



Digitalisierung und Nachhaltigkeit – rechtliche Herausforderungen für den Versicherungssektor, insbesondere beim Einsatz von Künstlicher Intelligenz

Christian Armbrüster 

Angenommen: 12. Januar 2022 / Online publiziert: 24. Januar 2022
© Der/die Autor(en) 2022

Zusammenfassung Digitalisierung und Nachhaltigkeit sind zwei aktuelle und für die Versicherungswirtschaft bedeutsame Themenfelder, die auf den ersten Blick wenig miteinander zu tun haben. Indessen gibt es eine ganze Reihe von inhaltlichen Bezügen und Querverbindungen. Der Beitrag behandelt unter diesem Blickwinkel die rechtlichen Herausforderungen, welche sich aus der Digitalisierung im Versicherungssektor und insbesondere aus dem Einsatz von KI-Systemen ergeben.

Digitalisation and sustainability – legal challenges for the insurance sector, especially with regard to the use of AI

Abstract Digitalisation and sustainability are two current and important topics for the insurance industry that at first glance have little to do with each other. However, there is a whole series of substantive references and cross-connections. From this perspective, the article deals with the legal challenges arising from digitalisation in the insurance sector and in particular from the use of AI systems.

Schriftfassung des Vortrags, den der Verfasser im Plenum II auf der digitalen Jahrestagung des Deutschen Vereins für Versicherungswissenschaft e. V. am 10.03.2021 gehalten hat. Der Autor dankt Herrn Wiss. Mitarb. *Jonathan Prill*, der im Rahmen eines vom Deutschen Verein für Versicherungswissenschaft e. V. geförderten Forschungsprojekts eine Dissertation zum Thema „Künstliche Intelligenz und Versicherung“ verfasst, für wertvolle Anregungen.

Christian Armbrüster (✉)

Fachbereich Rechtswissenschaft, Freie Universität Berlin, Van't-Hoff-Str. 8, 14195 Berlin, Deutschland

E-Mail: c.armbruester@fu-berlin.de

1 Einleitung

Der Zusammenhang zwischen Digitalisierung im Allgemeinen und Künstlicher Intelligenz im Speziellen auf der einen Seite und Nachhaltigkeit auf der anderen Seite liegt nicht auf der Hand. Gleichwohl bestehen zwischen beiden Bereichen vielfältige inhaltliche Bezüge und Querverbindungen.¹ Das Gebiet der Künstlichen Intelligenz ist ein sehr weites Feld, und über die sich daraus ergebenden Rechtsfragen wird im deutschen Recht in vielen Teildisziplinen – vom Vertragsrecht über das Deliktsrecht bis hin zum Datenschutzrecht – derzeit intensiv diskutiert.

Im Folgenden soll es nach einer Grundlegung zunächst um das Datenschutzrecht gehen, das für die Praxis von besonderer Bedeutung ist. Es folgt ein Blick auf einen konkreten Anwendungsfall, nämlich die Betrugsbekämpfung, und auf den Einsatz von KI in diesem Bereich. Anschließend werden Fragen des Zivilrechts, die IT-Sicherheit sowie das Problem der Nachvollziehbarkeit von unter Einsatz von KI getroffenen Entscheidungen erörtert. Zur Regulierung gilt es interessante aktuelle Entwicklungen auf europäischer Ebene zu berichten und zu kommentieren. Abgerundet wird der Beitrag mit einem Ausblick.

2 Nachhaltigkeit und Künstliche Intelligenz

2.1 Nachhaltigkeit

Der Ausdruck Nachhaltigkeit ist mittlerweile allgegenwärtig. Unter der Abkürzung ESG wird er etwas schärfer konturiert; sie steht für Environmental Social Governance, also Umwelt, Soziales und Unternehmensführung.² Dabei geht es im Bereich Umwelt um Themen wie Umweltschädigung, Treibhausgasemissionen oder Energieeffizienz. Soziales meint etwa Arbeitssicherheit und Gesundheitsschutz, Diversity oder gesellschaftliches Engagement (Corporate Social Responsibility). Bei der Unternehmensführung stehen Unternehmenswerte oder Steuerungs- und Kontrollprozesse (Corporate Governance) im Vordergrund.

2.2 Künstliche Intelligenz

Bevor es zu klären gilt, welche Bedeutung ESG in Zusammenhang mit dem speziellen Thema Künstliche Intelligenz (KI) hat, sei auch letztere hier thematisiert. Der Begriff wird zur schlagwortartigen Umschreibung einer gewissen Bandbreite von unterschiedlichen digitalen Technologien und Anwendungen verwendet. Dazu zählen die sog. *Expertensysteme*, also Computerprogramme, die datenbasiert Handlungsempfehlungen geben und damit praktisch als Experten Handelnde unterstützen.³

¹ S. dazu die Beiträge von *Oletzky* und *Pickel* auf der Jahrestagung 2021.

² *BaFin*, Merkblatt zum Umgang mit Nachhaltigkeitsrisiken, 2019, S. 9; näher *Kockrow*, ZRP 2021, 13.

³ *Niederée/Nejdl*, in: Ebers/Heinze/Krügel/Steinrötter (Hrsg.), Rechtshandbuch Künstliche Intelligenz und Robotik, 2020, § 2 Rn. 15.

