dass durch (…) geistesgegenwärtiges Handeln im Rahmen des „Menschenmöglichen“ nicht hätte verhindert werden können (vgl. OLG Köln 20. Oktober 1993, VersR 1994, 57) nicht halten können.

[3] Dies weicht von § 1 Abs. 2 Nr. 2 ProdhG ab, welches die Produkthaftungsrichtlinie in Deutschland umsetzt.

[4] Dies weicht von § 1 Abs. 2 Nr. 5 ProdhG ab, welches die Produkthaftungsrichtlinie in Deutschland umsetzt.

11.1.4 Verkehrssicherungspflichten im Rahmen der Verschuldenshaftung

Neben einer Gefährdungshaftung sollte den Betreiber, sowie den Produzenten auch im Rahmen der Verschuldenshaftung eine Haftung treffen. Die Expertengruppe geht auf bestimme Überwachungs-, Wartungs- und Auswahlpflichten, etc. ein, stellt jedoch auch fest, dass diese in den meisten Mitgliedsstaaten derzeit schon sehr differenziert von der Rechtsprechung ausgearbeitet worden sind (in Deutschland durch das Institut der Produzentenhaftung im Rahmen des § 823 Abs. 1 BGB) und weist nur darauf hin, dass diese auch beim Einsatz von KI weiterhin eine prominente Rolle spielen werden (NTF 2019, S. 44–45).

11.1.5 Haftung für fremdes bzw. autonomes Verschulden

Wird eine Technologie eingesetzt, die einen gewissen Grad an Autonomie innehat, so soll die Haftung des Betreibers einer Haftung für den Fall, dass er sich einer natürlichen Person bedient hätte, nicht nachstehen. Die Expertengruppe führt dabei das Risiko an, dass sich ein Unternehmen einer KI bedient und dadurch besser steht als wenn es sich einer natürlichen Person bedient hätte. Sie geht auf die Problematik ein, dass viele nationale Haftungsregime ein gewisses Anknüpfungsfehlverhalten der zuzurechnenden Person voraussetzen. So setzt bspw. § 831 BGB voraus, dass ein Verrichtungsgehilfe deliktisch tätig wird. Die Frage, wann bspw. eine KI sich entsprechend deliktisch verhält, konnte die Expertengruppe nicht abschließend klären. Der Ansatz, den Maßstab auf die KI anzuwenden, der auch für einen eingesetzten Menschen gilt, wurde als der Überzeugendste angesehen. Abweichend davon soll, sobald es KI gibt, die bessere Ergebnisse erzielt als Menschen, diese den Maßstab für ein Fehlverhalten bilden. Ebenfalls auf den Einsatz von autonomen Systemen angewandt werden sollen die bestehenden rechtlichen Regelungen zum Auswahlverschulden auf Seiten der die KI einsetzenden (juristischen oder natürlichen) Person (NTF 2019, S. 45–46).

11.1.6 Überwachungs- und Protokollierungspflichten

Der Bericht erkennt die Möglichkeit digitaler Technologien, ihre Verwendung und internen Abläufe dokumentieren zu können, als Vorteil bei der Analyse der Fehlerquellen und damit auch der Aufbereitung von Schadensfällen und deren Regulierung an. Technologie sollte ihrer Ansicht nach ab Werk, mit entsprechenden Protokollierungsmodulen ausgestattet werden. Diese sollten typischerweise den Nachweis ermöglichen, ob sich ein, der Technologie innewohnendes, Risiko verwirklicht hat und sich im zumutbaren und zulässigen Rahmen bewegen. Letzteren legt die Expertengruppe durch eine Vielzahl von Kriterien fest, zu denen die technische Durchführbarkeit, die Kosten, das Bestehen von Alter-

nativen zur Beweisfindung, die Größenordnung des der Technologie innewohnenden Risikos, sowie die Beeinträchtigung der Rechte Dritter durch die Dokumentation, gehören. Fehlen die protokollierten Daten oder werden diese nicht offengelegt, soll dies zu der widerlegbaren Vermutung führen, dass die jeweilige nachzuweisende Haftungsvoraussetzung erfüllt ist (NTF 2019, S. 47–48).

