Einführung in das Recht der

Künstlichen Intelligenz

von

Thomas Söbbing
und
Alexander Schwarz

Kapitelübersicht

Gliederung

Einleitung und Verbreitung

Das Recht der Künstlichen Intelligenz (KI) ist in den vergangenen Jahren zu einem der dynamischsten und zugleich herausforderndsten Felder der Rechtswissenschaft avanciert. Zwischen technologischer Disruption, regulatorischer Ambition und ethischer Verunsicherung entstehen neue Fragestellungen, die sich in klassischen Rechtskategorien kaum einfangen lassen – und die dennoch einer juristisch präzisen Auseinandersetzung bedürfen. Mit dem vorliegenden Werk *„Einführung in das Recht der Künstlichen Intelligenz"* wird dem Leser ein strukturierter und zugleich praxisnaher Einstieg in diese komplexe und interdisziplinär geprägte Materie ermöglicht.

Wir haben uns entschieden, dieses Werk bei einem Verlag der Bedey & Thoms Media GmbH, Hermannstal 119k, in 22119 Hamburg als Paperpack Buch zu verlegen zulassen oder einmal als PDF zum kostenlosen Download zur Verfügung zu stellen, da man so eine größere Verbreitung erreichen kann und wir schneller auf Änderungen in diesem sich sehr schnell entwickelnden Rechtsgebiet reagieren können. Hierzu würden wir uns sehr über konstruktive Hinweise von Lesern und Leserinnen freuen bzw. sind wir darauf sogar angewiesen. Zudem wäre es toll, wenn der Leser oder die Leserin einen von mir (Thomas Söbbing) sehr geschätzten und von mir als Student mitgegründeten Verein mit einer Spende anstelle einer Vergütung für dieses Buch beim kostenlosen Download bedenken würde:

Step by Step e. V. Münster

https://www.stepbystep-muenster.de

Die Kontoverbindung lautet:

Volksbank Münsterland Nord eG
IBAN: DE51 4036 1906 0013 0761 00
BIC: GENODEM1IBB

Der Verein und die Leute dahinter machen wirklich eine großartige Arbeit und das schon seit über 30 Jahren.

Ziel des Werkes

Die Autoren verfolgen das Ziel, juristisch fundierte Grundlagen zu legen und zugleich systematisch in jene Rechtsfragen einzuführen, die für ein elementares Verständnis des KI-Rechts erforderlich sind. Gerade weil sich das Werk als „Einführung" versteht, wurde bewusst auf eine vertiefte Auseinandersetzung mit sektorspezifischen Themenfeldern wie algorithmischem Handel (Algotrading), KI in der Medizin oder im militärischen Kontext verzichtet. Solche Fragen überschreiten den Anspruch eines einführenden Zugangs und verlangen nach spezialisierten Monografien.

Stattdessen setzt dieses Buch dort an, wo sich der rechtliche Diskurs noch finden muss: an der Schnittstelle zwischen Technologie und Norm, zwischen methodischer Ungewissheit und juristischer Systembildung. Das Besondere an diesem Werk liegt im konzeptionellen Ansatz, eine erste juristische Ordnung in ein technisches Phänomen zu bringen, das sich einer festen Begriffsbildung bislang weitgehend entzieht. Damit bietet es nicht nur Studierenden und Juristen ohne spezifisches technisches Vorwissen einen Zugang, sondern auch Praktikern und Forschenden, die Orientierung in einem unübersichtlichen Feld suchen. Der systematische Aufbau des Buches erlaubt es, sich sowohl überblicksartig als auch selektiv in Einzelfragen zu vertiefen. Im Folgenden werden die einzelnen Kapitel des Buches in ihren zentralen Inhalten zusammengefasst:

Kapitel A: Algorithmen

Das Werk beginnt mit der rechtlichen Einordnung von Algorithmen, dem Grundelement vieler KI-Systeme. Es wird deutlich, dass der juristische Umgang mit dem Begriff des Algorithmus an strukturelle Grenzen stößt: Die verschiedenen Darstellungsformen – vom Entscheidungsbaum über mathematische Formeln bis zum Quellcode – lassen sich nicht einheitlich juristisch fassen. Der Abschnitt beleuchtet daher die unterschiedlichen Schutzmöglichkeiten, insbesondere im Urheberrecht (§ 69a UrhG), und diskutiert das Verhältnis zu Geschäftsgeheimnissen und der Frage algorithmischer Diskriminierung. Abgeschlossen wird das Kapitel mit einem kurzen Exkurs zum algorithmischen Handel.

Kapitel B: Maschinelles Lernen

Im Zentrum dieses Kapitels steht das maschinelle Lernen (ML) als technisches Rückgrat vieler moderner KI-Systeme. Die Autoren erläutern anschaulich die Grundprinzipien des

ML, die Unterschiede zu Deep Learning und künstlichen neuronalen Netzwerken. Im juristischen Teil geht es um Fragen des Schutzes solcher Systeme – urheberrechtlich, patentrechtlich, über das Datenbankrecht sowie das Geschäftsgeheimnisrecht

Kapitel C: Generative KI

Dieses Kapitel behandelt aktuelle Entwicklungen rund um generative KI – insbesondere große Sprachmodelle (LLMs) – und ihre rechtlichen Implikationen. Dabei stehen Fragen im Zentrum wie: Ist der Output einer KI urheberrechtlich geschützt? Wer ist Urheber von Prompts? Liegt im generierten Inhalt ein Geschäftsgeheimnis? Die Autoren greifen dabei auch aktuelle Streitfragen der urheberrechtlichen Werkqualität auf und bewerten den praktischen Umgang mit KI-generierten Inhalten. Eine zentrale Rolle spielt auch das Text- und Data Mining im Kontext der §§ 44b und 60d UrhG.

Kapitel D: Halluzination

Das Phänomen der KI-Halluzinationen – also von sachlich falschen oder erfundenen Ausgaben – wird in seiner zivilrechtlichen Relevanz betrachtet. Die juristische Bewertung erfolgt entlang der Kategorien des Sach- bzw. Produktmangels sowie unter dem Blickwinkel des Kauf- und Werkvertragsrechts. Auch SaaS-Modelle für KI und deren urheberrechtliche Implikationen werden hier behandelt.

Kapitel E: Datenschutz

Eines der zentralen Felder der KI-Regulierung ist der Datenschutz. Das Kapitel bietet eine fundierte Analyse der datenschutzrechtlichen Relevanz von ML-Systemen, insbesondere unter der DSGVO. Es wird geprüft, ob das Training von KI eine Verarbeitung personenbezogener Daten darstellt, wie Art. 6 DSGVO greift, und welche Rollen „Verantwortliche“ dabei einnehmen. Ergänzt wird das Kapitel durch eine eingehende Darstellung der EuGH-Entscheidung C-634/21 zur automatisierten Entscheidungsfindung.

Kapitel F: KI-Verordnung (KI-VO)

Mit diesem Kapitel beginnt der regulatorische Kernbereich des Werkes. Die Autoren erläutern systematisch die zentralen Bestimmungen der KI-Verordnung, insbesondere zu Hochrisikosystemen, Transparenzpflichten, Governance-Vorgaben und Sanktionen. Ein eigenes Unterkapitel widmet sich der Vertragspraxis, insbesondere dem Verhältnis von Art. 25 Abs. 4 KI-VO zu Art. 28 DSGVO. Der Abschnitt zum Qualitätsmanagement (Art.

17 KI-VO) beleuchtet eingehend die Anforderungen an Managementsysteme und stellt die KI-VO in den Kontext von ISO 42001, ISO 9001 und ISO 27001. Das Kapitel schließt mit einer kritischen Analyse der Herausforderungen für Unternehmen – Stichwort: Innovationshemmnisse und Bürokratisierung.

Kapitel G: Autonomes Fahren

In diesem Abschnitt geht es um das verkehrsrechtliche und haftungsrechtliche Umfeld des autonomen Fahrens. Die verschiedenen Automatisierungsstufen werden dargestellt und mit der geltenden Rechtslage – insbesondere StVG und StVO – abgeglichen. Dabei spielen Fragen der Hersteller- und Halterhaftung sowie der Datenverarbeitung eine zentrale Rolle.

Kapitel H: Haftung

Die Haftungsfrage stellt sich als eines der umstrittensten Themen der KI-Rechtsdogmatik dar. Das Kapitel systematisiert die Vorschläge zur KI-Haftungsrichtlinie, beleuchtet Beweislastfragen, Produkthaftung und die Rolle der KI als Erfüllungsgehilfe. Auch die spezifische Verantwortung von Betreibern und Wartungsverträgen wird behandelt.

Kapitel I: Embedded Law in KI

Ein besonders innovatives Kapitel beschäftigt sich mit der Einbettung von Normen in KI-Systeme („Embedded Law"). Anhand praktischer Beispiele – etwa im HR-Kontext oder beim autonomen Fahren – wird analysiert, wie regulatorische Anforderungen technisch implementiert werden können. Auch der „Super Code" und die Idee eines „maschinellen Gewissens" werden kritisch diskutiert.

Fazit und Wert des Werkes

Mit dem vorliegenden Buch gelingt es den Autoren, ein facettenreiches Themenfeld strukturiert aufzubereiten und damit eine juristisch tragfähige Grundlage für weiterführende Diskussionen zu schaffen. Dabei ist das Werk keine bloße Sammlung von Einzelaspekten, sondern ein kohärentes System, das die Grundlagen, Methoden und Konfliktlinien des KI-Rechts systematisch erschließt.

Die Entscheidung, sektorspezifische Spezialfragen auszusparen, ist konzeptionell konsequent: Sie erlaubt es, die Grundarchitektur der juristischen Auseinandersetzung mit KI freizulegen – und gerade darin liegt die Stärke des Buches. Der Leser erhält einen Zugang, der so in der juristischen Literatur bislang nicht gegeben war: interdisziplinär informiert, juristisch differenziert und didaktisch klar strukturiert.

Als Einführung richtet sich das Werk nicht nur an Studierende, sondern ebenso an Praktiker, die sich mit KI-Recht erstmals systematisch auseinandersetzen wollen. Durch seine klare Sprache, das hohe wissenschaftliche Niveau und die didaktische Klarheit kann es zu einem unverzichtbaren Referenzpunkt im deutschsprachigen Diskurs über das Recht der künstlichen Intelligenz werden.

Die Autoren dieses Werkes

Prof. Dr. Thomas Söbbing, LL.M. (HHU)
lehrt Zivilrecht mit dem Recht der Digitalen Wirtschaft a.d. Hochschule Kaiserslautern und hat einen Forschungsauftrag für die Rechtsfragen Künstlicher Intelligenz.

Alexander Schwarz
ist VRiOLG am Pfälzischen Oberlandesgericht in Zweibrücken und Lehrbeauftragter a.d. Hochschule Kaiserslautern.

Besonderen Dank gilt unserer Wissenschaftlichen Mitarbeiterin Janina Penth, LL.B. für ihre tatkräftige Unterstützung.

Disclaimer
Die hier gemachten Ausführungen geben lediglich die privaten Meinungen der Autoren wieder.

A. Algorithmen[1]

Grundsätzlich ist ein Algorithmus allgemeingültig und es handelt sich dabei um eine Arbeitsweise, wie eine Aufgabe zu lösen ist, ggf. mit Hilfe eines Computers. Diese recht einfache Definition umschreibt sehr gut das Problem, wenn es um die juristische Beurteilung geht. Denn diese Kriterien für die juristische Beurteilung sind zu ungenau. Die Formen und Darstellungsvarianten von Algorithmen sind zahlreich. Die mangelnde mathematische Genauigkeit des Begriffs Algorithmus störte viele Mathematiker und Logiker des 19. und 20. Jahrhunderts, weswegen in der ersten Hälfte des 20. Jahrhunderts eine ganze Reihe von Ansätzen entwickelt wurden, die zu einer genauen Definition führen sollten. Formalisierungen des Berechenbarkeitsbegriffs sind die Turingmaschine (Alan Turing), Registermaschinen, das Lambda-Kalkül (Alonzo Church), rekursive Funktionen, Chomsky-Grammatiken (siehe Chomsky-Hierarchie) und Markow-Algorithmen.

Obwohl es Algorithmen schon sehr lang gibt, ist der rechtliche Status von Algorithmen nicht eindeutig geklärt. Dies hängt sicherlich mit der Frage zusammen, was ein Algorithmus wirklich ist. Die Unklarheit ergibt sich aus einer wenig aussagekräftigen Definition, wonach ein Algorithmus ein methodisches Rechenverfahren zur Lösung eines Problems ist. Allgemein wird unter Algorithmus auch die Lösung einer konkreten Aufgabe verstanden, wobei elementare Verarbeitungsschritte der Schlüssel für das Ergebnis sind. Da es für künstliche Intelligenz (KI) und insbesondere Algorithmen bisher wenige Spezialnormen gibt, ist man stark auf Analogien bzw. die Auslegung anderer Normen angewiesen. So blickt man gerne auf das Urheberrecht, welches mit der Spezialnorm des § 69a UrhG ggf. durch die Auslegung auch einen Schutz für Algorithmen bieten könnte.

KI-Unternehmen investieren sehr viel Geld in die Schaffung von komplexen Algorithmen und so mehr stellt sich die ganze KI-Branche die Frage, wie sie ihre Investitionen schützen kann. Ganz aktuell zeigt sich dies in den Vereinigten Staaten und dem

[1] Siehe auch Algorithmen und urheberrechtlicher Schutz CR 2020, 223-228.

angestrebten (Teil-)Verkauf der Plattform "TikTok". Neben den (macht-)politischen Fragestellungen ergibt sich eine besondere Schwierigkeit in der besonderen Werthaltigkeit des Algorithmus der Plattform. Bei Systemen künstlicher Intelligenz[2] und insbesondere Algorithmen ist zwischen den unterschiedlichen Elementen für deren Entwicklung zu unterscheiden.[3]

Es kann grundsätzlich unterstellt werden, dass ein Algorithmus allein zunächst einmal nicht als Patent, auch in den unterschiedlichen Formen (siehe II.2-II.5), angemeldet werden kann, denn abstrakte oder intellektuelle Methoden sind nicht patentierbar, vgl. § 1 Abs. 2 und 3 PatG sowie Art. 52 Abs. 2 und 3 EPÜ. Das Bundespatentgesetz spricht in der Regel vom "Algorithmus als solchem" in Unterscheidung zum "Algorithmus mit technischem Inhalt"[4]. Ein Algorithmus kann generell den Schutz des Geschäftsgeheimnisgesetzes genießen, wenn seine Schöpfer dafür sorgen, dass die Voraussetzungen nach § 2 GeschGehG für einen Algorithmus erfüllt worden sind. Das Ergebnis ist aber wenig befriedigend, da die Möglichkeiten der Verwertung nicht die gleichen sind, wie bei urheberrechtlichen Werken (z. B. die des § 31 UrhG). Somit besteht der große Wunsch, dass Algorithmen einen urheberrechtlichen Schutz genießen sollten.