Ein anderer Anwendungsbereich betrifft die *Mustererkennung*. Ein bekanntes Beispiel bietet eine Fotosequenz, welche die Mutation eines Blaubeermuffins zu einem Chihuahua aufzeigt.⁴ Daran werden auch die (noch) bestehenden Grenzen des Einsatzes von Künstlicher Intelligenz zur Bilderkennung deutlich: Bis heute ist es bei dieser Fotosequenz Maschinen nicht immer möglich, den Unterschied zwischen Tiergesicht und Gebäck zu ermitteln. Immerhin hat die Künstliche Intelligenz insoweit in den letzten zehn Jahren beträchtliche Fortschritte erzielt: Die Fehlerquote ist in diesem Zeitraum von 30% auf etwa 2–3% gesunken. Aber es ist nach wie vor nicht möglich, die Mustererkennung zu 100% zuverlässig durchzuführen. In der praktischen Anwendung spielt diese Technologie etwa in der Radiologie eine große Rolle. Fehler, die durch die abnehmende Leistungsfähigkeit des Menschen im Verlauf eines langen Arbeitstages oder durch Ablenkungsfaktoren entstehen, lassen sich auf diese Weise ausschließen. Auch in der Radiologie wird freilich immer noch für die Beurteilung von Zweifelsfällen ein Mensch hinzugezogen.

Auch der Begriff der *Robotik* (Robotertechnik) fällt unter Künstliche Intelligenz. Dabei geht es um die Interaktion der realen mit der physischen Welt auf der Grundlage von Sensoren und Informationsverarbeitung. Am stärksten mit Künstlicher Intelligenz verbunden wird freilich der Begriff des *maschinellen Lernens*.⁵ Hier geht es letztlich darum, Wissen aus Erfahrung zu generieren, d.h. also zu lernen. Das ist wiederum im sog. *deep learning* besonders ausgeprägt. Das ist ein Teilbereich des maschinellen Lernens, bei dem es darum geht, künstliche neuronale Netze zu entwickeln, also gewissermaßen das menschliche Gehirn digital nachzubilden, so dass die Künstliche Intelligenz in der Lage ist, Strukturen in Daten zu erkennen, sie auszuwerten und dann die Ergebnisse zu verbessern.⁶ Es handelt sich beim *deep learning* also nicht nur um eine reine Anwendung, sondern um eine Optimierung.

Alle diese Einsatzbereiche von Künstlicher Intelligenz werden letztlich durch ein und dasselbe übergeordnete Ziel geprägt. Es geht darum, menschliche Intelligenzleistungen zu ersetzen oder zumindest zu ergänzen.⁷ Dafür, dass dies gelingt, sind zwei Faktoren von entscheidender Bedeutung. Es sind dies die Quantität und die Qualität der Daten, die für die jeweilige Anwendung zur Verfügung stehen. Darauf wird noch zurückzukommen sein, ebenso wie auf die Einsatzgebiete im Versicherungssektor. Dabei geht es zum Teil um rein repetitive Aufgaben im Massengeschäft, namentlich um die Tiefenanalyse unstrukturierter Daten, teils reichen die Anwendungsfelder aber auch weit darüber hinaus.

Aus juristischer Sicht sind mit dem Einsatz von KI-Systemen ganz verschiedenartige Risiken verbunden: So können Fehlentscheidungen getroffen werden. Zudem können Sicherheitslücken und Manipulationsgefahren entstehen; genannt seien hier nur Cyberangriffe auf Systeme, die KI-basiert arbeiten. Immer wieder wird auch die

⁴ <https://www.arvato-systems.de/blog/was-ist-kuenstliche-intelligenz> (zuletzt aufgerufen am 18.01.2022).

⁵ Zu praktischen Anwendungsfällen in der Versicherungswirtschaft *Busch*, in: Reich/Zerres, Handbuch Versicherungsmarketing, 2. Aufl. 2019, S. 247 ff.

⁶ Näher *Niederée/Nejdl* (Fn. 3), § 2 Rn. 56 ff.; *Russel/Norvig*, AI—A Modern Approach, 4. Aufl. 2021, S. 651.

⁷ *Herberger*, NJW 2018, 2825, 2829.

Gefahr einer Diskriminierung genannt.⁸ Dabei gilt es zu beachten, dass nach den unionsrechtlichen Vorgaben zum Antidiskriminierungsrecht ein Verstoß nicht etwa eine böse, d. h. auf Ausgrenzung und Herabwürdigung gerichtete Absicht erfordert. Vielmehr genügt es bereits, wenn rein faktisch eine bestimmte Gruppe auf Grund eines geschützten Merkmals (Alter, Behinderung, Geschlecht usw.) ungleich behandelt wird, ohne dass ein Rechtfertigungsgrund eingreift. Eine derartige verbotene Ungleichbehandlung kann auch eintreten, wenn Entscheidungen etwa über einen Vertragsschluss, die Prämienhöhe oder die Schadensregulierung unter Einsatz von KI-Systemen getroffen werden.

