Rechtsfragen der Künstlichen Intelligenz

Datenkunst – Kunstdaten

Tobias Haar

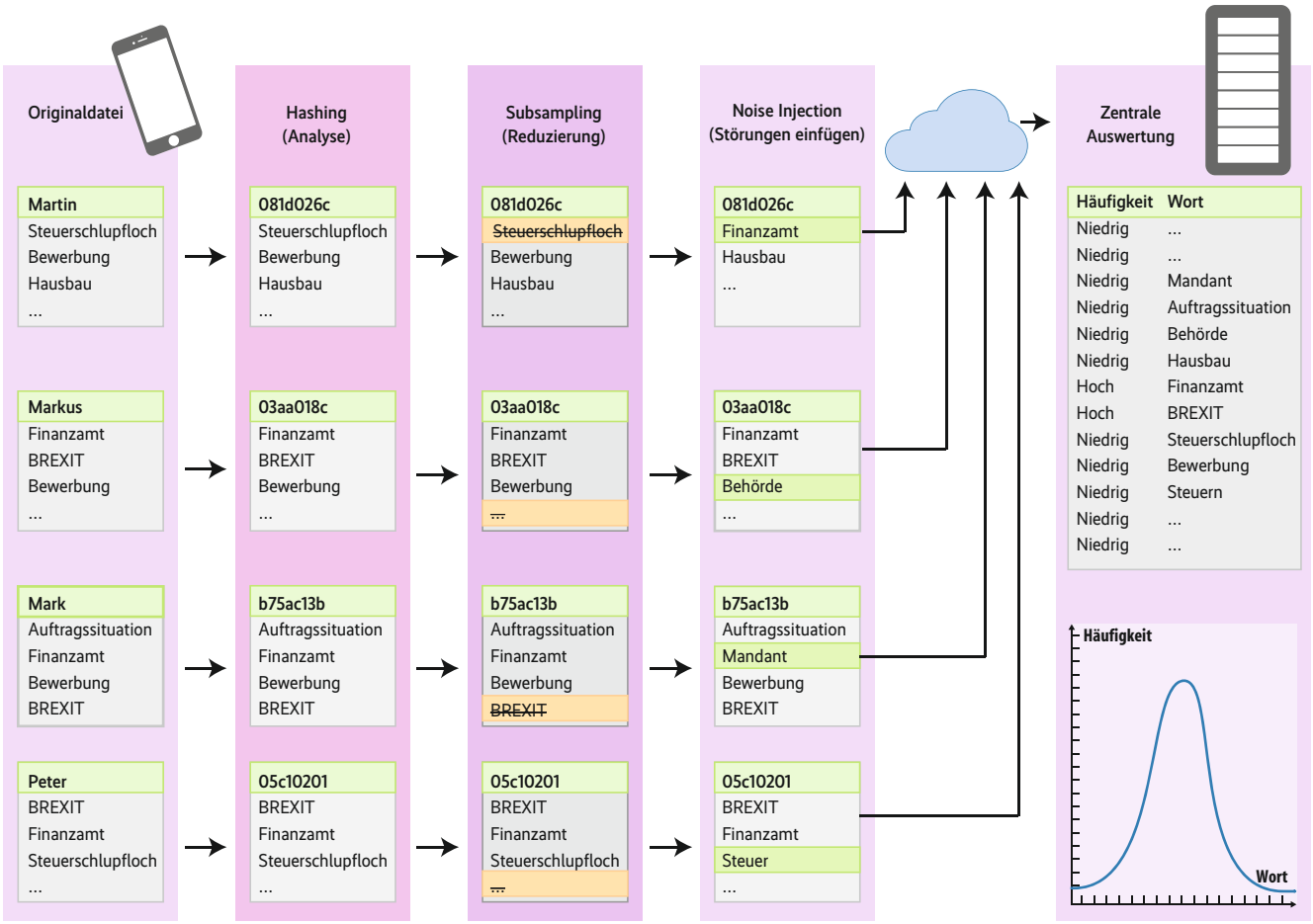
Künstliche Intelligenz und Machine Learning sind nicht nur in aller Munde, sondern kommen auch immer häufiger zum Einsatz. Neben dem Datenschutzrecht und Fragen der Haftung gibt es weitere relevante Rechtsgebiete. Anwender müssen sich auf dem Laufenden halten.