Der bisherige Fehler bei der rechtlichen Betrachtung von Algorithmen liegt darin begründet, dass man bei Algorithmen von einer feststehenden Form ausgeht[5], dass die Definitionen von Wissenschaftlern (vor allem Data-Scientists) doch sehr allgemein gehalten sind (siehe oben) und diese sich nur schwer rechtlich fassen lassen. Dabei gibt es sehr unterschiedliche Formen von Algorithmen (siehe II.2-II.5), welche somit auch unterschiedlich rechtlich betrachtet werden müssen. Die differenzierte Betrachtung muss insbesondere im Kontext des § 69a Abs. 1 und Abs. 2 UrhG erfolgen. Denn nach § 69a Abs. 1 UrhG sind Computerprogramme im Sinne dieses Gesetzes Programme in jeder Gestalt, einschließlich des Entwurfsmaterials. Nach § 69a Abs. 1 S. 1 UrhG gilt der gewährte Schutz für alle Ausdrucksformen eines

[2] S. zu verschiedenen Ausprägungen etwa *Stiemerling*, *O.* in: CR 2015, S. 762.
[3] *Antoine*, *L.* in: CR 2019, S. 1–8.
[4] BPatG, GRUR 1996, 866; GRUR 2015, 983 Rn 27.
[5] *Söbbing*, *T.*: Fundamentale Rechtsfragen künstlicher Intelligenz, 1. Auflage 2019, S. 11-14.

Computerprogramms (siehe III.), wovon auch das Entwurfsmaterial (siehe IV.2) und der Quellcode (siehe IV.3) erfasst sind. Dagegen sind gem. § 69a Abs. 1 S. 2 UrhG Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrundeliegenden Ideen und Grundsätze, nicht geschützt.

Somit könnte ein Algorithmus dadurch urheberrechtlichen Schutz i. S. v. § 69a UrhG erlangen, wenn die jeweilige Form des Algorithmus als Entwurfsmaterial oder Quellcode klassifiziert werden kann.

I. Transformation des Algorithmus

Algorithmen können in unterschiedlichen Formen dargestellt werden. Diese reichen von der mathematischen Formel bis zum konkret auf eine Maschine zugeschnittenen Programm. Dies liegt darin begründet, dass sich Algorithmen gut in Computerprogrammen umsetzen lassen (sog. Kompilieren), welche dann Algorithmen automatisiert durchführen.[6] Ein Algorithmus erlebt somit während seines Lebenszyklus eine gewisse Transformation[7] (siehe Abb. 1). Am Anfang steht immer das Problem (1), um das Problem zu visualisieren kann ein Entscheidungsbaum (2) erstellt werden, der Entscheidungsbaum wird umgesetzt, entweder in einen Pseudocode (3) oder eine mathematische Formel, z. B. einen euklidischen Algorithmus (4). Aus dieser Formel bzw. diesem Pseudocode wird ein Quellcode (5) generiert und dieser wird durch einen Compiler in ein Computerprogramm (6) transformiert und am Ende steht das Ergebnis (7).

[6] https://de.serlo.org/informatik/baustelle/algorithmen-ist-algorithmus, abgerufen am 03.03.2020.
[7] *von Rimscha, M.*: Algorithmen kompakt und verständlich – Lösungsstrategien am Computer, 4. Auflage 2017, S. 3.

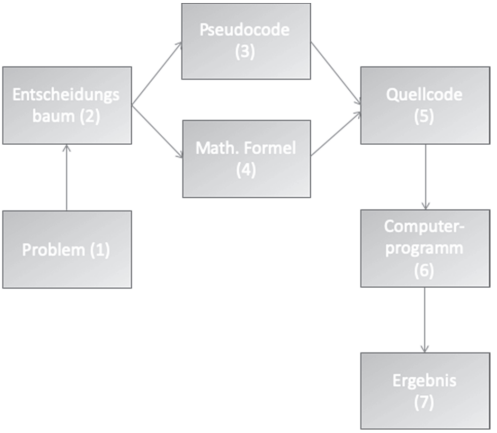


Abb. 1: Transformation eines Algorithmus

1. Entscheidungsbaum

Um Algorithmen zu entwickeln, kann man sich des Hilfsmittels der Entscheidungsbäume bedienen, was aber nicht zwingend notwendig ist. Entscheidungsbäume visualisieren abstrakte Probleme und machen diese für Menschen besser überschaubar. Ein klassischer Entscheidungsbaum, um in der Informatik die Arbeitsweisen von Algorithmen zu erläutern, ist der Entscheidungsbaum für die Überlebenschancen beim Untergang der Titanic (Abb. 2).[8] Analysiert wird dabei, welche Gruppen auf der Titanic beim Untergang am 15. April 1912 welche Überlebenschancen hatten:

[8] *Zweig*, *K.*: Ein Algorithmus hat kein Taktgefühl, 1. Auflage 2019, S. 140 ff.

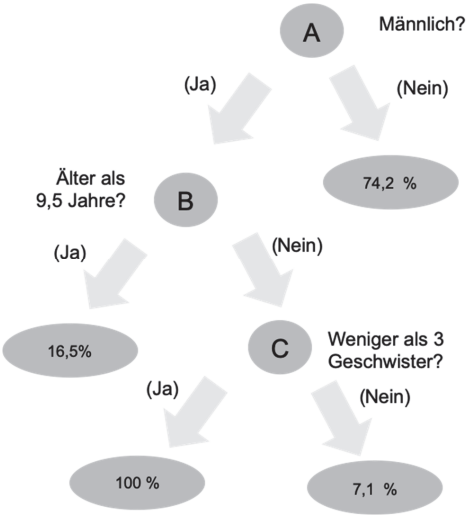


Abb. 2. Entscheidungsbaum

Die erste Frage (A) im Entscheidungsbaum ist, ob die Person, die auf der Titanic mitfuhr, männlich oder nicht männlich, sprich weiblich, gewesen ist. Wenn die Person weiblich war, so lag ihre Überlebenschance bei 74,2 %, denn 233 von 314 Frauen haben überlebt. Die zweite Frage (B) beschäftigt sich damit, ob die männliche Person älter als 9,5 Jahre gewesen ist, dann betrug die Überlebenschance 16,5 %. Denn von 545 Männern haben nur 90 Männer überlebt. Dritte Frage (C): War die männliche Person nicht älter als 9,5 Jahre und hatten diese weniger als drei Geschwister, dann lagen die Überlebenschancen bei 7,1 %, denn eines von 14 Kindern hat überlebt. Hatte das Kind mehr als drei Geschwister, dann betrug die Überlebenschance 100 %, denn 18 Kinder von 18 Kindern mit mehr als drei Geschwistern haben überlebt.[9] Natürlich könnte es beim Untergang eines anderen Schiffes zu ganz anderen Werten kommen. Aber darum geht es in dem vorliegenden Beispiel nicht, denn der Entscheidungsbaum ist lediglich die Vorlage, um zu erläutern, wie ein Entscheidungsbaum grundsätzlich arbeitet. Deutlich wird hier aber, dass entscheidend immer die Herausarbeitung der geeigneten Fragestellung ist. Ohne eine solche führt der

[9] Die Website www.kaggle.com/c/titanic (zuletzt abgerufen am 03.03.2020) bietet den kompletten Datensatz zu diesem Unglück an.

Entscheidungsbaum zwar zu nachvollziehbaren Ergebnissen, jedoch zu solchen ohne einen Erkenntnisgewinn.

2. Algorithmus als mathematische Formel

Die Darstellung von Algorithmen in mathematischen Formeln ist eine sehr verbreitete Methode. Exemplarisch dafür ist der euklidische Algorithmus, der aus dem mathematischen Teilgebiet der Zahlentheorie stammt.[10] Er dient daher im Folgenden für die juristische Betrachtung als Stellvertreter für einen generell mathematisch dargestellten Algorithmus. Mit einem euklidischen Algorithmus lässt sich der größte gemeinsame Teiler zweier natürlicher Zahlen berechnen. Das Verfahren ist nach dem griechischen Mathematiker Euklid benannt, der es in seinem Werk „Die Elemente" beschrieben hat.[11]

Der größte gemeinsame Teiler zweier Zahlen kann auch aus ihren Primfaktorzerlegungen ermittelt werden. Ist aber von keiner der beiden Zahlen die Primfaktorzerlegung bekannt, so ist der euklidische Algorithmus das schnellste Verfahren zur Berechnung des größten gemeinsamen Teilers. Der euklidische Algorithmus lässt sich nicht nur auf natürliche Zahlen anwenden. Vielmehr kann damit der größte gemeinsame Teiler von zwei Elementen eines jeden euklidischen Rings berechnet werden. Dazu zählen beispielsweise Polynome über einem Körper.[12]

Bei einem euklidischen Algorithmus ersetzt man die im klassischen Algorithmus auftretenden, wiederholten Subtraktionen eines Wertes jeweils durch eine einzige Division mit Rest. Der moderne euklidische Algorithmus führt nun in jedem Schritt solch eine Division mit Rest aus. Er beginnt mit den beiden Zahlen:[13]

$$A = a_1 * r_0 + r_1$$

[10] Wikipedia, Stichwort „Euklidischer Algorithmus", abgerufen am 29.02.2020.

[11] Das Verfahren wurde wahrscheinlich nicht von *Euklid* erfunden, da er in den „Elementen" die Erkenntnisse früherer Mathematiker zusammenfasste. Der Mathematiker und Historiker *Bartel Leendert van der Waerden* vermutet, dass Buch VII ein schon von den Pythagoreern verwendetes Lehrbuch der Zahlentheorie ist.

[12] Aus: *Euklid*, Die Elemente, herausgegeben von *Thaer*, *C.*, 1. Auflage 2011, § 2

[13] Wikipedia, Stichwort „Euklidischer Algorithmus", abgerufen am 29.02.2020.

In jedem weiteren Schritt wird mit dem Divisor und dem Rest des vorhergehenden Schritts eine erneute Division mit Rest durchgeführt. Und zwar so lange, bis eine Division aufgeht, das heißt, der Rest null ist:

$r_0 = q_2 * r_1 + r_2$

$r_0 = q_3 * r_1 + r_3$

.

.

$r_{n-1} = q_{n+1} * r_n + 0$

Der Divisor r_n der letzten Division ist dann der größte gemeinsame Teiler:

$ggT(a,b) = r_n$

Da sich die Zahlen in jedem zweiten Schritt mindestens halbieren, ist das Verfahren auch bei großen Zahlen extrem schnell.[14]
Dieses generelle Beispiel zeigt, dass der euklidische Algorithmus als eine abstrakte oder intellektuelle Methode zu verstehen ist, die sich mathematischer Funktionen bedient.

3. Pseudocode

Der Entscheidungsbaum dient lediglich der Visualisierung eines Algorithmus. Der Entscheidungsbaum ist natürlich noch kein Code, mit dem z. B. ein Computer Probleme lösen könnte.

Als notwendige Zwischenstufe der Transformation zwischen einer mathematischen Formel, wie die des euklidischen Algorithmus oder eines Entscheidungsbaums, und einem Computerprogrammcode ist der sog. Pseudocode notwendig. Der Pseudocode ist ein Programmcode, der nicht der maschinellen Interpretation, sondern lediglich der Veranschaulichung eines Paradigmas oder Algorithmus dient. Meistens ähnelt er

[14] Wikipedia, Stichwort „Euklidischer Algorithmus“, abgerufen am 29.02.2020.

höheren Programmiersprachen, gemischt mit natürlicher Sprache und mathematischer Notation. Mit dem Pseudocode kann ein Programmablauf unabhängig von zugrunde liegender Technologie beschrieben werden. Er ist damit oft kompakter und leichter verständlich als realer Programmcode.[15] Man kann ein Programm durch Pseudocode spezifizieren. Das sollte allerdings eher vermieden werden, denn die Formulierung als Pseudocode ist bereits eine Programmiertätigkeit, die von der Konzentration auf die Anforderungen ablenkt.[16] Setzt man den Entscheidungsbaum aus II.2 in einen Pseudocode um, würde dabei folgender Code entstehen:

```
START
Input männlich = 1
Input weiblich = 2
------------------------------------------------------------
REM „Grundfrage männlich oder weiblich“
IF Input = 1 THEN #2
ELSE #1
------------------------------------------------------------
END
------------------------------------------------------------
#1 REM „weiblich“
  PRINT „Überlebenschance bei 74,2 %“
END
------------------------------------------------------------
#2 REM „männlich“
  IF Input </= 9,5 Jahre THEN
          PRINT „Überlebenschance bei 16,5 %“
  ELSE
          IF Input </= 3 Geschwister THEN
          PRINT „Überlebenschance bei 7,1 %“
  ELSE
```

[15] *Mehlhorn*, *K.* / *Sanders*, *P.*: Algorithms and Data Structures, 2008, S. 26.
[16] *Siedersleben*, *J.* (Hrsg.): Softwaretechnik, Hanser, 2003, S. 44 ff.

```
        PRINT „Überlebenschance bei 100 %“
END
-----------------------------------------------------------
END
```

Dabei haben alle Worte in Großbuchstaben eine entsprechende Funktion und enthalten kleingeschriebene Worte eine Variable, sofern sie nicht in Anführungsstrichen stehen und damit lediglich eine beschreibende Funktion haben.

Entscheidend beim Pseudocode ist, dass diese Form der Darstellung eines Algorithmus schon sehr nah an einem eigentlichen Programmcode ist.

4. Quellcode

Eine Software besteht aus einem Quellcode, der eine Maschine (Computer) dazu veranlasst, bestimmte Befehle auszuführen.[17] Quelltext, auch Quellcode (englisch: source code) oder unscharf Programmcode genannt, ist in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes. Abstrakt betrachtet, kann der Quelltext für ein Programm auch als Software-Dokument bezeichnet werden, welches das Programm formal so exakt und vollständig beschreibt, dass dieses aus ihm vollständig automatisch von einem Computer in Maschinensprache übersetzt werden kann.[18] Wie bereits unter beschrieben, unterscheiden sich Pseudocode und Quellcode in ihrer Darstellung nicht sehr voneinander.

Der Besitz des Quellformats beinhaltet die Möglichkeit zur Bearbeitung und Änderung eines Programms und dadurch das Risiko unkontrollierbarer Piraterie: Wer über das Quellformat eines Programms verfügt, kann alle Hinweise auf den Urheber, insbesondere Copyright-Vermerke und Seriennummern, beseitigen und umfangreiche Änderungen innerhalb der Programmstruktur vornehmen. Aus diesem Grund wird

[17] *Antoine*, *L.* in: CR 2019, S. 1-8.
[18] Wikipedia, Stichwort „Quellcode“, abgerufen am 01.03.2020.

dem Anwender grundsätzlich nur das Programm im Objektformat überlassen; denn sonst würde er das im Programm enthaltene EDV-technische Know-how offenlegen und einer unkontrollierbaren Weiternutzung anheimgeben.[19]

II. Urheberrecht (§ 69a UrhG)

Für den Rechtsschutz nach dem UrhG ist der Unterschied zwischen einem Quellcode für eine Software und einem Algorithmus für eine KI von erheblicher Bedeutung. Denn es stellt sich die Frage, ob ein Algorithmus als Quellcode für ein Computerprogramm angesehen werden könnte und darüber den entsprechenden urheberrechtlichen Schutz erlangen könnte.