Ein weiteres rechtliches Risiko liegt in der Verletzung von Vorgaben zum Datenschutz (s. dazu sub 3). Nicht zuletzt ist das Aufsichtsrecht betroffen. Dabei geht es um die Gefahr der mangelnden Nachvollziehbarkeit von Entscheidungen, die unter Verwendung von KI-Systemen getroffen wurden. Wenn die BaFin KI-basierte Entscheidungen überprüft, muss sie nachvollziehen können, auf welche Weise diese zustande gekommen sind. Dabei geht es unter anderem darum zu ermitteln, mit welchen Vorgaben und mit welchem Datenmaterial das betreffende KI-System gespeist wurde.

2.3 Verbindungslinien

An dieser Stelle soll auf die eingangs aufgeworfene Frage nach dem Zusammenhang zwischen Nachhaltigkeit einerseits und Digitalisierung/Künstlicher Intelligenz andererseits zurückgekommen werden. Hier seien noch einmal die drei Buchstaben ESG aufgegriffen.

Das „E“ steht, wie dargelegt, für *Environmental*. In diesem Kontext spielt der Energieverbrauch beim Einsatz digitaler Techniken eine Rolle. Ein prägnantes Beispiel bietet der Stromverbrauch bei der Blockchain. Auch der Abbau der benötigten natürlichen Ressourcen für die Hardware ist bei KI-Systemen von Bedeutung.

Das „S“ für *Social* betrifft insbesondere ein Thema, das immer wieder diskutiert wird, nämlich die Sorge, ob durch den zunehmenden Einsatz von Künstlicher Intelligenz in der Versicherungswirtschaft Arbeitsplätze entfallen oder zumindest Umschulungen erforderlich werden, weil viele Tätigkeiten nunmehr durch KI-Systeme durchgeführt werden, die früher Menschen verantwortet haben, etwa Vertriebsmitarbeiter oder Schadensachbearbeiter.

Hinzu kommt speziell für die Versicherungswirtschaft ein besonders sensibles Thema, nämlich dasjenige der Empathie.⁹ Bisweilen wird davor gewarnt, dass etwa bei Regulierungsentscheidungen durch den Einsatz von KI-Systemen der menschliche Empathiefaktor verloren geht. Diese Warnung verdient nicht zuletzt deshalb Beachtung, weil es hier um die Kundenbindung und auch um die Frage der Reputation geht. Ein klassisches Beispiel bietet die Situation der Kulanzentscheidung: Der Sachbearbeiter hegt Zweifel, ob tatsächlich ein Versicherungsfall eingetreten ist, er sieht sich aber die Gesamtsituation an und gelangt dabei – etwa angesichts der Vertragsdauer und des Umfangs der Geschäftsbeziehung, des bisherigen Schadens-

⁸ Art.-29-Datenschutzgruppe, WP 251, Stand Februar 2018, S. 6; Steege, MMR 2019, 715.

⁹ Vgl. zum medizinischen Bereich Beck, MedR 2018, 772, 776.

verlaufs, der wirtschaftlichen Verhältnisse oder tragischer individueller Umstände, die mit dem Schadensfall zusammenhängen – zu dem Schluss, dass es geboten erscheint, hier kulant zu handeln. Ein solches menschliches Verhalten kann bis zu einem gewissen Grad, aber jedenfalls nach dem gegenwärtigen Stand der Technik nicht in vollem Umfang durch KI-Systeme nachgebildet werden.¹⁰

Man kann darin, dass die für Kulanzentscheidungen bedeutsamen Faktoren grundsätzlich (wenn auch unvollkommen) durch Künstliche Intelligenz abgebildet werden können, freilich auch einen Vorzug sehen. Schließlich werden dadurch Kulanzentscheidungen rationalisiert, indem die dafür maßgeblichen Kriterien anhand von feststehenden Eckdaten wie etwa Vertragsdauer, Prämienvolumen oder Schadensaufwand klar definiert und als verbindlich festgelegt werden. Dadurch kann dem Interesse an einer Gleichbehandlung aller Versicherungsnehmer Rechnung getragen werden. Allerdings lassen sich, wie erwähnt, damit nicht alle Faktoren erfassen, die bislang in Kulanzentscheidungen einfließen. Zudem fehlt der menschliche Aspekt, der die Leistungsbereitschaft des Versicherers als ein individuelles Eingehen auf die persönliche Situation des Versicherungsnehmers und nicht als das Ergebnis eines rein technischen, digitalisierten Vorgangs erscheinen lässt. Mit diesem Dilemma wird sich jeder Versicherer, der KI-Systeme bei seinen Regulierungsentscheidungen einsetzen will, auseinandersetzen und eine Abwägung vorzunehmen haben.

Das „G“ für *Governance* meint schließlich Compliance und Aufsicht, die Abhängigkeit von Softwareunternehmen sowie Rechtssicherheit und Haftungsrisiken. Nachhaltigkeit ist damit auch ein zunehmend bedeutsamer Teilaspekt der Corporate Governance.

3 Datenschutzrecht

3.1 Verarbeitung personenbezogener Daten

Der für das europäische Datenschutzrecht grundlegende Begriff der personenbezogenen Daten ist in einem sehr weiten Sinn zu verstehen.¹¹ Er erfasst außer klassischen Daten wie etwa dem Namen einer Person und bestimmten üblicherweise auch in Ausweispapieren dokumentierten physischen Identitätsmerkmalen (Alter, Geschlecht usw.) auch weitere Faktoren, insbesondere biometrische Daten wie Stimme, Fingerabdruck, Iris oder Gesicht. Das ist deshalb wichtig, weil beispielsweise die Stimme schon heute mittels KI-Systemen genutzt werden kann, um Betrugserkennung zu optimieren. Darauf wird noch zurückzukommen sein.