Eines der seit Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) kontrovers diskutierten Themen ist das Zusammenspiel zwischen dem, was man landläufig unter künstlicher Intelligenz versteht, und dem Datenschutzrecht. „Müssen sich Unternehmen in ihre Algorithmen schauen lassen?“ oder „Künstliche Intelligenz – Die Risiken für den Datenschutz“ [a, b] lauten nur zwei Überschriften von unzähligen Onlineartikeln zu diesem Thema. Wie in allen diesen Fällen kommt es zum einen darauf an, ob verarbeitete Daten tatsächlich einen Personenbezug haben, und zum anderen, wer sie wie und für welchen Zweck erhebt und verarbeitet.

Neben dem Datenschutz sind beim Einsatz von Künstlicher Intelligenz oder ihrem Teilgebiet, dem Machine Learning, weitere Rechtsfragen in der Diskussion. An erster Stelle steht hier die Haftung für Schäden, die von teilweise oder gänzlich autonomen Systemen verursacht wurden. Bedeutend ist auch die Frage nach der rechtlichen Schutzfähigkeit der Ergebnisse entsprechender Systeme. Besteht für autonom entwickelte Computerprogramme urheberrechtlicher Schutz? Sind Erfindungen patentierbar? Und was ist mit den durch sie geschaffenen Geschäftsgeheimnissen?

Für alle betroffenen Rechtsgebiete spielt es keine Rolle, ob neue Techniken, Verfahren und Geschäftsmodelle unter der Bezeichnung „Künstliche Intelligenz“ oder anderen Schlagwörtern diskutiert werden. Diesen Begriffen kommt juristisch keine Bedeutung zu, da sie (noch) nicht gesetzlich definiert sind. Es gilt der juristische Grundsatz, dass es nicht darauf ankommt, was auf der Verpackung einer Technologie draufsteht, sondern was im Detail enthalten ist. Die jeweiligen juristischen Grundlagen ergeben sich aus den geltenden Gesetzen und den darauf basierenden Gerichtsentscheidungen.

Wenn Künstliche Intelligenz oder ihr Teilbereich Deep Learning auf Big-Data-Analysen beruhen, ist der Datenschutz nicht weit. Es geht stets um große Datenmengen, die zu bestimmten Schlussfolgerungen führen sollen – sei es für von Menschen gesteuerte Anwendungen oder um „intelligente Maschinen“ in die Lage zu versetzen, eigenständig Entscheidungen in bestimmten Bereichen zu treffen. Selbst auf den ersten Blick reine Maschi-



So funktioniert Differential Privacy: Zuerst wird der Nutzername gehasht, dann durch Subsampling der Datensatz auf Stichproben reduziert. Mithilfe von Noise Injection werden die Daten so verfremdet, dass sie zwar noch statistisch auswertbar sind, sich aber keine verlässlichen Rückschlüsse auf einzelne Nutzer treffen lassen (Abb. 1).

nendaten können einen Personenbezug haben, wenn man von ihnen womöglich auf die Maschinen bedienenden Menschen oder die hinter einer Produktion stehenden Kunden schließen kann.

Personenbezogene Daten

Datenschutzrechtler fassen personenbezogene Daten sehr weit. Manche sprechen bereits davon, dass es angesichts der heutigen technischen Möglichkeiten gar keine nicht-personenbezogenen Daten mehr geben kann, denn jedes Datum könne mit anderen Daten kombiniert auf eine Person schließen lassen. Der objektive Datenbegriff bedeutet, dass ein Personenbezug auch dann vorliegt – und damit das Datenschutzrecht greift –, wenn irgendjemand aus einem Datum auf eine Person schließen kann. Ob der jeweilige Datenverarbeiter das kann, spielt danach keine Rolle.

Datenschutzrechtliche Probleme im Bereich Künstlicher Intelligenz ergeben sich beispielsweise aus Artikel 22 DSGVO. Dieser räumt den Betroffenen, um deren personenbezogene Daten es geht, das Recht ein, „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden“, die ihnen gegenüber „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. KI-Anwendungen, die diese Wirkungen haben, sind mit Personendaten nur zulässig, wenn sie Gegenstand eines Vertrags oder einer Einwilligung sind, die den datenschutzrechtlichen Vorgaben an Transparenz und Aufklärung genügen. Selbst bei vorliegender Einwilligung dürfen biometrische oder andere „besondere Kategorien personenbezogener Daten“ nicht für rein automatisierte Entscheidungen verwendet werden.