1. Schutzbereich des § 69a Abs. 1 UrhG

Das Computerprogramm ist nach den Vorgaben der §§ 2 Abs. 1 Ziff. 1 Abs. 2, 69a UrhG urheberrechtlich geschützt. Nach § 2 Abs. 1 Nr. 1 UrhG wird ein Computerprogramm als Sprachwerk eingeordnet.[20] Die Analogie zum Sprachwerk ist vor allem in Bezug auf den Programmcode selbst sehr passend.[21] Auch die natürliche Sprache besitzt mit ihrer Grammatik ein festes Regelwerk, welches befolgt werden muss, um einen richtigen und verständlichen Satz formulieren zu können. Beim Programmieren ist dies die Syntax der verwendeten Programmiersprache.[22] Es gibt unzählige Möglichkeiten, einen Programmcode zu schreiben, um eine Funktionalität umzusetzen. Diese Möglichkeiten werden durch Syntax der Programmiersprache, verfügbare technische Infrastruktur, angesteuerte Drittprogramme, Konventionen sowie Stilvorgaben eingeschränkt. [23] Dabei ist die Ausgestaltung des Code-Schreiben entscheidet, denn hier muss ein individueller Akt als Vorsausetzung des Urheberrechtsschutzes für Software vorliegen.[24]

Darüber hinaus muss sehr fein unterschieden werden, denn Software ist gem. § 69a Abs. 1 UrhG auch hinsichtlich der konkreten Ausdrucksform – im Gegensatz zu den

[19] *Hoeren*, *T.* in: CR 2004, 721-724.

[20] BGH, Urt. v. 3.3.2015 – I ZR 111/02, GRUR 2005, 860 (861) = MMR 2005, 845 (846) – Fa- sh 2000; OLG Frankfurt, Urt. v. 27.1.2015 – 11 U 94/13, GRUR 2015, 784 (787) = ZUM 2015, 497 (501) – Objektcode; Loewenheim in Schricker/Loewenheim, Urheberrecht 5. Aufl. 2017, § 2 Rz. 143 mit weiteren Nachweisen

[21] *Hoeren/Wehkamp,* CR 2018, 1-7.

[22] Vgl. Deselby, Journal of dyslexic programming 13 (2017), 131 ff.;

[23] *Hoeren/Wehkamp,* CR 2018, 1-7.

[24] *Hoeren/Wehkamp,* CR 2018, 1-7.

dem Programm zugrunde liegenden Ideen und Grundsätzen sowie den Funktionalitäten eines Computerprogramms – urheberrechtlich schutzfähig.[25] Nach diesen Bestimmungen erstreckt sich der Schutz auf Computerprogramme in jeder Gestalt, einschließlich des Entwurfsmaterials, vgl. § 69a Abs. 1 und 2 UrhG, während „Ideen und Grundsätze", die – nach der gesetzlichen Formulierung – „einem Element eines Computerprogramms zugrunde liegen", nach § 69a Abs. 2 Satz 2 UrhG ausdrücklich nicht dem Urheberschutz unterfallen.[26] Der EuGH hat in den Entscheidungen „BSA"[27] und „SAS Institute"[28] den Schutzbereich des Art. 1 SoftwareRL konkretisiert. Dieser umfasst die Ausdrucksformen eines Computerprogramms und das Entwurfsmaterial, das zur Vervielfältigung oder späteren Entstehung eines Computerprogramms führen kann.[29] Der Ausdrucksform eines Computerprogramms komme ab dem Moment Schutz zu, ab dem deren Vervielfältigung die Vervielfältigung des Computerprogramms zur Folge hätte und auf diese Weise der Computer zur Ausführung seiner Funktion veranlasst werden könne.[30] Der Schutz bezieht sich damit auf das reine Programm als solches, also auf „eine Folge von Befehlen, die nach Aufnahme in einen maschinenlesbaren Träger fähig sind zu bewirken, dass eine Maschine mit informationsverarbeitenden Fähigkeiten eine bestimmte Funktion oder Aufgabe oder ein bestimmtes Ergebnis anzeigt, ausführt oder erzielt".[31] Der Begriff des Computerprogramms ist zwar weit zu verstehen, betrifft aber doch nur Funktionen, die auf elektronischer Datenverarbeitung beruhen. Er erfasst z. B. Betriebssysteme, Anwendungsprogramme, Makros, Suchmaschinen, den Quellcode und auch einzelne Programmteile. Weiter ist nach der ausdrücklichen Formulierung des Gesetzes in § 69a Abs. 1 UrhG auch Entwurfsmaterial geschützt, darunter sind aber ebenfalls nur EDV-Materialien zu verstehen. Von der Einbeziehung erfasst sind sämtliche Vorstufen, wie etwa ein Flussdiagramm oder sonstige Vor- und Zwischenstufen der

[25] *Hetmank*, *S. / Lauber-Rönsberg*, *A*. in: GRUR 2018, S. 574.

[26] OLG Köln, 08.04.2005 – 6 U 194/04 = GRUR 2005, S. 863 (Ls.), GRUR-RR 2005, S. 303, K&R 2006, S. 43.

[27] EuGH, Urt. v. 22.12.2010 – C-393/09 = CR 2011, S. 221 (222) – BSA.

[28] EuGH, Urt. v. 02.05.2012 – C-406/10, CR 2012, S. 428 – SAS Institute m. Anm. *Heymann*.

[29] EuGH, Urt. v. 22.12.2010 – C-393/09, CR 2011, S. 221 (222) – BSA, Rz. 37; EuGH, Urt. v. 02.05.2012 – C-406/10, CR 2012, S. 428 – SAS Institute, Rz. 37. Bezugnahme auch durch vorl. schwed. Gericht, Svea Hovrätt, Beschl. v. 04.03.2018 – PMT 22-17 (in schwed. Sprache): http://www.patentochmarknadsoverdomstolen.se/Domstolar/pmod/2018/Svea%20HR%20PMT%2022-17%20Ej%20slutligt%20beslut%202018-04-03.pdf (letzter Abruf jeweils 10.12.2018), s. Rz. 19.

[30] EuGH, Urt. v. 22.12.2010 – C-393/09, CR 2011, S. 221 (222) – BSA, Rz. 38.

[31] vgl. *Dreier*, *T.* / *Schulze*, *G.*: Urheberrechtsgesetz, 2. Auflage, § 69a Rz. 12.

Programmentwicklung.[32] Demgegenüber sind die außerhalb der EDV liegenden Aufgabenstellungen und Vorgaben an den Programmierer als Ideen und Grundsätze, die einem Computerprogramm zugrunde liegen, nicht durch die §§ 69a ff. UrhG in den urheberrechtlichen Schutz einbezogen. Insbesondere ist die Idee, zur Lösung einer bestimmten Aufgabe überhaupt ein Programm zu entwickeln, nicht von § 69a UrhG erfasst. Geschützt ist also allein die Form als der konkrete Ausdruck eines Werkes, nicht hingegen der Werkinhalt.[33] Dies bedeutet, dass der Urheber nach dieser Bestimmung nur derjenige sein kann, der bestimmte von ihm selbst entwickelte oder ihm von dritter Seite vorgegebene Aufgabenstellungen in ein Computerprogramm umsetzt. Demgegenüber ist derjenige, der die Aufgabe stellt, also – möglicherweise auch sehr ins Detail gehend – die Anforderungen vorgibt, die das Programm erfüllen soll, nicht gleichzeitig Urheber des Programms. Das folgt aus dem Umstand, dass die Bestimmungen der §§ 69a ff. UrhG nur speziell Computerprogramme als urheberrechtsfähig schützen und damit darauf abstellen, dass eine eigene geistige Schöpfung des Betreffenden sich gerade als Computerprogramm niederschlägt (§ 69a Abs. 3 UrhG). Es kann indes nicht jemand auch nur Miturheber eines Computerprogramms sein, der selbst keinerlei Programmierarbeit eigenverantwortlich geleistet hat. Das gilt auch dann, wenn seine intellektuellen Vorarbeiten den Erfolg der Programmiertätigkeit erst ermöglicht haben.

2. Entwurfsmaterial

Für Entwurfsmaterial ist weitgehend offen, ab wann und bis zu welchem Zeitpunkt der Schutz greifen soll.[34] In der bisherigen Rechtspraxis schien das auch keine große Rolle zu spielen, weil es zu wenigen rechtlichen Auseinandersetzungen darüber kam.[35] Der Erwägungsgrund 7 der SoftwareRL[36] spricht insoweit nur dann von Entwurfsmaterial, „sofern die Art der vorbereitenden Arbeit die spätere Entstehung eines Computerprogramms zulässt". Entscheidend ist nach dem Wortlaut, dass Entwurfsmaterial geeignet bzw. soweit gediehen sein muss, um auf seiner Basis ein

---

32 Dreier, *T.*: Urheberrecht, 2. Auflage, § 69a, Rz. 14.

[33] vgl. OLG Karlsruhe, GRUR 94, S. 726, 729 – „Bildschirmmasken"; *Dreier*, *T.* / *Schulze*, *G.* a.a.O., Rz. 20; *Schricker*, *G.* / *Löwenheim*, *U.*: Urheberrecht, § 69a, Rz. 12; *Möhring*, *P.* / *Nicolini*, *K.*: Urheberrechtsgesetz, 2. Aufl. § 69a, Rz. 9.

[34] *Antoine*, *L.* in: CR 2019, S. 1-8.

[35] Ausnahme OLG Köln, 08.04.2005 – 6 U 194/04 = GRUR 2005, S. 863 (Ls.); GRUR-RR 2005, S. 303; K&R 2006, S. 43.

[36] RL 91/250/EWG v. 14.05.1991, ersetzt durch konsolidierte Fassung als RL 2009/24/EG v. 23.04.2009 über den Rechtsschutz von Computerprogrammen, folgend „SoftwareRL".

Computerprogramm in Codeform schreiben zu können.[37] Folgern lässt sich für einen Schutz als Entwurfsmaterial, dass eine hinreichende technische Nähe zum Programm in Codeform bestehen muss.[38] Dabei sind technische Spezifikationen und Programmvorgaben, wie Datenflusspläne und Programmablaufpläne sowie technische Grob- und Feinspezifikation, als Entwurfsmaterial schutzfähig.[39] Die darin festgelegten Anforderungen beziehen sich unmittelbar auf die Erstellung des Programms, so dass eine hinreichende Nähe zu diesem vorliegt – wenn auch in Frage steht, ob lediglich auf dieser Basis eine Codierung möglich ist.[40] Somit lässt sich festhalten, dass Entwurfsmaterial ab dem Zeitpunkt vorliegt, ab dem es möglich ist, auf Basis dessen ein Programm zu schreiben. Sobald eine Entwicklungsstufe erreicht wird, die Steuerungsbefehle in Codeform umsetzt und damit den Programmbegriff erfüllt, würde es sich nicht mehr um Entwurfsmaterial, sondern das Programm selbst handeln.[41]

Wenn man diese Erkenntnis auf die unterschiedlichen Formen eines Algorithmus anwendet, so ist zunächst einmal beim Entscheidungsbaum, so wie er dargestellt worden ist, kein Entwurfsmaterial für ein späteres Computerprogramm anzunehmen. Denn nach § 69a Abs. 2 S. 2 UrhG sind Ideen und Grundsätze, die einem Element eines Computerprogramms zugrunde liegen, einschließlich der den Schnittstellen zugrunde liegenden Ideen und Grundsätze, nicht geschützt. Die Ausprägungen beim Entscheidungsbaum haben noch nicht die Entwicklungsstufe erreicht, um Steuerungsbefehle (jetzt schon) in Codeform umzusetzen. Zumindest nicht, ohne dass weitere Zwischenschritte notwendig sind. Anders verhält es sich, wenn der Entscheidungsbaum schon eine solche Qualität erreicht, dass er als Programmablaufplan, z. B. nach DIN 66001 oder ISO 5807, gelten kann. Solche Programmablaufpläne genießen

[37] *Grützmacher*, *M.* in: *Wandtke*, *A.* / *Bullinger*, *W.*: UrhG, 4. Aufl. 2014, § 69a, Rz. 7; *Schneider*, *J.* in: *Schneider*, *J.*: Handbuch EDV-Recht, 5. Aufl. 2017, G. Rz. 79; *Karl*, *C.*: Der urheberrechtliche Schutzbereich von Computerprogrammen, 2009, S. 191 f.; vgl. *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5. Aufl. 2017, § 69a, Rz. 5.

[38] Unter Berücksichtigung der Sichtweise des BGH: *Antoine*, *L.* in: CR 2019, S. 1-8.

[39] BGH, Urt. v. 09.05.1985 – I ZR 52/83, CR 1985, S. 22 – Inkassoprogramm; *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5. Aufl. 2017, § 69a Rz. 5; s. a. *Schneider*, *J.* in: *Schneider*, *J.*: Handbuch EDV-Recht, 5. Aufl. 2017, G Rz. 117.

[40] *Antoine*, *L.* in: CR 2019, S. 1-8.

[41] *Antoine*, *L.* in: CR 2019, S. 1-8.

durchaus als Entwurfsmaterial den Schutz nach § 69a Abs. 1 und Abs. 2 S. 1 UrhG.[42] Bei Entscheidungsbäumen kommt es daher sehr auf den Einzelfall an.

Bei der Darstellung eines Algorithmus durch eine mathematische Formel ist es höchstwahrscheinlich nicht möglich, ohne weitere (größere) Zwischenschritte einen Programmcode zu erzeugen. Es fehlt eine hinreichende technische Nähe zum Programm in Codeform.[43] Somit ist die Darstellung eines Algorithmus in der Form einer mathematischen Formel nicht ausreichend, um als Entwurfsmaterial den urheberechtlichen Schutz des § 69a Abs. 1 UrhG zu erlangen.

Dagegen ist beim Pseudocode schon deutlich von einem Entwurfsmaterial auszugehen, da der Pseudocode eine Entwicklungsstufe erreicht hat, die ausreichend ist, um ihn für Steuerungsbefehle in Codeform umzusetzen. Der Pseudocode ist durch seine Form einer Programmiersprache schon sehr nah am eigentlichen Programmcode/Quellcode.

Der Quellcode (II.5) bedarf keiner Kategorisierung als Entwurfsmaterial, da gem. § 69a Abs. 1 UrhG Computerprogramme im Sinne dieses Gesetzes Programme in jeder Gestalt sind. Hierzu zählt ebenfalls der Quellcode.[44]

3. Quellcode

Wie bereits oben dargestellt fällt auch der Quellcode in den Schutzbereich des § 69a Abs. 1 UrhG. Fraglich ist, ob der beschriebene Pseudocode, als Methode zur Versinnlichung eines Algorithmus, den Schutz nach § 69a Abs. 2 S. 1 UrhG durch den Vergleich zu einem Quellcode verdient.

Darauf, dass die Software ablauffähig ist, kommt es angesichts der Formulierung „aller Ausdrucksformen" (vgl. § 69a Abs. 2 UrhG), was z.B. auch den Quellcode einschließt, nicht an.[45] Dies würde grundsätzlich dafür sprechen, dass der Pseudocode einen vergleichbaren Schutz wie der Quellcode erlangen könnte. Aber für den Programmbegriff legt der EuGH mit seiner Bezugnahme auf die Funktionsveranlassung als entscheidendes Kriterium ein Steuerungselement zugrunde, was dem Verständnis

[42] BGH, Urt. v. 09.05.1985 – I ZR 52/83, CR 1985, S. 22 – Inkassoprogramm; *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5. Aufl. 2017, § 69a, Rz. 5; s. a. *Schneider*, *J.* in: *Schneider*, *J.*:Handbuch EDV-Recht, 5. Aufl. 2017, G Rz. 117.