Sehr weit gefasst ist außer dem Begriff der personenbezogenen Daten auch derjenige der Verarbeitung von Daten. Die Legaldefinition in Art. 4 Nr. 2 der Datenschutzgrundverordnung (DSGVO), die seit 2018 europaweit gilt, erfasst ein breites Spektrum an Vorgängen. Juristisch bedeutsam ist der Befund, dass eine Anonymi-

¹⁰ *Grapentin*, Vertragsschluss und vertragliches Verschulden beim Einsatz von Künstlicher Intelligenz und Softwareagenten, 2018, S. 42.

¹¹ *Ernst*, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 DSGVO Rn. 3.

sierung der Daten beim Einsatz von KI-Systemen oftmals schwierig ist. Misslingt sie, so handelt es sich um personenbezogene Daten.¹²

3.2 Verbot mit Erlaubnisvorbehalt

Das Grundkonzept des Datenschutzrechts besteht darin, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, aber ein Erlaubnisvorbehalt besteht.¹³ Insbesondere ist der Betroffene in der Lage, in die Verarbeitung seiner personenbezogenen Daten einzuwilligen. Diese Einwilligungsmöglichkeit hat im juristischen Schrifttum zu einer Diskussion darüber geführt, ob damit eine höhere Akzeptanz der Datenverarbeitung bei den Betroffenen verbunden ist. Teils wird dies mit der Begründung bezweifelt, dass die Einwilligung nicht deshalb erfolge, weil man die Datenverarbeitung wirklich konsentiert, sondern weil man seinem eigentlichen Ziel, etwa einem gewünschten Vertragsschluss, zügig näher kommen möchte. Dabei wird eine Parallele zum Einverständnis des Kunden mit der Geltung von AGB gezogen, welches nach § 305 Abs. 2 a.E. BGB gleichfalls erforderlich, allerdings in der Praxis im Vergleich zum Datenschutzrecht an geringere Anforderungen geknüpft ist: Der Kunde hakt das Thema ab, weil er im Prozess hin zum Vertragsschluss weiterkommen will, und nicht, weil er von der Richtigkeit überzeugt ist (sog. rationale Ignoranz).¹⁴

Rechtliche Probleme beim Einsatz von KI-Systemen im Zusammenhang mit der Einwilligung entstehen vor allem dadurch, dass der Betroffene die von ihm erteilte Einwilligung nach Art. 7 Abs. 3 S. 1 DSGVO jederzeit ohne Begründung widerrufen kann. Darin liegt ein erheblicher Unsicherheitsfaktor für alle Verwender von KI-Systemen. Die Einwilligung ist zudem an qualifizierte Anforderungen geknüpft. Insbesondere muss sie vor der Datenverarbeitung erklärt werden, freiwillig sein, auf spezifischen Informationen beruhen sowie eindeutig sein. Die Beweislast dafür, dass eine wirksame Einwilligung vorliegt, trifft den Datenverarbeiter.¹⁵

Freilich gibt es in bestimmten Fällen auch jenseits der Einwilligung besondere Zulässigkeitsgründe. Am interessantesten für den Versicherungssektor ist dabei die Regelung in Art. 6 Abs. 1 U Abs. 1 lit. b DSGVO. Demnach ist die Einwilligung entbehrlich, wenn die Datenverarbeitung zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Dies führt freilich sogleich zu der Frage, ob auch der *Einsatz eines KI-Systems* erforderlich sein muss oder lediglich die *Datenverarbeitung als solche*. Die Debatte darüber entwickelt sich derzeit.¹⁶ Es spricht indes vieles dafür, dass es ausreicht, wenn überhaupt eine Datenverarbeitung erforderlich ist. Mit welchem technischen Mittel sie dann durch-

¹² Gausling, in: Ballestrem/Bär/Gausling/Hack/von Oelffen (Hrsg.), Künstliche Intelligenz – Rechtsgrundlagen und Strategien in der Praxis, 2020, S. 18 f.; Niemann/Kevekordes, CR 2020, 17, 19; Winter/Battis/Halvani, ZD 2019, 489, 492.

¹³ Frenzel, in: Paal/Pauly (Fn. 11), Art. 6 DSGVO Rn. 1.

¹⁴ Ausführlich zu diesem Phänomen Hacker, Datenprivatrecht, 2020, S. 61 f., 255 f.

¹⁵ EuGH, Urt. v. 11.11.2020 – C-61/19, ZD 2021, 89 Rn. 42.

¹⁶ Lüttringhaus, VW 2020, 88 f.; Prill, KI und Versicherung (in Vorbereitung).

geführt wird, ist auch unter dem Blickwinkel des Schutzes des Betroffenen nicht mehr entscheidend.