Risikofolgenabschätzung

Christopher Millard, Professor für Datenschutz- und Informationsrecht an der Queen Mary University in London, fordert eine vorherige Risikofolgenabschätzung [1], wenn auf Algorithmen basierende Systeme zur Analyse menschlichen Verhaltens eingesetzt werden. Das wäre beispielsweise beim Scoring zur Bonitätsprüfung erforderlich, für das zusätzliche datenschutzrechtliche Vorschriften existieren. Erst recht gilt es für Anwendungsfälle wie „Predictive Policing“ zur Berechnung der Wahrscheinlichkeit zukünftiger Straftaten. In diesem Bereich dürfte neben der DSGVO auch das jeweilige Polizei-, Ordnungs- und Strafrecht relevant sein. Das Beispiel der Risikobewertung bei Kreditkarteneinsätzen zeigt aber, dass KI-basierte „Predictive Fraud Prevention“ (Betrugsvermeidung durch Vorhersage) auch im privaten Sektor zunehmend eine Rolle spielt.

Schutz von Betriebs- und Geschäftsgeheimnissen

Ein Problem stellt sich allerdings bei der Risikofolgenabschätzung: KI-Systeme sollen selbstlernend sein und aus den jeweils neuen Erkenntnissen „eigene“ Entscheidungen oder Entscheidungsvorschläge ableiten. Das ist bei der Risikofolgenabschätzung nach der DSGVO deswegen zu berücksichtigen, da sich durch KI die Folgen der Datenverarbeitung für die Betroffenen mit der Zeit ändern können. Dann allerdings fordert das Gesetz eine erneute Risikofolgenabschätzung. Wie kurz die Intervalle zwischen zwei Abschätzungen aufgrund geänderter Risikolage sein sollen, bedarf einer Entscheidung im Einzelfall.

Das Aufklärungs- und Transparenzgebot im Datenschutzrecht findet aber dort seine Grenze, wo Betriebs- und Geschäftsgeheimnisse eines Unternehmens betroffen sind. Dass auch der Gesetzgeber Unternehmensgeheimnisse umfassend schützen will, zeigt sich in der 2016 in Kraft getretenen „EU-Geheimnisschutz-Richtlinie“, die derzeit von den EU-Mitgliedsstaaten umgesetzt wird.

Der Bundesgerichtshof hat im Jahr 2014 noch unter der alten Rechtslage entschieden, dass die Schufa ihre sogenannte Score-Formel für die Bonitätseinschätzungen nicht offenlegen muss (Az. VI ZR 156/13). Im Rahmen des datenschutzrechtlichen Auskunftsrechts muss das datenverarbeitende Unternehmen nicht angeben, welche „allgemeinen Rechengrößen wie etwa die herangezogenen statistischen Werte die Gewichtung einzelner Berechnungselemente bei der Ermittlung des Wahrscheinlichkeitswerts und die Bildung etwaiger Vergleichsgruppen als Grundlage der Scorekarten“ es verwendet.

Für den Einsatz „geheimer“ KI-Methoden dürfte nichts anderes gelten, denn die DSGVO ist auch verfassungsrechtlich auszulegen, und die Verfassung schützt Unternehmen und ihre Betriebs- und Geschäftsgeheimnisse, was bei der Abwägung zu berücksichtigen ist.

Problematisch ist es auch, wenn Unternehmen sich Künstliche Intelligenz von Dritten einkaufen, beispielsweise Watson von IBM. Manche sprechen hier von einer „Blackbox-KI“, da die eingesetzten Verfahren und Algorithmen nicht nur dem Betroffenen, sondern auch dem Verwender im Detail unbekannt sind. Dennoch muss der KI-Verwender aussagekräftige Informationen über die eingesetzte Logik offenlegen und das in klarer und verständlicher Sprache. Die Transparenzvorschriften in den Artikeln 13 ff. DSGVO betreffen nicht einseitig den Datenverwender, sondern gehen davon aus, dass im Einzelfall ein angemessener Ausgleich zwischen den widerstreitenden Interessen des Verbrauchers und seinem Recht auf „faire und transparente Verarbeitung“ und denen des Verantwortlichen gefunden werden muss.