11.1.7 Sicherheitsbestimmungen und Beweislastumkehr

Um die Umsetzung von Cybersecurity-Regelungen zu unterstützen und Konsumenten davor zu schützen, dass ein fehlerhaftes oder unsicheres digitales Produkt, weiteren, größeren Schaden in dessen digitaler Umgebung anrichtet, rät die Expertengruppe zu weiteren Regelungen zur Beweiserleichterung und/oder Beweislastumkehr. Wenn sich Schäden innerhalb des Schutzzweckes einer gesetzlichen (nicht: Verkehrsplicht, siehe hierzu unter: Abschn. 11.1.9) Sicherheitsnorm realisieren, soll eine Pflichtverletzung der Verkehrspflicht dazu führen, dass die Beweislast hinsichtlich (i) Ursächlichkeit, (ii) Verschulden, (iii) sowie Nachweis eines Schadens beim Schädiger liegt (NTF 2019, S. 48–49).

11.1.8 Beweiserleichterung hinsichtlich Kausalität

Wie auch sonst hat grundsätzlich der Geschädigte die kausale Verursachung seines Schadens durch den Schädiger nachzuweisen. Die folgenden Faktoren sollen jedoch, als Ergebnis einer Abwägung, Beweiserleichterungen nach sich ziehen können: (i) die Wahrscheinlichkeit, dass die verwendete Technologie den Schaden zumindest gefördert hat; (ii) die Wahrscheinlichkeit, dass der Schaden durch die verwendete Technologie verursacht wurde; (iii) das bekannte Fehlerrisiko der Technologie, auch ohne dass die konkrete Kausalität nachgewiesen wurde; (iv) die Verständlichkeit und ex-post Rückverfolgbarkeit von Prozessen innerhalb der eingesetzten Technologie, die möglicherweise für den Schaden ursächlich waren; (v) die Verfügbarkeit und ex-post Nachvollziehbarkeit von Daten innerhalb der eingesetzten Technologie; (vi) die Schwere des potenziell möglichen sowie des tatsächlich entstandenen Schadens. Die verschiedenen nationalen Prozessordnungen, so auch die deutsche, kennen derartige Beweiserleichterungen bereits in den verschiedensten Formen. Die Expertengruppe erkennt dies an und hält ihren Vorschlag daher bewusst abstrakt und offen für nationale rechtliche Besonderheiten. Wie die Beweiserleichterungen in den beschriebenen Fällen konkret umgesetzt werden sollen, lässt sie daher offen (NTF 2019, S. 49–52).

11.1.9 Beweislastumkehr hinsichtlich Pflichtverletzung und Verschulden

Ist erwiesen, dass ein Schaden durch die Verwendung einer digitalen Technologie verursacht wurde und hängt die Haftung davon ab, ob Vorsatz oder Fahrlässigkeit nachgewiesen werden können, so soll die Beweislast dann umgekehrt werden, wenn unverhältnismäßige Schwierigkeiten und Kosten damit verbunden sind, eine entsprechende Pflicht des Schädigers festzustellen oder eine Verletzung einer solchen Pflicht nachzuweisen. Gleiches soll hinsichtlich des Nachweis des Verschuldens, also in den meisten Fällen eines fahrlässigen Verhaltens des Schädigers gelten. Begründet wird dies damit, dass es im Rahmen des Einsatzes neuer digitaler Technologien, wie KI, oft noch keine standardisierten Verkehrspflichten gibt, deren Verletzung nachgewiesen werden kann. So wird es für einen Geschädigten nahezu unmöglich sein, nachzuweisen, wie die Eingabe eines bestimmten Datensatzes in einen KI-betriebenen Prozess dazu führen konnte, dass dieser fehlerhaft verlief. Noch schwieriger wird jedoch sein, einen Standard nachzuweisen, an dem sich der Betreiber bei der Dateneingabe hätte orientieren sollen. Ein solcher ist nämlich notwendige Voraussetzung für die Annahme einer Pflichtverletzung, wenn keine normativ festgelegten Verkehrspflichten bestehen (NTF 2019, S. 52–55). Inwieweit diese Vorschläge die deutsche Rechtslage zur deliktischen Produzentenhaftung nach § 823 Abs. 1 BGB verändern würden, bliebe abzuwarten, da bereits ausgiebige Beweiserleichterungen im deutschen Recht bestehen.

11.1.10 Mitverschulden

Die Expertengruppe stellt fest, dass sämtliche vorgeschlagenen Haftungsregelungen auch in der Opfersphäre Anwendungen finden sollen, wenn es darum geht in welcher Höhe der eigene Anspruch auf Grund eines Mitverschuldens (§ 254 BGB) zu kürzen ist (NTF 2019, S. 55).