[43] Unter Berücksichtigung der Sichtweise des BGH: *Antoine*, *L.* in: CR 2019, S. 1-8.

[44] EuGH v. 2.5.2012 C-406/10 = CR 2012, 428.

[45] *Schneider* in Schneider, Hdb. EDV-Recht, 5. Aufl. 2017, G. Rn. 54.

des nationalen Urheberrechts entspricht.[46] Aber gerade an solchen „tatsächlichen" Steuerungselementen fehlt es beim Pseudocode, da dieser nur der Veranschaulichung des Algorithmus dient. Der Pseudocode ist kompakter und leichter verständlich als realer Programmcode,[47] erzeugt aber nicht solche Befehle für einen Computer, die tatsächlich dazu führen, dass ein lauffähiges Computerprogramm entsteht. Denn hinsichtlich des Programms ergibt sich ein primärer Zuschnitt auf die in Codeform ausgedrückten Steuerungsbefehle (in Quell- oder Objektcode) als Schutzgegenstand.[48] Nicht steuerungsbezogenen Elementen soll Schutz nur nach allgemeinen Vorschriften zukommen.[49] Ein Schutz nach allgemeinen Vorschriften kann sich daraus ergeben, dass sich der Pseudocode als Entwurfsmaterial (siehe III.2) in den Schutzbereich des § 69a Abs. 2 S. 1 UrhG bringen lässt.

Somit lässt sich im Ergebnis festhalten, dass die Darstellung eines Algorithmus in der Form eines Pseudocodes nicht den Schutz des § 69a Abs. 2 S. 1 UrhG verdient, wenn dieser aus der Vergleichbarkeit zum Quellcode entstehen soll.

4. Einfluss der KI auf das Coding

Künstliche Intelligenz (KI) hat in den letzten Jahren die Art und Weise, wie Software entwickelt wird, tiefgreifend verändert. Besonders im Bereich der Code-Generierung zeigen sich enorme Fortschritte: Moderne Werkzeuge wie GitHub Copilot (entwickelt von GitHub und OpenAI), Amazon CodeWhisperer oder ChatGPT können auf Grundlage natürlicher Sprache oder einfacher Kommentare im Code vollständige Funktionen oder Code-Vorschläge generieren. Sie analysieren dabei nicht nur den unmittelbaren Kontext, sondern greifen auf umfangreiche Trainingsdaten zurück, um relevante und syntaktisch korrekte Vorschläge zu machen.

Ein besonderer Vorteil dieser Tools liegt in der Automatisierung sogenannter Boilerplate-Aufgaben. Dabei handelt es sich um sich wiederholende und oft mechanische

[46] *Marly*, *J.*: GRUR 2011, S. 204 (207); s. *Grützmacher*, *M.* in: *Wandtke*, *A.* / *Bullinger*, *W.*: UrhG, 4. Aufl. 2014, § 69a, Rz. 3 m. w. N.

[47] *Mehlhorn*, *K.* / *Sanders*, *P.*: Algorithms and Data Structures, 2008, S. 26.

[48] Laut EuGH Quell- und Objektcode lediglich Beispiele der Ausdrucksform, s. *Marly*, *J.*: GRUR 2012, S. 773 (777 f.); *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5. Aufl. 2017, § 69a, Rz. 10.

[49] Vgl. *Lesshafft*, *K.* / *Ulmer*, *D.* in: CR 1993, S. 607 (608); s. a. *Marly*, *J.* in: GRUR 2011, S. 204 (207); vgl. *Loewenheim*, *U.* / *Spindler*, *G.* in: *Schricker*, *G.* / *Loewenheim*, *U.*: UrhG, 5. Aufl. 2017, § 69a, Rz. 7, jew. hins. Bildschirm bzw. Benutzer-Oberflächen; vgl. auch EuGH, Urt. v. 22.12.2010 – C-393/09, CR 2011, S. 221 (222) – BSA.

Programmierarbeiten – etwa das Schreiben von Settern und Gettern, das Anlegen von REST-API-Endpunkten oder das Generieren einfacher Unit Tests und Validierungslogiken. Diese Prozesse lassen sich mithilfe KI-basierter Werkzeuge erheblich beschleunigen oder vollständig automatisieren, was Entwicklerinnen und Entwicklern mehr Raum für kreative und konzeptionelle Aufgaben gibt.

Darüber hinaus fördern KI-Systeme auch die Verbreitung von Low-Code- und No-Code-Plattformen. Solche Plattformen ermöglichen es, komplexe Anwendungen weitgehend ohne klassisches Programmieren zu erstellen. Benutzeroberflächen, Datenbanken oder Automatisierungsabläufe lassen sich per Drag-and-Drop oder durch einfache Befehle konfigurieren. Dieser Trend demokratisiert die Softwareentwicklung, da er auch Menschen ohne tiefgehendes technisches Know-how in die Lage versetzt, digitale Lösungen zu entwickeln. Gleichzeitig bringt diese Entwicklung neue Herausforderungen mit sich, insbesondere in Bezug auf Codequalität, Wartbarkeit und Sicherheit.

Insgesamt lässt sich feststellen, dass KI-gestützte Tools keineswegs das Programmieren im klassischen Sinne obsolet machen – sie verändern jedoch grundlegende Abläufe, verschieben Kompetenzanforderungen und eröffnen neue Formen der Mensch-Maschine-Kollaboration.

Im Zentrum der urheberrechtlichen Bewertung KI-generierten Codes steht die Frage, ob es sich bei solchen Erzeugnissen um persönliche geistige Schöpfungen im Sinne des § 2 Abs. 2 UrhG handelt. Der deutsche Urheberrechtsschutz knüpft zentral an die Individualität und das schöpferische Wirken einer natürlichen Person an. Nur Werke, die Ausdruck der persönlichen geistigen Leistung eines Menschen sind, können unter den Schutz des Urheberrechts fallen. Eine maschinelle Leistung – auch wenn sie formal dem Werkbegriff des § 2 Abs. 1 UrhG (hier konkret: Sprachwerke, einschließlich Computerprogramme gem. § 69a UrhG) zuzuordnen wäre – genügt dem nicht.[50]

KI-Systeme wie GitHub Copilot, ChatGPT oder Amazon CodeWhisperer operieren auf Basis statistischer Mustererkennung in großen Text- bzw. Codekorpora. Der

[50] Vgl. *Dreier/Schulze*, UrhG, 7. Aufl. 2022, § 2 Rn. 41 ff.; *Wandtke/Bullinger*, Urheberrecht, 6. Aufl. 2022, § 2 Rn. 100: „Voraussetzung ist stets ein individueller geistiger Akt des Menschen."

generative Akt – d.h. die konkrete Auswahl, Kombination und Ausformulierung von Codebestandteilen – erfolgt autonom durch das System, ohne menschliche Interventionsentscheidung im Einzelfall. Zwar erfolgt das Prompting durch den Nutzer, doch bleibt dieser Input regelmäßig auf allgemeine Instruktionen („Schreibe eine Funktion zur Umrechnung von Celsius in Fahrenheit") beschränkt. Es fehlt damit an einer eigenpersönlichen Gestaltungsentscheidung des Menschen hinsichtlich des konkreten Ausdrucks des Werkes.[51]

Die herrschende Meinung in der Literatur und die bisherige deutsche Rechtsprechung betonen durchgehend, dass eine persönliche geistige Schöpfung im Sinne des § 2 Abs. 2 UrhG eine individuelle Entscheidungsspielraum bei der Gestaltung voraussetzt, der gerade nicht in einer bloßen Bedienhandlung bestehen darf.[52] Eine bloße Nutzung technischer Hilfsmittel (z. B. Textverarbeitung, IDEs) steht der Schutzfähigkeit des Ergebnisses nicht entgegen – im Gegensatz zur vollständigen Delegation der Gestaltungsentscheidung an eine Maschine, wie sie bei KI-generiertem Code typischerweise vorliegt.

Daher ist nach geltender Rechtslage festzuhalten:

- KI-generierter Quellcode ist mangels menschlicher schöpferischer Leistung nicht als Werk im Sinne des § 2 Abs. 2 UrhG anzusehen und damit nicht urheberrechtlich geschützt.
- Der KI-Anwender erlangt mangels eigener individueller Gestaltungsentscheidung keine Urheberschaft am erzeugten Code, es sei denn, er nimmt substanzielle schöpferische Bearbeitungen vor (§ 3 UrhG).
- Die KI selbst kann mangels Rechtspersönlichkeit nicht Träger von Urheberrechten sein.[53]

In der Konsequenz steht KI-generierter Code, jedenfalls nach deutschem Urheberrecht, regelmäßig gemeinfrei zur Verfügung – es sei denn, es liegt eine menschliche

[51] Siehe dazu ausführlich: *J. Ohly*, „Maschinelles Lernen und Urheberrecht – Wer schafft was?", GRUR 2021, 25 (28 f.); sowie *M. Leistner*, „Generative KI und das Urheberrecht", GRUR 2023, 665

[52] BGH GRUR 1982, 37 – Inkasso-Programm; BGH GRUR 2015, 1189 – Pippi-Langstrumpf-Kostüm; LG Frankfurt a.M., Urt. v. 17.07.2023 – 2-06 O 52/23 (nicht rechtskräftig, vgl. GRUR-RS 2023, 19044).

[53] Vgl. auch die Mitteilung der EU-Kommission zur KI und geistigem Eigentum, COM (2020) 760 final, S. 7: „Rechtsfähigkeit und Urheberschaft können nur natürlichen Personen zukommen.

Mitwirkung vor, die über rein technische Steuerung hinausgeht und eine individuelle kreative Prägung erkennen lässt.

5. Resümee

Zusammenfassend lässt sich sagen, dass Algorithmen abhängig von ihrer unterschiedlichen Form einen urheberrechtlichen Schutz genießen oder auch nicht.

Somit wird die Darstellung eines Algorithmus in der Form eines einfachen Entscheidungsbaums i. d. R. keinen urheberrechtlichen Schutz genießen. Anders verhält es sich, wenn der Entscheidungsbaum schon die Qualität eines Programmablaufplanes erreicht. Bei einem mathematischen dargestellten Algorithmus, wie dem euklidischen Algorithmus, ist kein urheberrechtlicher Schutz anzunehmen. Dagegen ist bei der Darstellung eines Algorithmus in einem Pseudocode durchaus von einem urheberrechtlichen Schutz auszugehen, auch wenn dieser nicht aus der Vergleichbarkeit zum Quellcode zu entnehmen ist, sondern als Entwurfsmaterial entsprechenden urheberrechtlichen Schutz genießt.

III. Diskriminierung durch Algorithmen[54]

„Diskriminierung" bezeichnet eine Benachteiligung oder Herabwürdigung von Gruppen oder einzelnen Personen nach Maßgabe bestimmter Wertvorstellungen oder aufgrund unreflektierter, z. T. auch unbewusster Einstellungen, Vorurteile oder emotionaler Assoziationen.[55] Dabei werden Diskriminierungen aufgrund von Faktoren, welche vom Betroffenen beeinflussbar sind (Zugangsberechtigung zu Bildungseinrichtungen, Einkommenshöhe, soziales Verhalten), tendenziell eher akzeptiert oder toleriert als individuell nicht veränderbare Faktoren und Auslöser von Diskriminierungen (Ethnie, Geschlecht, Behinderung, Alter oder sexuelle Präferenzen).[56] Generell gilt das, was das Bundesverfassungsgericht über den Umgang mit dem Gleichheitsgrundsatz des Art. 3 GG ausdrückt: „Der allgemeine Gleichheitssatz des Art. 3 Abs. 1 GG gebietet dem Gesetzgeber, wesentlich Gleiches gleich und wesentlich Ungleiches ungleich zu behandeln."[57]

---

[54] Siehe auch „*Das Märchen vom bösen Algorithmus oder rechtliche Fragen zur Diskriminierung durch künstliche Intelligenz (KI)",* Söbbing RTLaw 2020, 62-69.

[55] *Epping*, *V.*: Grundrechte, 7. Auflage 2017, Rn. 770.

[56] *Weise*, *P.*; *Brandes*, *W.*; *Eger*, *T.*; *Kraft*, *M.*: Neue Mikroökonomie, Physica, Heidelberg 2005, S. 22.

[57] BVerfGE 98, S. 365 (385).

1. Art. 3 GG – „Gleichheitsgebot“

Art. 3 Absatz 1 GG enthält den allgemeinen Gleichheitssatz, der den Staat zur Gleichbehandlung aller Menschen verpflichtet. Gem. Art. 3 Abs. 1 GG sind alle Menschen vor dem Gesetz gleich. Art. 3 Abs. 1 GG schützt, anders als die meisten anderen Grundrechte, keine bestimmte Freiheitssphäre vor hoheitlichen Eingriffen. Dies beruht darauf, dass es sich bei diesem Grundrecht nicht um ein Freiheits-, sondern um ein Gleichheitsrecht handelt. Seine Gewährleistung ergibt sich daher erst aus einem Vergleich mehrerer Sachverhalte in Bezug auf ihre Behandlung durch den Staat. Art. 3 Abs. 1 GG verpflichtet diesen, gleiche Sachverhalte gleich zu behandeln.[58] Ungleichbehandlungen kann der Bürger mithilfe dieses Grundrechts gerichtlich abwehren.

Die Gleichheitssätze des Art. 3 Abs. 1 GG binden gem. Art. 1 Absatz 3 GG zunächst einmal nur die drei Staatsgewalten Exekutive, Legislative und Judikative. Fraglich ist, ob bei der Anwendung des Versicherungsalgorithmus dieses Grundrecht verletzt worden ist, da die drei Staatsgewalten in diesen Vorgang nicht einbezogen gewesen sind. Denn die Formulierung des Art. 3 Abs. 1 GG, wonach eine Gleichbehandlung lediglich vor dem Gesetz erfolgt, ist nach allgemeiner Auffassung zu eng formuliert.[59] Dazu wird vertreten, dass die Gleichheitsrechte nach vorherrschender Auffassung auch zwischen Privatleuten Anwendung finden. Dies ist zwar nicht unmittelbar grundrechtsgebunden, allerdings beeinflusst Art. 3 GG als Verfassungsnorm den Umgang mit untergeordneten Rechtssätzen, etwa den Zivilgesetzen, durch die Rechtsprechung im Rahmen von Gerichtsprozessen.[60] Diese mittelbare Drittwirkung führt dazu, dass die wesentlichen Aussagen des Art. 3 GG Einzug in das Privatrecht halten, insbesondere bei der Auslegung unbestimmter Rechtsbegriffe. Dies liefe auf eine Pflicht des Staates zum Eingriff in die Rechte Privater hinaus. Dies stellte einen Widerspruch dazu dar, dass Art. 3 GG Privatpersonen nicht unmittelbar bindet.[61] Aber

[58] BVerfGE 42, S. 64 (72): Zwangsversteigerung.

[59] *Jarass, H.*: Art. 3, Rn. 1b. In: *Jarass*, *H.*; *Pieroth*, *B.*: Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 28. Auflage, C. H. Beck, München 2014.