Nachvollziehbarkeit

Der Anspruch endet zudem dort, wo er mit einem „unverhältnismäßigen Aufwand“ verbunden wäre und wenn durch eine Datenauskunft die „Rechte und Freiheiten anderer Personen“ beeinträchtigt werden. KI-Anwender sollten sich stets darüber klar sein, welche Informationen sie den Betroffenen zur Verfügung stellen müssen, und sich eine gute Argumentation zurechtlegen, wenn sie Details der dahinterliegenden KI nicht offenbaren wollen.

IBM hat jüngst reagiert und mehr Transparenz über seine KI-Dienstleistungen angekündigt. Das soll dazu beitragen, das Vertrauen in diese Technologie zu stärken. Ein Tool soll in Echtzeit nachvollziehbar machen, wie eine KI-Anwendung zu ihren Entscheidungen kommt. IBM geht damit ein zentrales Problem an, das Big Blue im Rahmen einer Studie identifiziert hat. Zwar wollen 82 Prozent aller Unternehmen KI zur Umsatzsteigerung einsetzen, 60 Prozent hätten allerdings Angst vor Fehlentscheidungen der KI-Technologie.

Auch andere Datenschutzgrundsätze sind auf den ersten Blick „KI-inkompatibel“. Der Grundsatz der Datensparsamkeit und Datenminimierung läuft Big-Data-Ansätzen zuwider, bei denen mehr Daten immer besser sind. Zudem fordert die DSGVO in Artikel 25 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Systemen, also „Privacy by Default“ durch geeignete technische und organisatorische Maßnahmen.

Für diese Hürden sind derzeit einige Ansätze in der Diskussion, wie man den KI-Einsatz datenschutzkonform ausgestalten kann. Apple beispielsweise hat den „Crowd-Sourcing-Ansatz“ ins Spiel gebracht. Entwickler und andere Verwender von mittels KI verarbeiteten Daten sollen nur Datensätze bezogen auf bestimmte Kohorten erhalten, daraus aber keine Rückschlüsse auf Einzelpersonen ziehen können. Auf einer Apple-Supportseite heißt es hierzu: „Die von Apple erfassten Crowdsourcing-Daten werden in einer Form gesammelt, die keinerlei Rückschlüsse auf deine Person zulässt.“ Apple verwendet danach die Informationen von vielen Geräten für seine Ortungsdienste, den Aufbau einer Datenbank für den Straßenverkehr, aber auch Marketingzwecke et cetera.

Datenschutzkonforme KI

Letztlich geht dieser Ansatz in die Richtung der „Differential Privacy“. Wikipedia schreibt: „Differential Privacy (engl. für „differentielle Privatsphäre“) hat das Ziel, die Genauigkeit von Antworten zu Anfragen an Datenbanken zu maximieren, unter Minimierung der Wahrscheinlichkeit, die zur Beantwortung verwendeten Datensätze identifizieren zu können. […] Mechanismen, die Differential Privacy erfüllen, verhindern, dass Angreifer unterscheiden können, ob eine bestimmte Person in einer Datenbank enthalten ist oder nicht.“