3.3 Informationsansprüche

Nach Art. 13 Abs. 2 lit. f DSGVO steht dem Betroffenen bei der Erhebung personenbezogener Daten ein Informationsrecht über die Entscheidungslogik des Algorithmus zu. Dieser Informationsanspruch umfasst „aussagekräftige Informationen über die involvierte Logik und die bezweckten Auswirkungen auf den Betroffenen“. Ganz allgemein stehen die verschiedenen Ansprüche des Einzelnen gegen den Datenverarbeiter auf Informationserteilung keineswegs nur auf dem Papier. Vielmehr haben sie auch im Versicherungssektor bereits zu gerichtlichen Auseinandersetzungen geführt. Als Beispiel sei ein Verfahren vor dem Landgericht Köln genannt, in dem ein Versicherungsnehmer von seinem Krankenversicherer zahlreiche Auskünfte zur Verarbeitung seiner personenbezogenen Daten verlangt hat. Das Gericht hat in seiner Entscheidung zu diesem Auskunftsverlangen auch ausgeführt, dass der sog. Code of Conduct (CoC) des GDV die Gerichte nicht bindet.¹⁷ Dieser CoC existiert bereits seit 2012; er ist seitdem mehrfach überarbeitet worden und hat derzeit den Stand vom 29.06.2018. Er enthält Regeln zu den Voraussetzungen einer ordnungsgemäßen Datenverarbeitung. Nach Art. 30 Abs. 1 CoC verpflichten sich diejenigen Versicherer, die den Beitritt zum CoC erklären, zur Einhaltung der darin enthaltenen Regeln. Es handelt sich um Verhaltensregeln i.S.v. Art. 40 DSGVO, mit denen die allgemeinen Anforderungen der DSGVO branchenspezifisch für die Versicherungswirtschaft konkretisiert werden.

3.4 Datenquantität

Wie eingangs erwähnt, spielt neben der Qualität auch die Quantität der für ein KI-System verfügbaren Daten eine wesentliche Rolle für die damit erzielbaren Ergebnisse. Ein Beispiel dafür, wie KI-Systeme in der Versicherungswirtschaft bereits heute mit geradezu gigantisch großen Datenmengen operieren, bietet der chinesische Versicherer *Ping An*. Dieses Unternehmen setzt bereits flächendeckend KI-Technologie ein.¹⁸ Dies ist etwa bei der Kfz-Schadensbearbeitung der Fall, wo auch hierzulande schon einige Anbieter mit einer (bisher nicht vollautomatisierten) Schadens-App arbeiten. Der Versicherungsnehmer übermittelt dem Versicherer über die App Fotos des Kfz-Schadens, die anschließend in einem automatisierten Prozess ausgewertet werden. Das KI-System berechnet eine Entschädigungssumme, die dem Versicherungsnehmer sodann als rasche und endgültige Regulierung des Schadensfalls angeboten wird. Es kann auch zu einer Ablehnung kommen, weil es sich beispielsweise nach der KI-gestützten Analyse um einen Altschaden handelt. In diesem Fall wird,

¹⁷ LG Köln, Urt. v. 11.11.2020 – 23 O 172/19, BeckRS 2020, 30968 Rn. 19; mittlerweile anderweitig erledigt; vgl. OLG Köln, Beschl. v. 15.04.2021 – 9 U 246/20, GRUR-RS 2021, 9729; zum datenrechtlichen Auskunftsanspruch des Versicherungsnehmers gegen den Versicherer nach der DSGVO s. nunmehr auch BGH, Urt. v. 15.06.2021 – VI ZR 576/19, VersR 2021, 1019.

¹⁸ Krüger, VW 2020, 52f.

sofern der Versicherungsnehmer sich damit nicht zufrieden gibt, regelmäßig wie bislang die Einschaltung eines Sachverständigen geboten sein. Die Rahmenbedingungen in China, welche enorm große Datensammlungen ermöglichen, unterscheiden sich freilich deutlich von den Verhältnissen in Deutschland. Dies gilt zum einen im Hinblick auf die rein faktische Situation; China verfügt schon allein auf Grund der Bevölkerungszahl über sehr viel größere Datenbestände. Zum anderen ist auch die Rechtslage eine andere; insbesondere setzen datenschutzrechtliche Regeln deutlich weniger Grenzen.

3.5 Rechtsfolgen von Verstößen gegen die DSGVO

Besonderes Augenmerk verdienen die Rechtsfolgen von Verstößen gegen die Vorgaben der DSGVO. In solchen Fällen sind nicht allein materielle, sondern auch immaterielle Schäden, also Nichtvermögensschäden, zu ersetzen (Art. 82 DSGVO).

Ein prägnantes Beispiel für einen solchen Haftungsfall wäre etwa folgendes fiktive Szenario: Der Versicherer setzt ein KI-System ein, das anhand des Gesundheitszustandes des Versicherungsnehmers prüfen soll, wie wahrscheinlich es ist, dass er gegen eine ablehnende Regulierungsentscheidung gerichtlich vorgehen wird.¹⁹ Je nach dem Prüfungsergebnis entscheidet der Versicherer dann darüber, wie er den gemeldeten Schadensfall reguliert. Das KI-System könnte als Kriterien für eine Prognose außer klassischen Kriterien wie bisherigem Vertragsverlauf oder Gesundheitszustand etwa auch das Verhalten des Versicherungsnehmers auf Social-Media-Kanälen wie Twitter oder Facebook auswerten.