[60] *Heun*, *W.*: Art. 3, Rn. 70-71. In: *Dreier*, *H.* (Hrsg.): Grundgesetz Kommentar: GG. 3. Auflage. Band I: Präambel, Artikel 1-19. Tübingen, Mohr Siebeck 2013

[61] *Kischel, U.* Art. 3, Rn. 91. In: Beck'scher Online-Kommentar GG, 34. Auflage 2017

es zeigt doch die Pflicht des Staates auf, dafür zu sorgen, dass seine Bürger gleichberechtigt behandelt werden, da dies ein elementares Grundrecht des Bürgers in einer Demokratie ist. Dennoch lässt sich aus Art. 3 GG kein konkretes Abwehrrecht gegen die Anwendung des Versicherungsalgorithmus herleiten.

2. Benachteiligungsverbot

In Deutschland ist das Allgemeine Gleichbehandlungsgesetz (AGG)[62] das zentrale Gesetz, welches „Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität" verhindern und beseitigen soll (§ 1 AGG). Die konkreten Diskriminierungsverbote des Art. 3 Abs. 3 GG sind nicht völlig deckungsgleich mit denen des Allgemeinen Gleichbehandlungsgesetzes: So verbietet Art. 3 Abs. 3 GG eine Diskriminierung aufgrund der räumlichen Herkunft eines Menschen, nicht aber das AGG.

a) Anwendbarkeit § 19 Abs. 1 Nr. 2 AGG

Gem. § 19 Abs. 1 Nr. 1 AGG ist eine Benachteiligung aus Gründen der Rasse oder wegen der ethnischen Herkunft, wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität bei der Begründung, Durchführung und Beendigung zivilrechtlicher Schuldverhältnisse, die typischerweise ohne Ansehen der Person zu vergleichbaren Bedingungen in einer Vielzahl von Fällen zustande kommen (Massengeschäfte) oder bei denen das Ansehen der Person nach der Art des Schuldverhältnisses eine nachrangige Bedeutung hat und die zu vergleichbaren Bedingungen in einer Vielzahl von Fällen zustande kommen, unzulässig. Damit ist eine Benachteiligung aus den genannten Gründen bei der Begründung, Durchführung und Beendigung zivilrechtlicher Schuldverhältnisse, die eine private Versicherung zum Gegenstand haben, gem. § 19 Abs. 1 Nr. 2 AGG unzulässig. Diese konkrete Anwendung auf private Versicherungen ist in Teilen der Umsetzung der sogenannten „Gender-Richtlinie[63]" sowie der „Antirassismus-Richtlinie"[64] entstanden. Nr. 2 erfasst dabei auch privatrechtliche Versicherungen und somit auch Versicherungsverhältnisse,

[62] BGBl. I, S. 1897 (2006)

[63] Richtlinie 2004/112/EG des Rates vom 13.12.2004 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen beim Zugang zu und bei der Versorgung mit Gütern und Dienstleistungen, einschließlich von Wohnraum, ABl. EG L 373, S. 37.

[64] Richtlinie 2000/43/EG des Rates vom 29.06.2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft, ABl. EG L 180, S. 22.

die nach individuellen Risikoindikatoren ausgestaltet werden,[65] einschließlich betrieblicher Altersversorgung.[66] Sind Nr. 1 und Nr. 2 einschlägig, geht Nr. 2 als speziellere Regelung vor.[67]

Die Regelung in § 19 Abs. 1 Nr. 2 AGG steht natürlich im Spannungsfeld zur Vertragsfreiheit.[68] Sie ist durch die allgemeine Handlungsfreiheit in Art. 2 Abs. 1 GG garantiert. Deren Ausprägung durch den Grundsatz der Privatautonomie ist im deutschen Zivilrecht geschützt,[69] kann aber durch zwingende Vorschriften des geltenden Rechts, gesetzliche Verbote oder wenn sie gegen die guten Sitten verstößt, eingeschränkt werden.[70] Somit verstößt die Anwendung des § 19 Abs. 1 Nr. 2 AGG nicht gegen Art. 2 Abs. 1 GG.

Es stellt sich in diesem Zusammenhang die Frage, warum der Gesetzgeber das Thema „private Versicherung" durch Nr. 2 besonders hervorgehoben hat. Eine Begründung ist darin zu sehen, dass private Versicherungen sich von sämtlichen anderen Vertragstypen, die durch das allgemeine Benachteiligungsverbot des § 19 AGG erfasst werden, in einem für die Anwendung des Gesetzes grundlegenden Punkt unterscheiden: Die Privatversicherung (§ 19 Abs. 1 Nr. 2 AGG) ist im Gegensatz zu den sogenannten „Massengeschäften" (§ 19 Abs. 1 Nr. 1 AGG) ein von vornherein auf die Differenzierung zwischen verschiedenen Risikomerkmalen angelegter Vertrag.[71] Häufig sind diese Risikomerkmale personenbezogen; dementsprechend knüpfen die Merkmale vielfach just an die durch das AGG geschützten Kriterien, wie Geschlecht oder Alter, an. Derartige Differenzierungen erkennt der Gesetzgeber als so bedeutsam für die ordnungsgemäße Funktionsweise des Versicherungsvertrags an, dass er sie teils den Versicherern sogar verbindlich vorschreibt. Besonders deutlich kommt dies in § 12 Abs. 1 Nr. 1 Versicherungsaufsichtsgesetz (VAG) zum Ausdruck. Nach dieser Regelung ist in der substitutiven (an die Stelle einer gesetzlichen Versicherung tretenden)

[65] BTDrs 16/1780, S. 42.
[66] BAG NZA-RR 10, 664 [BAG 18.03.2010 – 6 AZR 434/07].
[67] *Prütting*, *H.*; *Wegen*, *G.*; *Weinreich*, *G.*: BGB Kommentar, AGG § 19 AGG – Zivilrechtliches Benachteiligungsverbot, Rn. 7.
[68] BVerfGE 8, S. 274 – siehe dort Absatzrandnummer 212.
[69] BVerfGE 95, S. 267 – siehe dort Absatzrandnummer 142.
[70] BVerfGE 8, S. 274 – siehe dort Absatzrandnummer 212.
[71] *Armbrüster*, *C.*: Benachteiligungsverbot und Rechtfertigungsgründe beim Abschuss privatrechtlicher Versicherung, Expertise erstellt im Auftrag der Antidiskriminierungsstelle des Bundes, Mai 2010, S. 6.

Krankenversicherung eine alters- und geschlechtsabhängige Tarifgestaltung zwingend erforderlich.[72] Dies wurde auch bei der EU-Gesetzgebung berücksichtigt; so heißt es im Amtsblatt der EU[73], dass die Mitgliedstaaten vor dem 21. Dezember 2007 beschließen können, proportionale Unterschiede bei den Prämien und Leistungen dann zuzulassen, wenn die Berücksichtigung des Geschlechts bei einer auf relevanten und genauen versicherungsmathematischen und statistischen Daten beruhenden Risikobewertung ein bestimmender Faktor ist. Den auf Differenzierung angelegten Charakter der privatrechtlichen Versicherung erkennt auch der Gesetzgeber des AGG an. Die Einbeziehung dieses Vertragstyps in das Benachteiligungsverbot des AGG soll daher ausweislich der Regierungsbegründung lediglich den Schutz vor Willkür bezwecken,[74] also vor Ungleichbehandlungen ohne sachlichen Grund.[75] Eine Differenzierung nach dem ex ante beurteilten individuellen Risiko soll damit nicht unmöglich gemacht werden. Raum für eine derartige Risikodifferenzierung bieten insbesondere die verschiedenen, in § 20 Abs. 2 AGG speziell für Versicherungsverträge vorgesehenen Rechtfertigungstatbestände.[76]

b) Voraussetzung von § 19 Abs. 1 Nr. 2 AGG

Wie bereits oben dargestellt, ist gem. § 19 Abs. 1 Nr. 2 AGG eine Benachteiligung aus Gründen des Geschlechts und des Alters bei der Begründung zivilrechtlicher Schuldverhältnisse, die eine private Versicherung zum Gegenstand haben, unzulässig.

Nach dem in Abschnitt I dargestellten Versicherungsalgorithmus würden Männer, die älter als 9,5 Jahre sind, nicht versichert. Auch Männer (Jungen), die jünger als 9,5 Jahre alt sind und mehr als drei Geschwister haben, würden nach dem Versicherungsalgorithmus nicht versichert. Durch die Und-Verknüpfung von „männlich“ und „mehr drei Geschwister haben“ würde der diskriminierende Faktor des Geschlechts und des Alters in die Entscheidung des Versicherungsalgorithmus einbezogen werden. Die

[72] *Armbrüster*, *C.*: Benachteiligungsverbot und Rechtfertigungsgründe beim Abschuss privatrechtlicher Versicherung, Expertise erstellt im Auftrag der Antidiskriminierungsstelle des Bundes, Mai 2010, S. 7.

[73] ABl. EU, L 373/41 Art. 5 (2).

[74] Regierungsbegründung, BT-Drucks. 16/1780, S. 45; siehe auch OLG Saarbrücken, VersR 2009, S. 1522 (1525).

[75] BVerfGE 91, S. 118 (123).

[76] *Armbrüster*, *C.*: Benachteiligungsverbot und Rechtfertigungsgründe beim Abschuss privatrechtlicher Versicherung, Expertise erstellt im Auftrag der Antidiskriminierungsstelle des Bundes, Mai 2010, S. 8.

Rechtsfolge wäre nach § 19 Abs. 1 Nr. 2 AGG, dass eine solche Entscheidung zunächst einmal nicht zulässig wäre.

c) Ausnahmen nach §§ 3, 20 AGG

Eine Abweichung von dem in § 19 Abs. 1 Nr. 2 AGG normierten Verbot der Benachteiligung ist unter bestimmten, in den §§ 3, 20 AGG festgelegten Voraussetzungen zulässig. Gem. Art. 20 Abs. 1 AGG ist eine Verletzung des Benachteiligungsverbots nicht gegeben, wenn für eine unterschiedliche Behandlung wegen der Religion, einer Behinderung, des Alters, der sexuellen Identität oder des Geschlechts ein sachlicher Grund vorliegt. Dabei führen Ziffer 1-4 einige Beispiele auf. Was die geschlechtsbezogene Ungleichbehandlung angeht, so übernimmt § 20 Abs. 2 S. 1 AGG weitgehend wörtlich die Formulierung aus Art. 5 Abs. 2 der Gender-Richtlinie.[77] Danach ist eine unterschiedliche Behandlung wegen des Geschlechts bei Prämien und Leistungen nur zulässig, wenn die Berücksichtigung „bei einer auf relevanten und genauen versicherungsmathematischen und statistischen Daten beruhenden Risikobewertung ein bestimmender Faktor ist". Daraus lässt sich zunächst entnehmen, dass die europarechtlichen Vorgaben der Gender-Richtlinie – anders als diejenigen der Antirassismus-Richtlinie[78] in Bezug auf das Merkmal Rasse/ethnische Herkunft – eine geschlechtsbezogene Differenzierung ausdrücklich zulassen.[79] Die Formulierung von § 20 Abs. 2 S. 1 AGG wirft die Frage nach dessen Anwendungsbereich auf. Der Wortlaut spricht allein von einer unterschiedlichen Behandlung „bei den Prämien oder Leistungen". Richtigerweise müsste jedoch auch die gänzliche Ablehnung eines Vertragsschlusses von § 20 Abs. 2 S. 1 AGG erfasst sein.[80] Eine gänzliche Verweigerung des Versicherungsschutzes durch Vertragsablehnung oder Kündigung trifft die

[77] Richtlinie 2004/112/EG des Rates vom 13.12.2004 zur Verwirklichung des Grundsatzes der Gleichbehandlung von Männern und Frauen beim Zugang zu und bei der Versorgung mit Gütern und Dienstleistungen, einschließlich von Wohnraum, ABl. EG L 373, S. 37.

[78] Richtlinie 2000/43/EG des Rates vom 29. Juni 2000 zur Anwendung des Gleichbehandlungsgrundsatzes ohne Unterschied der Rasse oder der ethnischen Herkunft, ABl. EG L 180, S. 22.

[79] *Armbrüster*, *C.*: Benachteiligungsverbot und Rechtfertigungsgründe beim Abschuss privatrechtlicher Versicherung, Expertise erstellt im Auftrag der Antidiskriminierungsstelle des Bundes, Mai 2010, S. 11.

[80] *Ambrosius*, *B.* in: *Däubler*, *W.*; *Bertzbach*, *M.*: AGG, 2. Aufl. 2008, § 20 Rn. 40; vgl. bereits *Armbrüster*, *C.* in: *Begemann*, *M.*; *Bruns*, *A.* (Hrsg.): Die Versicherung des Alterns, 2008, S. 43, 49 (im Kontext des Merkmals Behinderung); a. A. MünchKomm-BGB/Thüsing, 5. Aufl. 2007, § 20 AGG Rn. 55: Rechtfertigung nach Abs. 1 möglich; *Schiek*, *D.* in: *Schiek*, *D.*: AGG, 2007, § 20 Rn. 8; *Rödl*, *F.* in: *Rust*, *U.*; *Falke*, *J.*: AGG, 2007, § 20 Rn. 26 f.: gar keine Rechtfertigung möglich.

Versicherungswilligen härter als ein sie benachteiligender Vertragsinhalt.[81] Der Versicherer kann zwar nicht gezwungen werden, für den Fall eines sehr hohen Risikos gleichwohl ein Versicherungsangebot zu unterbreiten, wenn sich das Risiko versicherungstechnisch als nicht versicherbar erweist. Freilich muss er sich bei einer Vertragsablehnung an den strengen Rechtfertigungserfordernissen des § 20 Abs. 2 S. 1 AGG und nicht lediglich an denjenigen des § 20 Abs. 1 S. 1 AGG messen lassen.

Sofern es nicht um Prämien, Leistungen oder eine Vertragsablehnung geht, kann die Rechtfertigung einer Ungleichbehandlung auf § 20 Abs. 1 S. 1 AGG gestützt werden.[82] Dementsprechend genügt es, wenn ein sachlicher Grund für die Ungleichbehandlung besteht, etwa hinsichtlich Obliegenheiten oder Kulanzregelungen. Auf solche Fälle sind die Rechtfertigungskriterien von § 20 Abs. 2 S. 1 AGG ersichtlich nicht zugeschnitten.

3. Ergebnis

Es lässt sich somit festhalten, dass das Ergebnis des Versicherungsalgorithmus für Reisende der Titanic II in jetziger Form, nämlich mit der reinen Entscheidung, ein Versicherungsangebot zu erstellen oder nicht, unzulässig wäre.