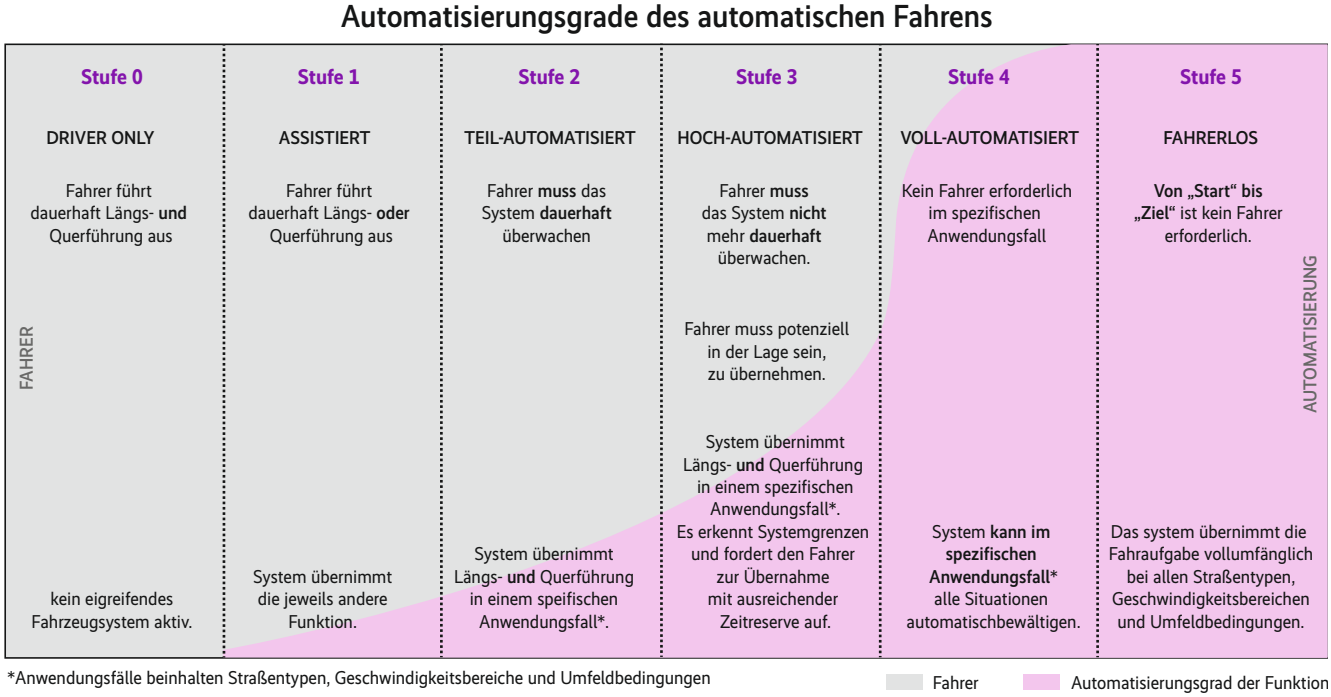
Die zugrunde liegenden Mechanismen umfassen etwa das Hinzufügen von Datendummies, einem „Rauschen“, um die genaue Herkunft von Daten – und damit deren Personenbezug – zu verschleiern. Dass hierdurch letztlich aber auch die Qualität der Datenbank beeinträchtigt und die Aussagekraft der darauf basierenden KI-Ergebnisse geschwächt wird, liegt auf der Hand.

Haftungsfragen beim Einsatz von KI

Gerade im Zusammenhang mit der Diskussion um den Einsatz von KI-gesteuerten autonomen Fahrzeugen stellen sich Fragen nach der Haftung für Schäden, die durch sie verursacht werden – aber nicht nur in diesem Bereich. Immer dann, wenn Technik und Technologien eingesetzt werden, können Schäden entstehen. Im Straßenverkehr gelten nach dem Straßenverkehrsgesetz Sonderregeln, die den allgemeinen Haftungstatbeständen vorgehen. Auch im Bereich der Produkthaftung gibt es mit dem Produkthaftungsgesetz, kurz ProdHaftG, eine vorrangige Regelung.

Das ProdHaftG regelt die Haftung des Herstellers für Schäden, die ein fehlerhaftes Produkt verursacht. Daraus ergibt sich bereits, dass der Verwender eines Produkts nicht nach diesen Vorschriften in die Haftung genommen werden kann. Eine Haftung besteht auch nur, wenn der Fehler schadensursächlich ist. Eine Haftung scheidet nach § 1 ProdHaftG aus, wenn „der 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“.

Wenn beispielsweise die Steuerung eines Roboters unter Einsatz von KI autonom weiterentwickelt wird, muss die Steuerungssoftware bereits von Beginn an mit entsprechenden Sicherungsmaßnahmen ausgestattet sein, damit Schäden vermieden werden. Welche Maßnahmen das im Einzelnen sind, muss anhand des Einzelfalls und des Standes von Wissenschaft und Technik bestimmt werden. Erwirbt ein Dritter den Roboter und setzt diesen ein, treffen ihn aber ebenfalls sogenannte Verkehrssicherungspflichten. Wie bei Kraftfahrzeugen muss der Halter oder Eigentümer für den stets verkehrssicheren Zustand sorgen – er unterliegt einer Verkehrssicherungspflicht.