11.1.11 Gesamtschuldnerische Haftung in technischen Gewerbe- / Geschäftseinheiten

Als eine der größeren Herausforderungen auf Seiten der Geschädigten sieht der Bericht den Nachweis an, welcher Teil eines komplexen digitalen Ökosystems für den Schaden verantwortlich ist. Diese verhärtet sich, wenn verschiedene Elemente einer Anwendung von verschiedenen Betreibern oder Herstellern stammen. Um ineffiziente Schadensregulierung durch eine hohe Unsicherheit, die falsche Partei in Anspruch zu nehmen, zu verhindern, schlägt der Bericht die Bildung von sog. kommerziellen und technischen Einheiten vor. Ob eine solche kommerzielle und technische Einheit vorliegt, soll danach bestimmt werden, ob (i) ein gemeinsames oder koordiniertes Marketing der verschiedenen Elemente

stattfindet, (ii) inwieweit die Elemente technisch voneinander abhängig sind und zusammenarbeiten, und (iii) dem Level an Exklusivität oder Spezifität der konkreten Kombination. Solche Einheiten sollen dann, wenn sie verschiedene Elemente einer einheitlichen Leistung bereitstellen, im Außenverhältnis als Gesamtschuldner haften, wenn der Geschädigte nachweisen kann, dass wenigstens ein Element für den Schaden verantwortlich ist, er aber nicht bestimmen kann, in wessen Sphäre dieses liegt und unter wessen Kontrolle dieses stand. Das Risiko, das mit einer, meist wirtschaftlich motivierten, Aufgabenteilung und der stetigen Verknüpfung verschiedener Betreiberdienste einhergeht, soll nicht beim Benutzer liegen, wenn ein ähnlicher Service auch von nur einem Betreiber hätte erbracht werden könnte (NTF 2019, S. 55–57).

11.1.12 Entschädigung zwischen mehreren Schädigern

Grundsätzlich soll, wie auch die aktuelle Rechtslage in Deutschland es vorsieht, jeder Schädiger im Innenverhältnis zwischen mehreren Schädigern nur entsprechend seines Beitrags einstehen. Liegt jedoch eine technische und kommerzielle Einheit vor (s. o. unter Abschn. 11.1.11), soll deren gesamtschuldnerische Haftung jedoch auch gegenüber anderen Schädigern im Innenverhältnis gelten (NTF 2019, S. 57–58).

11.1.13 Beschädigung von Daten

Mit dem Aufschwung digitaler Technologien ändert sich aus Sicht der Expertenkommission auch die Relevanz von Schäden an Daten. Eine Begrenzung des Schadensbegriffes auf die körperliche, greifbare Welt sei nicht länger zeitgemäß. Vorgeschlagen werden daher Anpassungen im Deliktsrecht, neben der in den meisten Mitgliedsstaaten gut funktionierenden vertraglichen Haftung, wenn es zu Vermögensschäden durch die Beschädigung von Datensätzen kommt. Die Haftung sollte ergänzt werden, wenn in das Eigentumsrecht an dem datentragenden Medium eingegriffen wurde oder dieses Medium anderweitigen deliktischen Schutz (in Deutschland bspw. Besitz, das Recht am eingerichteten und ausgeübten Gewerbebetrieb, etc.) erfährt, die in den meisten Mitgliedsstaaten besteht. Das Gremium schlägt hierfür eine deliktische Haftung vor, wenn Strafnormen verletzt wurden (bspw. Die Budapest Convention on Cybercrime), deren Schutzzweck in der Vermeidung derartiger Schäden liegt. Als Muster für eine solche Haftung wird Art. 82 DS-GVO angeführt. Hier ist eine Entschädigung zu zahlen, wenn der Schaden aus einer Verletzung von Vorschriften der DS-GVO resultiert. Solche spezifischen verhaltensbezogenen Haftungsregelungen zieht die Expertengruppe einer denkbaren allgemeinen Haftungsnorm bei Datenzugriffen vor. Sonst sei das Haftungsrisiko schlicht zu hoch. Abschließend wird noch die Haftung für vorsätzliche Schäden an Daten gefordert. In Deutschland ist diese Fallgruppe schon heute abgedeckt durch die Haftung wegen vorsätzlicher, sittenwidriger Schädigung gem. § 826 BGB, deren Rechtsfolge auch reine Vermögensschäden umfasst (NTF 2019, S. 59–60).