Der Benachteiligte des Versicherungsalgorithmus kann gem. § 21 Abs. 1 S. 1 AGG bei einem Verstoß gegen das Benachteiligungsverbot, unbeschadet weiterer Ansprüche, die Beseitigung der Beeinträchtigung verlangen. Sind weitere Beeinträchtigungen gegeben, so kann er gem. § 21 Abs. 1 S. 2 AGG auf Unterlassung klagen. Bei einer Verletzung des Benachteiligungsverbots ist der Benachteiligende verpflichtet, den hierdurch entstandenen Schaden gem. § 21 Abs. 2 AGG zu ersetzen. Dies gilt nicht, wenn der Benachteiligende die Pflichtverletzung nicht zu vertreten hat. Wegen eines Schadens, der kein Vermögensschaden ist, kann der Benachteiligte eine angemessene Entschädigung in Geld verlangen. Ein solcher Anspruch muss gem. § 21 Abs. 5 AGG innerhalb einer Frist von zwei Monaten geltend gemacht werden. Nach Ablauf der

---

[81] *Ambrosius*, *B.* in: *Däubler*, *W.*; *Bertzbach*, *M.*: AGG, 2. Aufl. 2008, § 20 Rn. 40; vgl. bereits *Armbrüster*, *C.* in: *Begemann*, *M.*; *Bruns*, *A.* (Hrsg.): Die Versicherung des Alterns, 2008, S. 43, 49 (im Kontext des Merkmals Behinderung); a. A. MünchKomm-BGB/Thüsing, 5. Aufl. 2007, § 20 AGG Rn. 55: Rechtfertigung nach Abs. 1 möglich; *Schiek*, *D.* in: *Schiek*, *D.*: AGG, 2007, § 20 Rn. 8; *Rödl*, *F.* in: *Rust*, *U. Falke*, *J.*: AGG, 2007, § 20 Rn. 26 f.: gar keine Rechtfertigung möglich.

[82] Insoweit wie hier MünchKomm-BGB/Thüsing (Fn. 22), § 20 AGG Rn. 55; siehe auch Landgericht Offenburg, Urt. v. 13.11.2009 – 3 O 82/09 (unveröff.), Urteilsumdruck, S. 9.

Frist kann der Anspruch nur geltend gemacht werden, wenn der Benachteiligte ohne Verschulden an der Einhaltung der Frist verhindert war.

Die Ansprüche aus § 21 AGG würden entfallen, wenn man den Versicherungsalgorithmus um folgende Regelungen erweitert, würde: Anstelle der Optionen OFFER / NO OFFER würde eine Berechnung für eine höhere Versicherungsprämie erfolgen. Wie unter Abschnitt II Nr. 2 dargestellt, wäre das Ergebnis dieses erweiterten Versicherungsalgorithmus wiederum zulässig:

```
START
Input männlich = 1
Input weiblich = 2
------------------------------------------------------------
REM „Grundfrage männlich oder weiblich“
IF Input = 1 THEN #2
ELSE #1
------------------------------------------------------------
END
------------------------------------------------------------
#1 REM „weiblich“
  PRINT „Überlebenschance bei 74,2 %“
  OFFER (Prämie + Risikoaufschlag)
END
------------------------------------------------------------
#2 REM „männlich“
  IF Input </= 9,5 Jahre THEN
          PRINT „Überlebenschance bei 16,5 %“
          OFFER (Prämie + Risikoaufschlag)
  ELSE
          IF Input </= 3 Geschwister THEN
          PRINT„ Überlebenschance bei 7,1 %“
          OFFER (Prämie + Risikoaufschlag)
```

ELSE

PRINT „ Überlebenschance bei 100 %“

OFFER (Prämie ohne Risikoaufschlag)

END

END

IV. Algorithmischer Handel (Algo Trading)

Zu den Auswirkungen des algorithmisch gesteuerten Wertpapierhandels hat die BaFin eine Studie in Auftrag gegeben.[83] Danach führen Big Data und Artificial Intelligence (in der Sprache der BaFin: BDAI) einen tiefgreifenden Wandel herbei und erfolgreiche Umsetzungen von BDAI können sich selbstverstärkend rasch ausbreiten. Durch die Kombination von Analytik und massenhaft verfügbaren Daten lassen sich neue Erkenntnisse gewinnen. Diese können auch im Finanzsystem für Produkt- und Prozessinnovationen genutzt werden. Solche Innovationen könnten disruptiv auf bestehende Wertschöpfungsprozesse wirken. In der Folge können neue Anbieter in den Markt eintreten (z.B. FinTechs) und etablierte Geschäftsprozesse und Marktstrukturen können sich ändern. Aufsicht und Regulierung müssen sich frühzeitig mit innovativen Entwicklungen auseinandersetzen.

Bei der Betrachtung der Anwendung von BDAI in der Finanzdienstleistungsbranche werden drei zentrale Gruppen von Anbietern unterschieden:

- traditionell tätige Unternehmen (Incumbents), insbesondere beaufsichtigte Unternehmen, wie Banken und Versicherer
- vergleichsweise junge, technologieorientierte Anbieter mit spezifischen Funktionen, von denen einige direkt beaufsichtigt werden (Fintechs, Insurtechs, Regtechs, Legaltechs)
- große, global agierende Technologieunternehmen (Bigtechs), die bislang überwiegend nicht unter die Aufsicht fallen

[83] BDAI-Studie: Big Data trifft auf künstliche Intelligenz. Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen. https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html, abgerufen am 17. Dezember 2018.

Große Datenmengen stehen zusammen mit leistungsfähiger Hardware und marktreifen Auswertungs- und Verarbeitungstechnologien für Daten zur Verfügung. Dabei haben Technologieunternehmen bewiesen, dass sich durch den Einsatz von BDAI ein erheblicher Wettbewerbsvorteil erzielen lässt. Folglich fließt zunehmend mehr Kapital in Big-Data-Lösungen und AI-anwendende Unternehmen, wie Fintechs.[84]

1. Gesetzliche Grundlagen

Zum Teil werden der algorithmisch gesteuerte Handel und der Hochfrequenzhandel zusammen genannt. Geht es beim Hochfrequenzhandel lediglich um die Geschwindigkeit, geht es beim algorithmisch gesteuerten Handel darum, intelligenter als andere Marktteilnehmer zu sein.

a) Algorithmisch gesteuerter Handel

Grundsätzlich muss ein Wertpapierdienstleistungsunternehmen gem. § 80 Abs. 1. S. 1 WpHG (Wertpapierhandelsgesetz) die organisatorischen Pflichten nach § 25a Abs. 1 und § 25e des Kreditwesengesetzes sowie die zusätzlichen Verpflichtungen aus § 80 Abs. 1. S. 2 WpHG einhalten. Diese umfassen im Wesentlichen Sicherheitsmaßnahmen, z. B. organisatorische oder IT-Sicherheitspflichten.[85] Zusätzliche Pflichten ergeben sich beim algorithmisch gesteuerten Wertpapierhandel. Denn nach § 80 Abs. 2 S. 1 WpHG muss ein Wertpapierdienstleistungsunternehmen zusätzlich die in § 80 Abs. 2 S. 1 WpHG genannten Bestimmungen einhalten, wenn es in einer Weise Handel mit Finanzinstrumenten betreibt, dass ein Computeralgorithmus die einzelnen Auftragsparameter automatisch bestimmt. Dies gilt allerdings nicht, wenn es sich um ein System handelt, das nur zur Weiterleitung von Aufträgen zu einem oder mehreren Handelsplätzen, zur Bearbeitung von Aufträgen ohne die Bestimmung von Auftragsparametern, zur Bestätigung von Aufträgen oder zur Nachhandelsbearbeitung ausgeführter Aufträge verwendet wird (algorithmischer Handel). Dabei ist nach § 80 Abs. 2 S. 2 WpHG zu beachten, dass Auftragsparameter im Sinne des S. 1 insbesondere Entscheidungen sind, ob der Auftrag eingeleitet werden soll, außerdem über Zeitpunkt, Preis oder Quantität des Auftrags oder wie der Auftrag nach seiner

[84] BDAI-Studie: Big Data trifft auf künstliche Intelligenz. Herausforderungen und Implikationen für Aufsicht und Regulierung von Finanzdienstleistungen. https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html, abgerufen am 17. Dezember 2018.

[85] *Voigt*, *P.*: Sonstige branchenspezifische Vorschriften zur IT-Sicherheit. In: *Voigt*, *P.*: IT-Sicherheitsrecht, 1. Auflage 2018.

Einreichung mit eingeschränkter oder überhaupt keiner menschlichen Beteiligung bearbeitet wird. Dabei gelten für Wertpapierdienstleistungsunternehmen seit 3. Januar 2018 neue Anzeigepflichten aufgrund der Umsetzung der Finanzmarktrichtlinie[86] durch das Zweite Finanzmarktnovellierungsgesetz. Danach sind Wertpapierdienstleistungsunternehmen von diesen Anzeigepflichten betroffen, wenn sie algorithmischen Handel im Sinne des § 80 Abs. 2 S. 1 WpHG (Fassung, 3. Januar 2018) betreiben, oder wenn sie gem. § 2 Abs. 30 WpHG (Fassung 3. Januar 2018) einen direkten elektronischen Zugang (DEA – Direct Electronic Access) zu einem Handelsplatz anbieten. Einerseits sind die Anzeigen sind gegenüber der Behörde abzugeben, die für die Beaufsichtigung der betroffenen Wertpapierdienstleistungsunternehmen zuständig ist. Die Anzeigen sind andererseits auch an die Behörden zu übermitteln, die die Aufsicht über die betroffenen Handelsplätze haben.[87]

Daher sind Wertpapierdienstleistungsunternehmen in folgenden Fällen gegenüber der BaFin anzeigepflichtig:

- Die Wertpapierdienstleistungsunternehmen werden von der BaFin beaufsichtigt und bieten einen DEA zu einem Handelsplatz an oder betreiben algorithmischen Handel. In diesem Fall ergibt sich die Anzeigepflicht aus den §§ 77 Abs. 2 Satz 1 und 80 Abs. 2 S. 5 WpHG (Fassung 3. Januar 2018).
- Die Wertpapierdienstleistungsunternehmen sind Mitglieder oder Teilnehmer eines multilateralen Handelssystems (MTF) oder eines organisierten Handelssystems (OTF), das von der BaFin beaufsichtigt wird, und bieten zu diesem MTF oder OTF einen DEA an oder betreiben dort algorithmischen Handel. In diesen Fällen können von der Anzeigepflicht gegenüber der BaFin auch solche Unternehmen betroffen sein, die nicht unter der Aufsicht der BaFin stehen. Für diese Unternehmen kann sich die Anzeigepflicht aus den Vorschriften anderer EU-Mitgliedsstaaten ergeben, die Art. 17 Abs. 2 Unterabs. 1 und Art. 17 Abs. 5 Unterabs. 3 MiFID II in nationales Recht umsetzen.

Nach § 33 Abs. 1a WpHG müssen Wertpapierdienstleistungsunternehmen, die algorithmischen Handel betreiben, über **angemessene System- und Risikokontrollen** für ihre Handelssysteme verfügen. Zudem müssen sie wirksame Notfallvorkehrungen einsatzbereit vorhalten, damit sie unvorhergesehenen Störungen in ihren Handelssystemen bewältigen

[86] Markets in Financial Instruments Directive II – MiFID II
[87] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.

können. Des Weiteren müssen sie sicherstellen, dass jede Änderung eines zum Handel verwendeten Computeralgorithmus den Vorschriften entsprechend dokumentiert wird. Die Pflicht, angemessene System- und Risikokontrollen verfügbar zu haben, gilt auch für Kapitalanlagegesellschaften und selbstverwaltende Investmentaktiengesellschaften.[88]
Die Eurex Exchange führte zum 1. April 2014 die Pflicht zur **Kennzeichnung** der durch Algo-Trading[89] erzeugten Aufträge sowie der jeweils angewandten Handelsalgorithmen („Algo-Flagging") ein. Im Einzelnen sind dies:

- durch Algo-Trading im Sinne des § 33 1a WpHG erzeugte Aufträge und Quotierungen
- verwendete Handelsalgorithmen
- der gesamte automatisierte Entscheidungsweg[90]

Hierbei muss die Kennzeichnung von Algorithmen eindeutig, konsistent und nachvollziehbar erfolgen und sich auf alle Orders und Quotes erstrecken, die durch Systeme und anhand von Handelsalgorithmen erzeugt, geändert oder gelöscht werden. „Die Kennzeichnungslogik sowie die technischen Eingabemöglichkeiten werden von den Börsenplattformen vorgegeben und haben in deren EDV-Systemen zu erfolgen. Handelsteilnehmer werden ihrerseits eine Analyse der verschiedenen Handelsalgorithmen, eine konsistente Ein- und Zuordnung dieser sowie eventuelle Kosten-Nutzen-Kalkulationen durchführen."[91]

b) Hochfrequenzhandel

Das Wertpapierhandelsgesetz (WpHG) definiert in § 2 Abs. 8 Nr. 2 lit. d den Hochfrequenzhandel als Kaufen oder Verkaufen von Finanzinstrumenten auf eigene Rechnung als unmittelbarer oder mittelbarer Teilnehmer eines inländischen organisierten Marktes oder eines multilateralen oder organisierten Handelssystems mittels einer hochfrequenten algorithmischen Handelstechnik im Sinne von Abs. 44, auch ohne Dienstleistung für andere (Hochfrequenzhandel). Ferner charakterisiert sich der Hochfrequenzhandel nach dem

[88] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.
[89] hochfrequente algorithmischer Handelstechnik.
[90] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.
[91] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.

WpHG dadurch, dass die einzelnen Parameter des jeweiligen Auftrags vom Computeralgorithmus selbstständig bestimmt werden. Die Charakteristika der Parameter sind beispielsweise Zeitpunkt, Preis oder Menge des Auftrags.[92]

Um den Risiken entgegenzuwirken, die mit dem Hochfrequenzhandel verbunden sind, hat der Gesetzgeber gehandelt und das Gesetz zur Vermeidung von Gefahren und Missbräuchen im Hochfrequenzhandel (Hochfrequenzhandelsgesetz – HFHG) erlassen;[93] es ist am 15. Mai 2013 es in Deutschland in Kraft getreten. Das Gesetz soll den Risiken des Hochfrequenzhandels entgegenwirken und vorhandene Aufsichtslücken schließen. „*Aufgrund der inhärenten Erweiterung des Kreditwesengesetzes (KWG) unterliegen Firmen ab sofort einer KWG-Erlaubnispflicht, sobald sie auf eigene Rechnung mittels hochfrequenter algorithmischer Handelstechnik (Algo Trading) handeln.*“[94] Diese Erlaubnispflicht gilt sowohl für Handelsteilnehmer als auch für Handelsplätze. Das Gesetz orientiert sich an den europäischen Regelungen zum algorithmischen Handel und Hochfrequenzhandel, die aufgrund der Überarbeitung der Finanzmarktrichtlinie[95] vorgesehen sind.[96] Börsenplätze werden durch das HFHG verpflichtet, ein angemessenes Verhältnis zwischen Auftragseingaben und den tatsächlich ausgeführten Geschäften der Handelsteilnehmer sicherzustellen. In diesem Zusammenhang änderte die Eurex Exchange die Börsenordnung und führte zum 1. Dezember 2013 das Order-Transaktions-Verhältnis (order to trade ratio – OTR) einschließlich eines zu überwachenden Transaktionslimits ein.[97] Nach dem HFHG sind Handelsteilnehmer dazu verpflichtet, durch Algo-Trading erzeugte Aufträge und Quotes sowie den jeweils angewandten Handelsalgorithmus zu kennzeichnen. Die Eurex Exchange führte deshalb zum 1. April 2014 das „Algo-Flagging“, die Kennzeichnungspflicht für Algorithmen, ein.[98]
Im Wesentlichen enthält das HFHG die folgenden Regelungen:

---

[92] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.