Unter sehr hohen Anforderungen ist in Deutschland für Fahrzeuge bis Stufe 4 bereits heute eine Zulassung möglich – für die Stufe 5 hingegen nicht (Abb. 2).

Das Produkthaftungsgesetz greift bei Schäden an Leib und Leben. Auch bei mehreren Geschädigten ist die Haftung auf insgesamt 85 Millionen Euro beschränkt. Bei Sachbeschädigungen greift eine Haftung nur, „wenn eine andere Sache als das fehlerhafte Produkt beschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist“. Schäden an Betriebsmitteln eines Unternehmers sind damit beispielsweise nicht geschützt.

Spezialfall autonome Fahrzeuge

Für autonome Fahrzeuge, die am Straßenverkehr teilnehmen, gilt für die Haftung das Straßenverkehrsgesetz. Wenn ein Fahrzeug nicht schneller als 20 km/h fahren kann, gilt das Gesetz nicht. Autonome Roboter etwa für die Zustellung von Post oder im Einsatz eines lokalen Lieferservice, die technisch nicht schneller fahren können, sind von der Haftung nach diesem Gesetz ausgenommen. Für die Haftung kommt es zum Schutz der geschädigten Personen zunächst einmal auch nicht darauf an, ob das Fahrzeug über eine Straßenverkehrszulassung verfügt.

Gleichwohl ist eine Zulassung zur Teilnahme am Straßenverkehr gesetzlich vorgeschrieben und ihr Fehlen kann Sanktionen nach sich ziehen. Inwieweit autonome Fahrzeuge eine solche Zulassung erlangen können, wird seit einiger Zeit diskutiert. Teilautonome Systeme, wie Fahrassistenzsysteme, sind häufig schon Teil der allgemeinen Betriebserlaubnis für Kraftfahrzeuge. Vollautonome Fahrzeuge erhalten bislang allenfalls eine Sondererlaubnis für Test- und Erprobungszwecke und nur für einen eingeschränkten Einsatz.

Inwieweit künftig autonome Systeme „eigenverantwortlich“ am Straßenverkehr teilnehmen dürfen, steht derzeit weltweit zur Diskussion. Die Straßenverkehrszulassung ist hierzulande bislang davon abhängig, dass eine Haftpflichtversicherung für das Fahrzeug besteht. Entsprechende Versicherungsprodukte werden bislang noch nicht allgemein angeboten. Für Sonderzulassungen gibt es vereinzelt individuell verhandelte Versicherungen mit angesichts der noch ungeklärten Haftungs- und Schadensrisiken entsprechend hohen Prämien.

Bei der Frage, welche autonomen Fahrzeuge überhaupt am Straßenverkehr teilnehmen dürfen, kommt es auf den Grad der Automation an. Man unterscheidet weltweit grundsätzlich zwischen fünf Stufen, wobei sich nach nationalem Recht im Detail Unterschiede ergeben können: Mensch als Fahrer (Stufe 0), Assistenzsysteme (Stufe 1), teilautomatisiertes Fahren (Stufe 2), hochautomatisiertes Fahren (Stufe 3), vollautomatisiertes Fahren (Stufe 4) und fahrerloses Fahren (Stufe 5). Für Fahrzeuge bis Stufe 4 ist in Deutschland unter sehr hohen Anforderungen bereits heute eine Zulassung möglich. Das fahrerlose Fahren ist hierzulande hingegen noch nicht zulassungsfähig.

Höhere Gewalt und Fahrlässigkeit

Der „Vorteil“ des Geschädigten bei einem Verkehrsunfall ist, dass die Haftung des Halters unabhängig von einem Verschulden greift. Juristen sprechen von einer Gefährdungshaftung, weil es grundsätzlich gefährlich ist, mit einem maschinengetriebenen Fahrzeug unterwegs zu sein. Nur in Fällen höherer Gewalt ist ein Schaden ausgeschlossen. Wie sonst auch gelten hier Regeln für Schäden, die durch mehrere Fahrzeuge verursacht werden oder wenn den Geschädigten ein Mitverschulden trifft.