Ein solcher Einsatz von Künstlicher Intelligenz wäre datenschutzrechtlich unter jedem denkbarem Gesichtspunkt unzulässig. Was speziell die Auswertung des Gesundheitszustands angeht, so läge darin eine unzulässige Verarbeitung von Gesundheitsdaten. Der Schutz dieser besonders sensiblen Daten wird durch Art. 9 Abs. 1 DSGVO und überdies durch § 213 VVG in besonderem Maße gesetzlich gewährleistet.

4 Betrugsbekämpfung

Auch im Bereich der Betrugserkennung mittels KI-Systemen stellen sich datenschutzrechtliche Fragen. Dabei geht es beispielsweise um den Fall, dass anhand der *Stimme* einer Person, die etwa eine Schadensmeldung abgibt oder Fragen zu einem Versicherungsfall beantwortet, analysiert wird, ob die Person die Wahrheit sagt. Dabei geht es gewissermaßen um einen modernen digitalen Lügendetektor. Die menschliche Stimme ist als personenbezogenes Datum von den Vorgaben des Datenschutzrechts erfasst, sodass es hier hohe Hürden zu beachten gilt.

Weniger komplex ist unter datenschutzrechtlichen Aspekten die Betrugsaufdeckung im Zusammenhang mit der *Belegprüfung*. Hierbei geht es darum, dass KI-Systeme eingesetzt werden, um die unproblematischen Routinefälle „durchzuwin-ken“ und nur bei Unregelmäßigkeiten den Fall an einen Sachbearbeiter weiterzu-

¹⁹ Beispiel in Anlehnung an *Kähler*, NJW 2020, 113, 114.

leiten. Interessant ist in diesem Zusammenhang die Frage, ob eine Erweiterung des Hinweis- und Informationssystems der Versicherungswirtschaft (HIS) geboten ist. Es könnte sinnvoll sein, auf deutscher und womöglich auf europäischer Ebene die Datenbasis zu verbreitern, indem nicht jedes Unternehmen die relevanten Daten nur für sich sammelt und unter Einsatz von KI auswertet, sondern man eine gemeinsame Datensammlung anlegt. Dies müsste unter Einhaltung der Datenschutzregeln erfolgen, was dadurch erleichtert wird, dass diese Regeln, wie dargelegt, mittlerweile innerhalb der EU vereinheitlicht sind. Die Daten, um die es hier geht, etwa zur Schadensanalyse, lassen sich weitgehend anonymisieren, sodass die datenschutzrechtlichen Hürden nicht unüberwindlich erscheinen.

5 Zivilrecht

5.1 KI-Systeme als rechtfähige Einheiten

Im Zivilrecht wird derzeit intensiv erörtert, inwieweit die bestehenden Regeln etwa zum Vertragsschluss und zur Deliktshaftung auch auf durch KI-Systeme gesteuerte Erklärungen und sonstige Verhaltensweisen anwendbar sind. So gibt es eine lebhafte Diskussion darüber, ob ein KI-System jedenfalls de lege ferenda als eine juristische Person oder zumindest als eine sonstige eigenständige rechtfähige Einheit anzusehen sein soll. Die Befürworter meinen, dass sich damit viele Zurechnungsprobleme lösen lassen, etwa wenn das KI-System Entscheidungen trifft und oder auch Schäden verursacht.²⁰

Diese Diskussion erscheint bereits deshalb nicht weiterführend, weil die Anerkennung einer solchen Rechtspersönlichkeit ohne gleichzeitige Ausstattung mit einer eigenen Haftungsmasse sinnlos erschiene.²¹ Sollte hingegen eine Haftungsmasse gebildet werden, würde sich sogleich die Frage stellen, wer diese aufzubringen hätte. Daneben sprechen auch einige weitere Argumente dagegen, etwa das Fehlen eines eigenen Überlebenswillens oder der Umstand, dass es sich bei KI-Systemen gar nicht um eine einheitliche Technologie handelt, womit sich schwierige Fragen der Grenzziehung stellen würden.²² Überspitzt könnte man die Frage stellen, ob dann, wenn ein Haushaltsroboter mit eigener Rechtspersönlichkeit versehen würde, die Hausratversicherung zu einer solchen für fremde Rechnung wird, weil der Roboter ein Interesse an seiner eigenen Integrität hat.

²⁰ S. nur *Mathias*, Automaten als Träger von Rechten, 2. Aufl. 2010, S. 36f.; *Teubner*, AcP 218 (2018), 155, 156f. Eingehend jüngst *Linaratos*, Autonome und vernetzte Aktanten im Zivilrecht. Grundlinien zivilrechtlicher Zurechnung und Strukturmerkmale einer elektronischen Person, 2021; s. dazu *Armbrüster*, ZVersWiss (2022). <https://doi.org/10.1007/s12297-022-00516-5>.

²¹ *Janal*, in: Gless/Seelmann (Hrsg.), Intelligente Agenten und das Recht, 2016, S. 141, 157; *Riehm*, in: Kaulartz/Braegelmann (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kapitel 6.1 Rn. 33.

²² *Riehm* (Fn. 21), Rn. 24 ff., 28 ff.