11.1.14 Pflichtversicherung

Die Sinnhaftigkeit einer Pflichtversicherung für neu entstehende Risiken digitaler Technologien hängt nach Meinung der Expertengruppe von zwei Hauptvariablen ab: Der Häufigkeit mit der sich erhebliche Schäden realisieren einerseits sowie der Wahrscheinlichkeit, dass eine individuelle Entschädigung überhaupt möglich ist, andererseits. Ist erstere hoch und letztere niedrig, ist eine Pflichtversicherung für Betreiber ein adäquates legislatives Mittel. Die Expertengruppe betont jedoch, dass eine Versicherungspflicht, gerade für schwer einzuschätzende Technologien, für die keine Erfahrungswerte bestehen, zu Problemen führen kann. In Fällen, in denen keine Versicherungen für unkalkulierbare Risiken angeboten werden, könne dies dazu führen, dass die Technologie nicht eingesetzt werde. Dem könne wiederum mit einer Höchsthaftungssumme für bestimme Haftungsrisiken entgegengewirkt werden. Denkbar seien auch andere finanzielle Absicherungen, die nicht notwendig Versicherungen sein müssen (NTF 2019, S. 61–62).[5]

11.1.15 Kompensationsfonds

Zuletzt geht die Expertengruppe noch auf das Instrument der Kompensationsfonds ein. Diese sollen in Fällen, in denen mit regulatorischen Versicherungspflichten gearbeitet wird, flankierend wirken, indem die Öffentliche Hand Fonds bereithält, um Schäden durch nicht versicherte Technologie oder noch nicht bekannte Technologien abzusichern. Als Beispiel wird auf Art. 10 der Motor Insurance Directive abgestellt. Vorgeschlagen werden auch sog. Cybercrime-Fonds, die ähnlich eingreifen, wie bereits existierende staatliche Fonds, etwa für Fälle vorsätzlicher Gewalttaten, die eine gesundheitliche Schädigung hervorrufen (NTF 2019, S. 62–63).

Die Frage, ob die umfassende Hersteller-, bzw. Betreiberhaftung dahingehend ausgedehnt werden muss, dass sie bei Missachtung ethischer Grundsätze eingreift, lässt der Bericht offen. Insbesondere mit der Frage, ob der Fehlerbegriff aus der Produkthaftung um Faktoren wie einen diskriminierenden Output eines KI-Vorgangs erweitert werden sollte, setzt sich die Expertengruppe nicht ausdrücklich auseinander.[6]

11.2 Fazit

Der Bericht der Expertengruppe zu Haftungsfragen in Bezug auf KI führt fundierte Argumente für mögliche Änderungen des Haftungsregimes auf EU-Ebene an. Ob und inwieweit diese tatsächlich seitens des europäischen Gesetzgebers aufgegriffen werden, bleibt abzuwarten. Insgesamt ist hier eher mit gesetzgeberischer Zurückhaltung zu rechnen. Für

[5] Unter Verweis auf Rubin (2016, S. 431–442).

[6] Zu dieser Fragestellung Pieper und Gehrmann (2019, S. 126).

Sie als Anbieter von KI-Lösungen oder Produkten, die KI beinhalten, ist es jedoch empfehlenswert, derartige Gesetzgebungstendenzen im Blick zu behalten. So können Sie das Risiko, zu einem späteren Zeitpunkt aufgrund von Gesetzesänderungen unter Umständen kostspielige Produktänderungen vornehmen zu müssen, so weit wie möglich minimieren. Grundsätzlich ist allerdings schon jetzt davon auszugehen, dass sowohl Hersteller als auch Betreiber größtmögliche Anstrengungen unternehmen um ausschließlich sichere Lösungen in den Markt zu bringen. Wo dies dennoch fehl schlägt greifen die etablierten Haftungskonzepte die inzwischen auch für mehr als 40 Jahre den zunehmenden Einsatz von Software begleitet haben ohne, dass es zu unvertretbaren Haftungsdefiziten gekommen ist.

Literatur

Europäische Kommission (2018) Commission Staff Working Document – Liability for emerging digital technologies, (COM(2018) 237 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0137&from=en. Zugegriffen am 26.02.2020

Expert Group on Liability and New Technologies – New Technologies Formation (2019) Liability for Artificial Intelligence – and other emerging digital technolo-gies. https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608. Zugegriffen am 26.02.2020

Pieper F-U, Gehrmann M (2019) Künstliche Intelligenz – Wer haftet? LR 2019:123–128. https://legal-revolution.com/images/pdf/Knstliche_Intelligenz_-_Wer_haftet.pdf. Zugegriffen am 26.02.2020

Rubin D (2016) Conclusions. In: Fenyves A, Kissling C, Perner S, Rubin D (Hrsg) Compulsory liability insurance from a European perspective. de Gruyter, Berlin, S 431–442