Greifen keine Spezialvorschriften, kommt es auf die allgemeinen Haftungstatbestände an. Zentral hierfür ist § 823 des Bürgerlichen Gesetzbuches. Er greift, wenn „das Leben, der Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen“ widerrechtlich verletzt wird. Allerdings nur bei vorsätzlichem oder fahrlässigem Handeln. Fahrlässig handelt etwa, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt. Maschinen können nach heutigem Rechtsverständnis jedoch weder vorsätzlich noch fahrlässig handeln. Sie können nicht sorgfältig oder unsorgfältig sein. Wer aber haftet bei Schäden autonom agierende Systeme?

Um dieses Dilemma zu lösen, fordern einige die Einführung einer „elektronischen Person“ durch den Gesetzgeber. Damit gäbe es eine aus haftungsrechtlicher Sicht verantwortliche Person, die für einen Schaden in Anspruch genommen werden kann. Andere lehnen diesen Ansatz ab. Soll eine elektronische Person

auch für Straftaten in Anspruch genommen werden können und als Strafe beispielsweise verschrottet werden?

Gefährdungshaftung

Letztlich muss der Gesetzgeber entscheiden, welche Antworten er auf diese Fragen geben möchte. Die meisten Juristen sind aber wohl der Meinung, dass man mit den heute schon geltenden Prinzipien der Gefährdungshaftung auch im Bereich KI und autonome Fahrzeuge arbeiten kann. Wie bei Autos auch, muss der Halter beziehungsweise Verwender solcher Systeme für durch diese verursachte Schäden haften und sollte eine Haftpflichtversicherung abschließen. Und dass sich diese selbstlernenden Systeme weiterentwickeln, gehört dann zum Haftungsrisiko und ist entsprechend bei der Versicherung zu berücksichtigen.

Das funktioniert jedenfalls grundsätzlich solange, wie man Menschen Kontrollmöglichkeiten über Systeme einräumen kann, um bei Fehlverhalten einzuschreiten. Bei vollständig autonomen Systemen wird das vielleicht nicht mehr möglich sein. Aber auch dann könnte es angebracht sein, den Verwender des Systems in die Haftung zu nehmen. Wie sich die Diskussion weiterentwickelt, bleibt spannend.

Im Bereich des (teilweise) autonomen Fahrens wurde diese Frage mittlerweile beantwortet. § 1a Abs. 4 StVG lautet: „Fahrzeugführer ist auch derjenige, der eine hoch- oder vollautomatisierte Fahrfunktion – aktiviert und zur Fahrzeugsteuerung verwendet, auch wenn er im Rahmen der bestimmungsgemäßen Verwendung dieser Funktion das Fahrzeug nicht eigenhändig steuert“. Ende 2019 soll es dazu eine Evaluierung geben, damit bei Bedarf das Gesetz angepasst werden kann.

Kreative Künstliche Intelligenz

Spannend sind auch die Fragen nach dem Immaterialgüterschutz von Ergebnissen des Einsatzes von KI. In § 1 des Urheberrechtsgesetzes heißt es: „Die Urheber ... genießen für ihre Werke Schutz ...“. Urheber kann (bislang) nur ein Mensch sein. Ein bekanntes Beispiel für die Konsequenzen dieses Grundsatzes ist das sogenannte „Affen-Selfie“. Ein Affe hatte mittels einer zuvor installierten Selfiekamera von sich ein Foto gemacht, das anschließend in einem Buch verwendet wurde. In einer Klage verlangte eine Tierrechtsorganisation „im Namen des Affen“ eine Entschädigung wegen Urheberrechtsverletzung, was durch das Gericht abgelehnt wurde.

Urheberrechtlich geschützte Werke müssen also das Ergebnis einer kreativ schöpferischen Tätigkeit eines Menschen sein. Dann gibt es urheberrechtlichen Schutz bis 70 Jahre nach dem Tod des Urhebers. Selbstverständlich schadet es dabei nicht, wenn man sich Hilfsmitteln bedient. Hierfür kommen auch Computerprogramme, Datenbanken oder Roboter in Betracht. Wann ein Werk noch – im Schwerpunkt jedenfalls – auf einen Menschen zurückzuführen ist, ist wieder einmal eine Frage des konkreten Einzelfalls. Juristisch gesehen geht es um die „Prägung der wesentlichen Gestaltungsentscheidungen“, die nicht rein auf Technik und KI beruhen dürfen.