[93] *Kindermann*, *Coridass*, ZBB 2014, S. 178; *Schultheiß*, WM 2013, S. 596; *Jaskulla*, BKR 2013, S. 221; *Kasiske*, WM 2014, S. 1933; *Mattig*, WM 2014, S. 1940.

[94] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.

[95] Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates vom 21. April 2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG des Rates und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 93/22/EWG des Rates.

[96] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.

[97] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.

[98] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.

- System- und Risikokontrollen
- Erlaubnispflicht für Hochfrequenzhändler
- angemessenes Order-Transaktions-Verhältnis
- Kennzeichnungspflicht
- weitere Regelungen

Nach dem KWG ist das Betreiben von Hochfrequenzhandel **erlaubnispflichtig**. Diese Erlaubnispflicht betrifft alle unmittelbaren und mittelbaren Handelsteilnehmer an einem organisierten Markt oder multilateralen Handelssystem (MTF) in Deutschland, welche mittels hochfrequenter algorithmischer Handelstechniken Handel treiben und dabei keine Dienstleistung für Dritte erbringen. Eine solche Handelstechnik ist gekennzeichnet durch die Nutzung von Infrastrukturen, die darauf abzielen, Latenzzeiten zu minimieren (z. B. Collocation, Proximity Hosting), außerdem durch die Entscheidung des Systems über die Einleitung, das Erzeugen, das Weiterleiten oder die Ausführung eines Auftrags ohne menschliche Intervention für einzelne Geschäfte oder Aufträge und durch ein hohes Mitteilungsaufkommen während des Tages. Im Hinblick auf Risikomanagement und Eigenkapital sowie Meldepflichten gegenüber der Aufsicht zieht die Erlaubnispflicht bestimmte Pflichten nach sich.[99]

Zur Einhaltung eines angemessenen Verhältnisses zwischen Auftragseingaben, -änderungen und -löschungen und den tatsächlich ausgeführten Geschäften der Handelsteilnehmer (**angemessenes Order-Transaktions-Verhältnis**) führte die Eurex Exchange zum 1. Dezember 2013 ein verpflichtendes Order-Transaktions-Verhältnis (OTR) ein. Daraus ergaben sich Höchstgrenzen für Aufträge und Quotierungen der Handelsteilnehmer, die sich aus dem individuellen monatlichen Handelsvolumen ausgeführter Geschäfte in dem

[99] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.

jeweiligen Finanzinstrument ableiten. Das angemessene Order-Transaktions-Verhältnis ist folgendermaßen definiert:[100]

$$\text{OTR} = \frac{\text{geordertes Volumen}}{\text{Volumenlimit}}$$

Dabei ist das georderte Volumen die Anzahl der Kontrakte im Orderbuch, die mittels Orders oder Quotes generiert und von der Matching Engine akzeptiert werden. Selbst die Kontrakte, die ein Handelsteilnehmer aus der Matching Engine löscht und somit nicht ausführt, werden hierzu gezählt. Die Änderung eines Auftrags wird dabei als Löschung des bisherigen Auftrags mit anschließender Eingabe eines neuen Auftrags gewertet. Einerseits beinhaltet das Volumenlimit eine Volumenkomponente und andererseits einen Grundfreibetrag pro Finanzinstrument. Die Volumenkomponente ist die Anzahl der ausgeführten Geschäfte pro Handelsteilnehmer in dem jeweiligen Finanzinstrument, multipliziert mit einem festgesetzten Volumenfaktor pro Finanzinstrument. Für jeden Handelsteilnehmer wird ein Grundfreibetrag festgesetzt, der von seiner Handelsfunktion abhängig ist – so unterscheidet sich der Grundfreibetrag für Market Maker vom Grundfreibetrag anderer Handelsteilnehmer. Das OTR-Limit von 1 zielt also auf eine dynamische Begrenzung des Ordervolumens der Handelsteilnehmer ab, das folglich stets mit den tatsächlich erfolgten Transaktionen und dem sich dadurch verändernden Volumenlimit abgeglichen werden muss. Da ein OTR größer als 1 am Ende eines Kalendermonats einen Verstoß gegen das HFG und angepasste Börsenordnungen darstellt und mit Sanktionen belegt ist, kommen die Handelsteilnehmer um eine entsprechende Anpassung interner Kontroll- und Überwachungssysteme nicht herum.[101]

Außer den genannten Regelungen nennt das Gesetz **weitere Pflichten für Handelsplätze**. Diese betreffen die Erhebung von separaten Entgelten oder Gebühren bei übermäßiger Nutzung der Börsensysteme, die Festlegung einer angemessenen Größe der kleinstmöglichen Preisänderung und zu Volatilitätsunterbrechern. Zudem stellt das Gesetz klar, dass auch Handelspraktiken, die Computeralgorithmen beinhalten, unter bestimmten Voraussetzungen Marktmanipulationen darstellen können. Drüber hinaus enthält das Gesetz

[100] Eurex-Rundschreiben 213/13 vom 27. September 2013.

[101] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.

Auskunftsbefugnisse für die Aufsichtsbehörden im Hinblick auf den algorithmisch betriebenen Handel.[102]

Die Definition des Hochfrequenzhandels unmittelbarer und mittelbarer Handelsteilnehmer hat die BaFin[103] konkretisiert: Sie spezifiziert – neben dem Handel auf eigene Rechnung – die Gültigkeit folgender Kriterien:

- selbstständiges Treffen von Handelsentscheidungen durch das System
- digitaler Handel mit einer Bandbreite von 10 Gigabit pro Sekunde und
- mit mindestens 75.000 Mitteilungen pro Handelstag im Jahresdurchschnitt

Weil das KWG um die genannten Kriterien erweitert wurde, fallen alle Hochfrequenzhändler unter die Aufsicht der BaFin; sie benötigen deshalb eine Lizenz nach § 32 KWG. „*Die KWG-Erlaubnispflicht für Hochfrequenzhändler löst somit u. a. Pflichten hinsichtlich des Risikomanagements, des Eigenkapitals und der Meldungen an die Aufsicht aus. Insbesondere die Eigenkapital- und Liquiditätsvorschriften des KWG führen nach derzeitigem Stand dazu, dass Eigenhändler ihr hochfrequentes Algo-Trading künftig mit Eigenkapital unterlegen müssen.*“[104]

Seit 3. Januar 2018 gelten durch das Zweite Finanzmarktnovellierungsgesetz auch neue Anzeigepflichten für Wertpapierdienstleistungsunternehmen zum Hochfrequenzhandel. Wie für den algorithmisch gesteuerten Wertpapierhandel ist auch hier die Grundlage die Umsetzung der Finanzmarktrichtlinie (Markets in Financial Instruments Directive II – MiFID II). Wertpapierdienstleistungsunternehmen sind von diesen Anzeigepflichten betroffen, wenn sie algorithmischen Handel im Sinne des § 80 Abs. 2 S. 1 WpHG (Fassung 3. Januar 2018) betreiben, oder wenn sie gemäß § 2 Abs. 30 WpHG (Fassung 3. Januar 2018) einen direkten elektronischen Zugang (Direct Electronic Access – DEA) zu einem Handelsplatz anbieten,[105] wie es beim Hochfrequenzhandel der Fall ist.

Fraglich ist, ob durch die Umsetzung der Richtlinie 2014/65/EU (MiFID II) das HFHG noch anwendbar ist, da durch lex posterior (lat.: „*Das jüngere Gesetz hebt das ältere Gesetz auf*“)

[102] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.
[103] Schreiben der BaFin vom 21. Mai 2013.
[104] Hochfrequenzhandel – Regulatorischer Rahmen und Handlungsbedarf seitens Börsen und Handelsteilnehmer. Stellungnahme von BearingPoint, https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.
[105] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.

man durchaus auch zu der Ansicht kommen könnte, dass MiFID II und dessen Umsetzung in nationale Gesetze das HFHG aufgehoben haben könnte. Hierzu ist aber im Gesetz und in der Literatur nichts zu finden. Das BaFin sieht durchaus die Anforderungen von MiFID II an den algorithmisch betriebenen Handel, spricht aber an der gleichen Stelle von der Anwendbarkeit des HFHG.[106] Somit ist davon auszugehen, dass die Regelungen des HFHG weiterhin angewendet werden müssen.

c) Börsenaufsicht

Gem. § 26d Abs. 1 S. 1 BörsG muss die Börse sicherstellen, dass algorithmische Handelssysteme nicht zu Beeinträchtigungen des ordnungsgemäßen Börsenhandels führen oder zu solchen Beeinträchtigungen beitragen. Die Vorschrift in § 26d BörsG wurde durch das Zweite Gesetz zur Novellierung von Finanzmarktvorschriften auf Grund europäischer Rechtsakte (Zweites Finanzmarktnovellierungsgesetz – 2. FiMaNoG)[107] vom 23. Juni 2017 eingefügt und trat am 3. Januar 2018 in Kraft. Damit werden auch die Anforderungen von Art. 48 Abs. 4 MiFID II umgesetzt. Um den von algorithmischen Handelssystemen ausgehenden Gefahren für den ordnungsgemäßen Börsenhandel vorzubeugen, hat die Börse gem. § 26d Abs. 1 S. 2 BörsG geeignete Vorkehrungen zu treffen, einschließlich Vorkehrungen zur Begrenzung des Verhältnisses von nicht ausgeführten Handelsaufträgen zu ausgeführten Handelsaufträgen für den Fall, dass die Systemkapazität der Börse übermäßig in Anspruch genommen wird und die Gefahr besteht, dass die Kapazitätsgrenze erreicht wird. Die Regelung stellt sicher, dass die Börse Sicherungen im Hinblick auf den algorithmischen Handel, insbesondere den Hochfrequenzhandel, vorsieht. Dies beruht auf der Sorge, dass diese Form des Handels u. a. aufgrund des Umfangs und der Geschwindigkeit zu Belastungen der elektronischen Systeme der Börsen und damit zu Beeinträchtigungen des Börsenhandels führen könnte. Insbesondere die Anforderungen an Preisanfrage- und Hybridsysteme sollen sich an Art, Umfang und Komplexität des algorithmischen Handels ausrichten.[108] Wegen der geeigneten Vorkehrungen nach Abs. 1 und der Anforderungen an die Ausgestaltung der Tests nach Abs. 2 wird auf die Delegierte Verordnung (EU)

[106] Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.
[107] BGBl. I, S. 1693.
[108] Delegierte Verordnung (EU) 2017/584 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Handelsplätze (ABl. L 87 vom 31. März 2017, S. 350).

2017/584[109], in der jeweils geltenden Fassung, verwiesen. Ergänzt werden die Regelungen durch die Delegierte Verordnung (EU) 2017/584 (III). Diese enthält u. a. Regelungen hinsichtlich des Tests der Systeme, die Mitglieder einsetzen (Art. 8), und zu deren Konformität mit den Systemen des jeweiligen Handelsplatzes (Art. 9) sowie hinsichtlich der von Mitgliedern eingesetzten Algorithmen (Art. 10), außerdem zu vorbeugenden Maßnahmen gegen marktstörende Handelsbedingungen (Art. 18), Mechanismen zur Steuerung der Volatilität (Art. 19) und zur Vorhandels- und Nachhandelskontrolle (Art. 20). Algorithmische Handelssysteme dürfen den Börsenhandel nicht beeinträchtigen (I). Da ein „Beitragen" ausreicht, ist es nicht erforderlich, dass die Handelssysteme so ausgelegt sind, dass sie allein zu Handelsbeeinträchtigungen führen. Es genügt vielmehr, dass sie (nur) mit anderen Systemen gemeinsam den Handel beeinträchtigen, damit die Börse Maßnahmen dagegen ergreifen muss. Zu den dafür „geeigneten Vorkehrungen" gehören die in Art. 18 I Delegierte VO (EU) 2017/584 aufgelisteten vorbeugenden Maßnahmen gegen marktstörende Handelsbedingungen, z. B. Obergrenzen für die Anzahl der pro Sekunde pro Mitglied aufgebbaren Orders, Mechanismen zur Steuerung der Volatilität (dazu auch Art. 19 der VO) und die in Art. 20 Delegierte VO (EU) 2017/584 weiter ausgeführten Vorhandelskontrollen, z. B. Preisbänder, Auftragshöchstwerte und -höchstvolumina.[110] Da in Art. 18 I Delegierte VO (EU) 2017/584 davon die Rede ist, dass diese Maßnahmen „mindestens" getroffen werden müssen, haben alle Börsen diese Vorkehrungen einzuführen.[111] Hinzu kommt die Festlegung des Verhältnisses von nicht ausgeführten Handelsaufträgen zu ausgeführten Handelsaufträgen, die sich an die Regelung in § 26a BörsG anlehnt. Da diese Maßnahmen „einschließlich" einzuführen ist, hat der deutsche Gesetzgeber die Einführung dieser vorbeugenden Maßnahme verbindlich vorgesehen. Allerdings bleibt die nähere Ausformung den Börsen überlassen, die je nach ihrer Systemkapazität für sich eigene Schwellenwerte festlegen können.[112] Die Börsen (Handelsplätze) sind nach Art. 2 Delegierte VO (EU) 2017/566 verpflichtet, das Verhältnis von nicht ausgeführten Aufträgen und Geschäften

[109] Delegierte Verordnung (EU) 2017/584 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der organisatorischen Anforderungen an Handelsplätze (ABl. L 87 vom 31. März 2017, S. 350).

[110] *Groß* Kapitalmarktrecht: Kommentar zum Börsengesetz, 6. Auflage 2016, § 26d Rn. 1.-4.

[111] *Kasiske* WM 14, 1933, *Kindermann/Coridaß* ZBB 14, 178.

[112] *Groß* Kapitalmarktrecht: Kommentar zum Börsengesetz, 6. Auflage 2016, § 26d Rn. 1. ff.

zu berechnen und dafür die Methodik gemäß Art. 3 Delegierte VO (EU) 2017/566 zu verwenden.[113]

Nach § 26d Abs. 2 S. 1 BörsG sind die Handelsteilnehmer verpflichtet, ihre Algorithmen in einer von der Börse zur Verfügung gestellten Umgebung zu testen. Dabei überwacht gem. § 26d Abs. 2 S. 1 BörsG die Geschäftsführung die Einhaltung der Pflicht nach S. 1 und teilt der Börsenaufsichtsbehörde Anhaltspunkte für Verstöße mit. Mit diesen Tests erhält die Börse die Möglichkeit, die Auswirkungen der Algorithmen zu untersuchen und ihre Vorkehrungen entsprechend anzupassen, notfalls auch ein gefährliches algorithmisches Handelsprogramm nicht zuzulassen. Da die Börse die Umgebung zur Verfügung stellen muss, kann sie von den Handelsteilnehmern nicht verlangen, dass diese entweder selbst eine Testumgebung schaffen oder ihre Handelsprogramme andernorts testen lassen. Die Börsengeschäftsführung überwacht die Tests und informiert gegebenenfalls die Börsenaufsichtsbehörde, wenn es zu Verstößen kommt.[114]

2. Resümee

Mit den Regelungen im WpHG, im HFHG, im BörsG und den Ausführungen der BaFin haben der Gesetzgeber und die Aufsicht auf den algorithmisch gesteuerten Wertpapierhandel reagiert und einen entsprechenden rechtlichen Rahmen geschaffen. Spannend ist dabei die Regelung in § 26d Abs. 2 S. 1 BörsG, wonach die Handelsteilnehmer verpflichtet sind, ihre Algorithmen in einer von der Börse zur Verfügung gestellten Umgebung zu testen. Fraglich ist, wie dieser Test in der Praxis ausgestaltet ist und wie der Test die Risiken des algorithmisch gesteuerten Wertpapierhandels beherrschbar machen soll.