Fazit und Ausblick

12

Sabine von Oelffen und Ulrike Bär

Zusammenfassung

Ein Rückblick auf die in diesem Buch behandelten Themen zeigt, dass sich die in Zusammenhang mit dem Einsatz von KI-Lösungen aufkommenden Rechtsfragen bereits jetzt gut unter Rückgriff auf den bestehenden Rechtsrahmen lösen lassen. Die aktuell auf EU-Ebene stattfindende Evaluationsarbeit, inwieweit europäisch einheitliche Spezialregelungen für den Bereich KI notwendig sind, ist zur Schaffung von Vertrauen in KI, aber auch zur Schaffung von Rechtssicherheit essenziell.

In diesem Buch haben wir versucht, den Bogen zu schlagen von Einsatzfeldern für KI-Lösungen über rechtliche Fragen rund um den Zugang und die Kommerzialisierung von Daten als „Rohstoff" für KI-Lösungen bis hin zum rechtlichen Schutz der KI-Lösung selbst. Wie sie sehen, sind die rechtlichen Fragen rund um KI facettenreich und reichen vom Datenschutz über das gesamte Recht des geistigen Eigentums, das Wettbewerbs- und Kartellrecht bis hin zum Steuerrecht und allgemeinem Zivilrecht. Auf nationaler Ebene in Deutschland existieren bisher wenige Regelungen, die speziell den Einsatz von KI betreffen. Dennoch zeigt dieses Buch, dass unser deutsches Rechtssystem bereits heute Antworten auf die in Zusammenhang mit dem Einsatz von KI-Lösungen aufkommenden Rechtsfragen weiß. Es ist jedoch zu erwarten, dass die zunehmende Bedeutung von KI in der Wirtschaft, aber auch in der Medizin mittelfristig zu der ein oder anderen spezialgesetzlichen Regelung führen wird.

S. von Oelffen (✉) · UlrikeBär
Osborne Clarke, Köln, Deutschland
E-Mail: sabine.vonoelffen@osborneclarke.com; ulrike.baer@osborneclarke.com

J. G. Ballestrem et al., *Künstliche Intelligenz*,
https://doi.org/10.1007/978-3-658-30506-2_12

Positiv ist, dass aktuell sowohl auf nationaler als auch auf europäischer Ebene intensiv diskutiert wird, ob und in welchen Bereichen spezielle gesetzliche Regelungen für KI wirklich notwendig sind. Insgesamt zielt diese Diskussion darauf ab, die richtige Balance zu finden zwischen notwendiger Regulierung insbesondere zur Schaffung von Vertrauen in KI durch einen klar definierten rechtlichen Rahmen und der Wahrung ethischer Aspekte und der Vermeidung von Überregulierung, welche Entwicklung und Investitionen in KI hemmen würde. Das gilt im Grundsatz auch für das Steuerrecht und die schon seit einiger Zeit geführte internationale Diskussion um die Einführung einer „Digitalsteuer" bzw. einer „digitalen Betriebsstätte", wenngleich dabei eine gerechte Aufteilung der Besteuerungsrechte im Vordergrund steht. Vor diesem Hintergrund sind die zahlreichen Initiativen der EU, welche Ihnen in Kap. 10 und 11 vorgestellt wurden, zu begrüßen. Es ist wahrscheinlich, dass aus einigen dieser Initiativen konkrete Gesetzgebung auf europäischer Ebene erwächst. Wie aus den diversen Themenpapieren und Erwägungen in EU-Richtlinien und Verordnungen ersichtlich wird, dürften ethische Aspekte, der Zugang zu Daten und Fragen der rechtssicheren Nutzung von KI sowie Sonderregelungen für die Haftung für KI wesentliche Schwerpunkte einer zukünftigen EU-Gesetzgebung bilden. Europaweit einheitliche Regelungen in diesem Bereich sind absolut wünschenswert, da gerade KI keine Grenzen kennt und ein Flickenteppich unterschiedlicher nationaler Regelungen die Bedeutung der EU auf dem Weltmarkt in diesem Sektor klar schmälern dürfte.

Bis diese Thematik jedoch gesetzlich geregelt ist, kommt vertraglichen Vereinbarungen der betroffenen Stakeholder überragende Bedeutung zu. Im Übrigen sind die nicht immer auf den ersten Blick ersichtliche Anwendbarkeit gesetzlicher Schranken des Urheber-, Wettbewerbs- und Kartellrechts zu beachten und steuerrechtliche Implikationen rechtzeitig zu bedenken.