Patentierte Künstliche Intelligenz

Diskutiert wird in diesem Bereich über die Einführung eines Leistungsschutzrechts. Bei Datenbanken beispielsweise genießt bereits heute derjenige Schutz, der die Investition für deren Zusammenstellung getätigt hat. Auf eine eigene, menschliche Leistung kommt es darüber hinaus nicht an. Warum also sollte man nicht auch demjenigen ein Schutzrecht einräumen, dessen „Maschine“ etwas ansonsten urheberrechtlich oder „kommerziell Wertvolles“ schafft? Auch hier ist vieles derzeit noch Gegenstand umfassender Diskussionen.

Können Erfindungen von autonomen Systemen patentierbar sein? Das Patentrecht verlangt nicht, dass die erfinderische Tätigkeit von einem Menschen erbracht wird. Auch intelligente Maschinen könnten technische Erfindungen hervorbringen, die sich – wenn sie neu sind – patentieren lassen. Bis allerdings solche künstlichen Intelligenzen auch den komplexen Patentantrag nebst Patentschrift erstellen können, dürfte es noch dauern – abwegig ist die Vorstellung allerdings nicht.

Schließlich können KI-Ergebnisse auch als Geschäftsgeheimnisse geschützt sein, wenn der Verwender „angemessene Geheimhaltungsmaßnahmen“ ergreift und den erzeugten Informationen ein wirtschaftlicher Wert zukommt. So jedenfalls sieht es das Geheimnisschutzgesetz vor, das derzeit im Bundestag diskutiert und bis Jahresende verabschiedet werden soll. Darauf, dass die geheime Information von einem Menschen stammt, kommt es nicht an.

Fazit

Der Einsatz von künstlicher Intelligenz wirft zahlreiche juristische Fragen auf. Neben Haftungs- und Ethikaspekten ist hier das Datenschutzrecht zu nennen. Und die Gemengelage zwischen KI und dem Datenschutz wird weiter an Brisanz gewinnen. Es gibt Forderungen nach einer gesetzlichen Begrenzung der Verwendung von Erkenntnissen aus KI-Anwendungen.

Soll etwa bei vorliegender Einwilligung eine Verhaltensanalyse oder Krankheitserkennung für Versicherungen erlaubt sein? Darf es Predictive Policing geben, um Straftaten zu vermuten, bevor sie begangen wurden? Die meisten KI-Anwendungen werden aber voraussichtlich zulässig bleiben.

Für autonome Fahrzeuge gilt bislang, dass vollständig autonome Fahrzeuge noch nicht zugelassen werden können. Für hochautomatisierte oder vollautomatisierte Fahrzeuge bestehen für die Zulassung hohe Anforderungen, nicht zuletzt beim Versicherungsschutz. Für Schäden haftet in jedem Fall der Halter. Für den Einsatz von KI in anderen Bereichen dürften die Grundsätze der Gefährdungshaftung greifen und Verantwortung sowie Haftung ebenfalls dem Halter beziehungsweise Verwender der Systeme zuweisen.

Der Einsatz von KI bewegt sich in einer juristischen Grauzone. Was zulässig ist und wer bei Schäden haftet, ist im Zweifel anhand des Einzelfalls zu beurteilen – am besten in Zusammenarbeit zwischen Fachleuten aus den Bereichen IT und Recht. Das gilt auch für die Frage, wann Ergebnisse von KI-Systemen Schutz nach dem Urheberrechtsgesetz genießen können – wie bei autonom erzeugter Software oder befüllten Datenbanken. (map@ix.de)

Literatur

[1] Tobias Haar; DSGVO II; Folgenreich; Risikofolgenabschätzung nach der Datenschutz-Grundverordnung; *iX* 9/2018, S. 46

Tobias Haar
ist LL.M. (Rechtsinformatik), MBA, und Rechtsanwalt bei Vogel & Partner in Karlsruhe.