5.2 Zurechnung

Was die Zurechnungsfragen angeht, lässt sich die Thematik auf die Formel bringen, dass das im Jahr 1900 in Kraft getretene Bürgerliche Gesetzbuch (BGB) auch im Zeitalter der KI-Systeme die erforderlichen Regeln bereithält, um Willenserklärungen zuzurechnen: Demjenigen, der das KI-System einsetzt, werden die Erklärungen zugerechnet, auch wenn er nicht mehr selbst einen situativen, d. h. auf den Einzelfall bezogenen, Willen bildet.²³ Dies gilt beispielsweise dann, wenn unter Einsatz eines KI-Systems über Annahme oder Ablehnung eines Versicherungsantrags entschieden wird.

Setzt ein Versicherer ein KI-System ein, so ist fraglich, ob er den Versicherungsnehmer darüber zu informieren hat. Bei internen Routinevorgängen ist dies eher abzulehnen. Bei einer KI, die in Interaktion mit Kunden tritt, lässt sich hingegen eine Informationspflicht als Schutzpflicht aus § 241 Abs. 2 BGB herleiten. Dies gilt etwa dann, wenn ein Beratungs-Chat ausschließlich unter Einsatz von Künstlicher Intelligenz und ohne menschlichen Berater durchgeführt wird. In diesem Fall sollte der Vertragsinteressent in dem Chat vorab informiert werden, dass kein Mensch die Antworten auf seine Fragen verfasst, sondern dass dies allein mittels Künstlicher Intelligenz funktioniert. Dies deckt sich auch mit Art. 52 des jüngst vorgestellten Verordnungsentwurfs der EU-Kommission.²⁴

5.3 Haftungsfragen

Ein wichtiges Thema im Bereich des automatisierten und autonomen Fahrens ist die Frage, ob sich mit dem Einsatz von KI-Systemen die Haftung vom Fahrer und Halter des Kfz auf den Hersteller der KI-Systeme und damit von der Kfz-Haftpflichtversicherung auf die Produkthaftpflichtversicherung verlagert. Davon ist, wie an anderer Stelle näher dargelegt wurde,²⁵ nicht auszugehen. Zwar wird die verschuldensabhängige Fahrerhaftung mit zunehmender digitaler Steuerung des Kfz an Bedeutung abnehmen. Hingegen gilt der für die Halterhaftung als einer Gefährdungshaftung maßgebliche Grundgedanke, dass derjenige, der den Nutzen aus dem Halten eines Kfz zieht, auch die damit für Dritte verbundenen Risiken zu tragen hat, auch bei automatisiertem und autonomem Fahren.

6 IT-Sicherheit

Was die Gewährleistung der IT-Sicherheit angeht, ist eine interessante neuere Entwicklung auf EU-Ebene zu verzeichnen. Die Kommission hat den Entwurf einer Verordnung über Betriebsstabilität digitaler Systeme des Finanzsektors vorgelegt, die man durchaus zur in dem oben aufgezeigten weiten Sinne verstandenen Nachhaltigkeitstrategie rechnen kann.

²³ Zum Diskussionsstand s. nur *Schubert*, in: MüKo BGB, 9. Aufl. 2021, § 164 Rn. 118.

²⁴ *EU-Kommission*, COM(2021) 206 final.

²⁵ *Armbrüster*, in: FS Ch. Huber, 2020, S. 27, 32 ff.

7 Nachvollziehbarkeit der Entscheidungen

Das Gebot der Nachvollziehbarkeit von mittels KI-Systemen generierten Entscheidungen dürfte künftig weiter an Bedeutung gewinnen. Dies hängt nicht zuletzt damit zusammen, dass die Komplexität der Algorithmen kontinuierlich zunimmt. Damit gelangen die Frage nach der Transparenz sowie nach der Eigenkontrolle durch den Versicherer als dem Verwender und durch die Versicherungsnehmer sowie Versicherten als den Betroffenen verstärkt in den Blick. Beides ist wichtig, um die Datenqualität zu verbessern und um Vertrauen zu generieren.

Hinzu kommt die bereits erwähnte Frage nach der Kontrollierbarkeit durch die Aufsichtsbehörden. Die *BaFin* weist in einer nach wie vor aktuellen Publikation aus dem Jahr 2018 ausdrücklich darauf hin, dass sogenannte Blackbox-Verweise nicht zulässig sind.²⁶ Vielmehr haben die Versicherer die Erklärbarkeit von KI basierten Entscheidungen für sachkundige Dritte zu gewährleisten. Dabei wird zutreffend dargelegt, dass dies auch zur Selbstkontrolle innerhalb der Unternehmen wichtig ist. Bei einer Funktionsausgliederung von KI-Bereichen erfasst die Aufsicht insoweit auch die jeweiligen KI-Dienstleister, ohne dass die Versicherer dadurch aus ihrer Verantwortung entlassen würden (vgl. § 32 VAG).

Beim Thema Nachvollziehbarkeit durch die Aufsicht geht es freilich keineswegs allein um die Finanzdienstleistungsaufsicht durch die BaFin, sondern auch um die Beaufsichtigung durch die *Datenschutzbehörden*. Bislang nicht geklärt ist etwa die Frage, ob dann, wenn ein Verwender neue KI-Modelle einsetzen möchte, eine Anzeigepflicht oder sogar ein Genehmigungserfordernis besteht. Dies soll durch den Verordnungsentwurf der EU-Kommission für hochriskante Anwendungen geändert werden.

8 Künftige Regulierung auf EU-Ebene

Was die künftige Regulierung des Einsatzes von KI-Systemen angeht, sind auf europäischer Ebene umfangreiche Aktivitäten zu verzeichnen. Insbesondere hat das *Europäische Parlament* mit großer Mehrheit die Kommission zur Vorlage eines Legislativvorschlag über die Haftung für Schäden durch KI-Systeme aufgefordert und dazu bereits selbst einen Vorschlag ausformuliert.²⁷ Dieser Vorschlag geht inhaltlich sehr weit. So sieht er für sogenannte *Systeme mit hohem Risiko* eine verschuldensunabhängige Haftung, flankiert durch eine Pflichthaftpflichtversicherung, vor. Das Brisante daran für den Versicherungssektor ist, dass nach der Vorstellung des Europäischen Parlaments auch dieser Bereich unternehmerischer Betätigung als ein System mit hohem Risiko eingestuft werden soll. Dementsprechend ist der Versicherungssektor in einem Anhang zu der EntschlieÙung als ein hohes Risiko aufgeführt. Zur Begründung wird darauf verwiesen, dass der Einsatzbereich ein erhöhtes Gefährdungspotential aufweise. Diese Einschätzung liegt indessen nicht zuletzt im Vergleich zu anderen Branchen keineswegs auf der Hand. Hinzu kommt die Frage,

²⁶ *BaFin*, Big Data trifft auf künstliche Intelligenz, 2018, S. 13.

²⁷ *EU-Parlament*, EntschlieÙung v. 20.10.2020, P9_TA(2020)0276.

ob es überhaupt einer so strikten Regulierung durch eine europaweit geltende Verordnung bedarf oder ob es nicht sinnvoller ist, einen Soft Law-Ansatz zu wählen, insbesondere, indem zur Qualitätssicherung eine Zertifizierung eingeführt wird.

Die *EU-Kommission* wählt in ihrem nun vorgelegten Verordnungsvorschlag denn auch einen anderen Ansatz. Umfangreiche Regulierung erfahren demnach nur noch solche KI-Komponenten und KI-Produkte, die nach bestimmten produktrechtlichen EU-Rechtsakten einer Konformitätsbewertung bedürfen (z.B. Spielzeug, Medizinprodukte, Fahrzeuge). Der Einsatz von KI im Versicherungsunternehmen wird von dem Entwurf bis auf die Informationspflicht bei Kundeninteraktion nicht mehr berührt. Bleibt es bei diesem modifizierten Regelungsansatz, so lohnt es sich für die Versicherungswirtschaft über einen – von der Verordnung als Soft Law bevorzugten – KI-spezifischen Code of Conduct nachzudenken, um möglichen Erweiterungen der Verordnung vorzugreifen und zugleich einen rechtssicheren Einsatz der Technologie zu ermöglichen.

9 Ausblick

Welche Anforderungen bestehen für einen nachhaltigen Umgang mit KI-Systemen? Zusammenfassend lässt sich festhalten: Datenqualität und Transparenz sind wichtig. Die Haftungsrisiken müssen beachtet werden, nicht zuletzt im Datenschutzrecht. IT-Sicherheit sollte als Schwerpunktthema identifiziert werden. Die Modelle müssen nachvollziehbar und damit kontrollierbar werden, insbesondere für die versicherungs- und die datenschutzrechtlichen Aufsichtsbehörden und für die Gerichte. Erwägenswert erscheint es, auf europäischer Ebene anonymisierte Daten auszutauschen und damit höhere Datenmengen zu generieren als bislang, was den KI-Anwendungen zugutekommt. Sofern es jedem Versicherer überlassen bleibt, wie er mit den dadurch geschaffenen Datenbeständen verfährt, dürften dabei auch keine kartellrechtlichen Hürden zu überwinden sein.

Abschließend sei die grundlegende Frage aufgegriffen, ob KI-Systeme die drei großen Bereiche und Ziele der Nachhaltigkeit voranzubringen geeignet sind. Auf diese Frage kann es nur die typische Juristenantwort geben: Es kommt darauf an. Das Gesamtbild ist durchaus zwiespältig: Beispielsweise werden durch die Digitalisierung immer größere Stromressourcen benötigt, und dem sozialen Zusammenhalt sind KI-basierte Regulierungsentscheidungen ohne menschliche (Kulanz-)Spielräume eher abträglich. Allerdings bringen KI-Systeme in vielerlei Hinsicht auch unter dem Gesichtspunkt der Nachhaltigkeitskriterien Vorteile, etwa indem sie Entscheidungsprozesse optimieren und damit für mehr Rationalität, Fehlerfreiheit und Effizienz bei Vorgängen wie der Antragsannahme oder der Schadensregulierung sorgen. Wie das Beispiel der Telematik-Tarife in der Kfz-Versicherung zeigt, können sie auch über Verhaltensanreize regelkonformes Verhalten fördern und dadurch Sicherheitsstandards erhöhen, was letztlich wiederum qua Unfallvermeidung Ressourcen schont.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.