[113] *Aldridge*, High-Frequency Trading, 2nd ed 2013, *Gresser*, Praxishandbuch Hochfrequenzhandel, 2016, *Jaskulla* BKR 13, 221, *Kobbach* BKR 13, 233, *Schultheiß* WM 13, 596, *Kasiske* WM 14, 1933, *Kindermann/Coridaß* ZBB 14, 178.

[114] *Groß* Kapitalmarktrecht: Kommentar zum Börsengesetz, 6. Auflage 2016, § 26d Rn. 1-4.

B. Maschine Learning[115]

Laut Wikipedia[116] entwickelt, untersucht und verwendet Maschinelles Lernen (ML) statistische Algorithmen, auch Lernalgorithmen genannt. Dabei werden Künstliche neuronale Netze (KNN) beim maschinellen Lernen verwendet, um eine komplexe Lernstruktur zu erschaffen, deren Ziel es ist, intelligente Verhaltensweise zu ermöglichen. Ein ganz praktisches Beispiel für solche intelligenten Maschinen sind autonome Saugroboter, die mittels unterschiedlicher Sensoren lernen, einen Raum zu erkunden und aus diesen Erkenntnissen die Motoren des Saugroboters steuern. Eine ähnliche Arbeitsweise wird auch beim algorithmischen Wertpapierhandel angewendet. Informationen aus unterschiedlichen Quellen werden erfasst, bewertet und gewichtet und der Output kann z. B. das Kaufen oder Verkaufen eines Wertpapiers sein. Die Erstellung solcher Lern- und Steuerungsmechanismen kann als sehr aufwendig betrachtet werden und ist daher mit hohen Investitionen verbunden. Um diese Investitionen abzusichern bzw. die Schaffung des KNN zu schützen, bedarf es rechtlicher Antworten. Wie so häufig bei neuen Technologien, ist die juristische Antwort nicht so eindeutig zu geben, wie sich das die Entwickler von Systemen mit künstlicher Intelligenz (KI) immer wünschen. Der folgende Artikel soll helfen, zunächst einmal die Arbeitsweise von KNN zu verstehen, um somit Optionen für einen rechtlichen Schutz zu evaluieren.

I. Grundelemente des maschinellen Lernens

Das maschinelle Lernen, zu dem man KNN verwendet, ist ein wichtiger Anwendungsfall der KI und kommt bereits heute viel häufiger vor als man vermutet. Ein prominentestes Beispiel ist das Mobiltelefon, welches lernt, wie der Fingerabdruck oder die Iris der Besitzer aussieht, um das Mobiltelefon zu entsperren. Erfolgt das maschinelle Lernen durch ein mehrschichtiges Lernen, bzw. tiefes Lernen oder tiefgehendes Lernen, so wird dieses als „Deep Learning“ bezeichnet.[117]

[115] Siehe auch „Künstliche neuronale Netze: Wie KI-Lernstrukturen rechtlich zu betrachten sind“ MMR 2021, 111

[116] https://de.wikipedia.org/wiki/Maschinelles_Lernen

[117] *Bruderer, H.*: Erfindung des Computers, Elektronenrechner, Entwicklungen in Deutschland, England und der Schweiz. In: Meilensteine der Rechentechnik. 2., völlig neu bearbeitete und stark erweiterte Auflage. Band 2. De Gruyter, 2018, ISBN 978-3-11-060261-6; Wörterverzeichnis zur Technikgeschichte, S. 408 (eingeschränkte Vorschau in der Google-Buchsuche, abgerufen am 23.11.2019).

Die Abbildung eines solches „Deep Learnings“ erfolgt häufig in KNN. Solche Deep-Learning-Modelle sind vor allem im Bereich der Bild-, Sequenz- und Spracherkennung zu finden. Die KI-Anwendungen können Fotos „aufhübschen“[118] und Gesichter je nach gewählter Einstellung manipulieren, beispielsweise ein Lächeln nachbilden.[119] Außerdem können die Deep-Learning-Systeme die „Verpixelung“ bestimmter Bilder, die in der Regel dem Schutz der Privatsphäre (z. B. bei Partnerbörsen) dienen, durch Algorithmen rückgängig machen.[120] Hintergrundinformationen, wie Metadaten können zudem aus den Fotos automatisch ausgelesen werden,[121] z. B. um ähnliche Produkte aus Shops zu verlinken.[122] Weiterhin findet Deep Learning erfolgreich Anwendung in der Fahrzeugkonstruktion (selbstfahrende Autos), in der Finanzwelt (Aktienkursvorhersage, Risikoprognose, automatische Handelssysteme), in der Medizin (maschinelle Bilderkennung von Karzinomen) und Biologie (Genomik), im E-Commerce (Recommendation-Systeme) und im Webumfeld (Anomalieerkennung).[123]

II. Arbeitsweisen von maschinellem Lernen

Die generelle Arbeitsweise von maschinellem Lernen orientiert sich eher an der Heuristik. Heuristik bezeichnet (altgr. εὑρίσκω heurísko: „ich finde“; von εὑρίσκειν heurískein: „auffinden“, „entdecken“) die Kunst, mit begrenztem Wissen (unvollständigen Informationen) und wenig Zeit dennoch zu wahrscheinlichen Aussagen oder praktikablen Lösungen zu kommen.[124] Dabei ist erstaunlich, wie fortschrittlich die dabei erzeugten Ergebnisse sind. Das folgende Beispiel von *Tariq Rashid*[125] zeigt auf, wie Strukturen maschinellen Lernens in Iterationsschleifen arbeiten. So soll ein KI-System erkennen, ob Raupen oder Marienkäfer vorliegen. Eine solche KI wird auch als Prädiktor bezeichnet, weil sie eine Eingabe übernimmt und eine Vorhersage

[118] https://www.heise.de/newsticker/meldung/KI-retuschiert-Smartphonefotos-in-Echtzeit-3792720.html, abgerufen am 11.05.2020.
[119] https://www.heise.de/ct/ausgabe/2017-11-Kuenstliche-Intelligenz-macht-Bildbearbeitung-intuitiv-3705914.html, abgerufen am 11.05.2020.
[120] Vgl. https://www.golem.de/news/google-brain-algorithmus-macht-ge-sichter-auf-schlechten-bildern-erkennbar-1702-126066.html, abgerufen am 11.05.2020; https://netzpolitik.org/2016/verpixelung-macht-unsichtbar-oder-doch-nicht, abgerufen am 11.05.2020.
[121] http://t3n.de/news/facebook-ki-bilderkennung-chrome-781194/, abgerufen am 11.05.2020.
[122] Vgl. https://www.heise.de/newsticker/meldung/eBay-Produkte-mithilfe-von-Fotos-suchen-und-kaufen-3784371.html, abgerufen am 11.05.2020.
[123] *Heinz*, *S.*: Deep Learning – Teil 1: Einführung, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, abgerufen am 11.05.2020.
[124] *Gigerenzer*, *G.*; *Todd*, *P. M.*; ABC Research Group: Simple heuristics that make us smart. Oxford University Press, New York 1999.
[125] *Rashid*, *T.*: Neuronale Netz selbst programmiert, 1. Auflage 2017, S. 8.

darüber trifft, wie die Ausgabe sein sollte. Um diese Vorhersage im Sinne der Heuristik zu verfeinern, werden die internen Parameter angepasst.

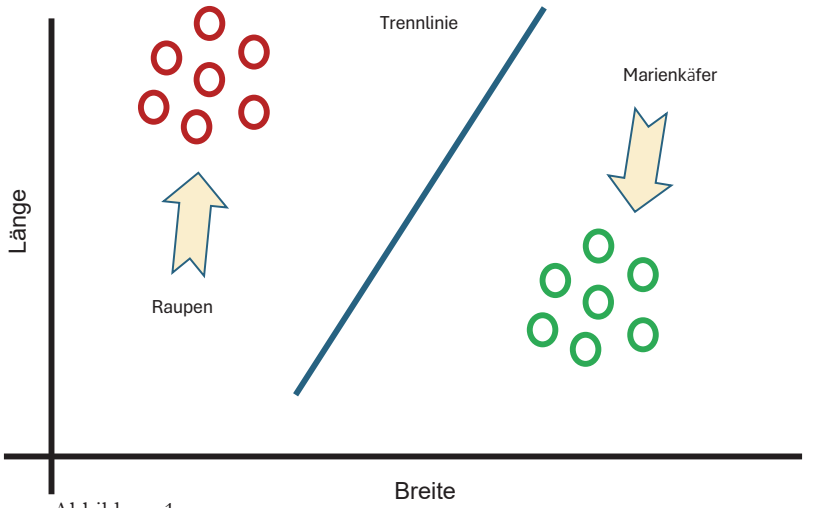


Abbildung 1

In der Abbildung 1 lassen sich zwei Gruppen von Tieren ausmachen, Raupen und Marienkäfer. Raupen sind allgemein dünn und lang, dagegen sind Marienkäfer breit und kurz (diese Aussage wurde aus Darstellungsgründen simplifiziert). Der Prädiktor sucht nach Unterscheidungsmerkmalen zwischen Raupen und Marienkäfern und wird durch eine heuristische Herangehensweise versuchen, eine Trennlinie zwischen diesen Gruppen von Tieren zu definieren. Eine Trennlinie ist kein absoluter Wert, sondern wird sich im Wege der Heuristik auch wieder verschieben können, wenn der Prädiktor durch neue Informationen lernt, wann die identifizierten Tiere eher Raupen oder Marienkäfern entsprechen. Dazu muss der Prädiktor seine Ergebnisse immer wieder mit der sog. Grundwahrheit[126] vergleichen. Die Grundwahrheit ist die absolute Wahrheit, also im vorliegenden Fall, ob nun wirklich Raupen und/oder Marienkäfer vorliegen. Dabei wird die Wahrheit des Prädiktors nicht die absolute Wahrheit beinhalten, aber sein Ergebnis, was sehr nah an der Grundwahrheit ist.[127]

[126] *Zweig, K.*: Ein Algorithmus kennt kein Taktgefühl, 1. Auflage 2019, S. 140 ff.
[127] *Rashid, T.*: Neuronale Netz selbst programmiert, 1. Auflage 2017, S. 10.

Mit jeder Iterationsschleife sammelt der Prädiktor Informationen über Raupen und Marienkäfer und vergleicht diese mit der Grundwahrheit. Gerade bei den ersten Iterationsschleifen muss der Mensch das Lernen des Prädiktors überprüfen, sprich, die Ergebnisse des Prädiktors mit der Grundwahrheit vergleichen. Je mehr Informationen der Prädiktor hat, desto besser wird seine Unterscheidung zwischen Raupen und Marienkäfern werden.

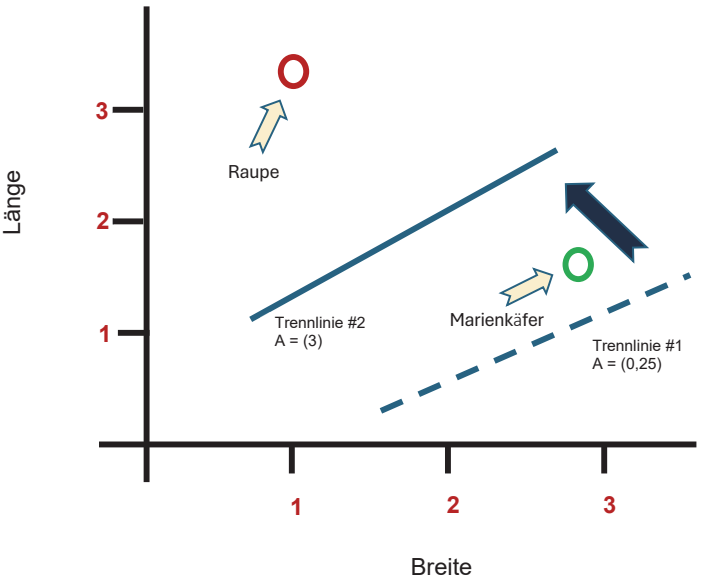


Abbildung 2

Die Abbildung 2 zeigt, wie die Trennlinie sich verschiebt und somit das Ergebnis liefert, ob nun eine Raupe oder ein Marienkäfer vorliegt. Dabei ist A der Wert für die Verschiebung der Trennlinie nach links oben. Ist der Wert A = 0,25, dann liegt keine Trennung von Marienkäfer und Raupen (Trennlinie #1) vor. Liegt der Wert A = 3 (Trennlinie #2), dann liegt eine Trennung zwischen Marienkäfern und Raupen vor. Der (vereinfachte) Lernalgorithmus lautet:

Fehlerwert = Sollwert – Istwert

Überprüfung mit der Grundwahrheit

Fehlerwert = 0 => kein Fehler

III. Arbeitsweisen von Deep Learning und künstlichen neuronalen Netzwerken

Deep Learning nutzt gegenüber dem einfachen maschinellen Lernen eine Reihe hierarchischer Schichten bzw. eine Hierarchie von Konzepten, um den Prozess des maschinellen Lernens durchzuführen. Die hierbei benutzten KNN sind wie das menschliche Gehirn gebaut, wobei die Neuronen wie ein Netz miteinander verbunden sind.[128] Die erste Schicht des KNN, der sichtbare „Input Layer" verarbeitet eine Rohdateneingabe, wie beispielsweise die einzelnen Pixel eines Bildes.[129] Die Dateneingabe enthält Variablen, die wir beobachten können, daher „sichtbare Schicht."[130]

In Erweiterungen der Lernalgorithmen für Netzstrukturen mit sehr wenigen oder keinen Zwischenlagen, wie beim einlagigen Perzeptron, ermöglichen die Methoden des Deep Learnings auch bei zahlreichen Zwischenlagen einen stabilen Lernerfolg.[131] Deep Learning beinhaltet die Fähigkeit von Computern, aus der Erfahrung zu lernen und die Welt in Bezug auf eine Hierarchie von Konzepten zu verstehen.[132] Durch das Sammeln von Wissen aus der Erfahrung vermeidet dieser Ansatz die Notwendigkeit für die menschlichen Bediener, all das Wissen, das der Computer für seine Arbeit benötigt, formal spezifizieren zu müssen.[133] Die Hierarchie der Konzepte erlaubt es dem Computer, komplizierte Konzepte zu erlernen, indem er sie aus einfacheren zusammensetzt.[134] Wenn man ein Diagramm zeichnet, das zeigt, wie diese Konzepte übereinander aufgebaut werden, dann ist das Diagramm tief, mit vielen Schichten.[135]

[128] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz, 4. Auflage 2016, S. 132, 258, 300, 331, 333. (Ertel, 2016)
[129] *Rashid*, *T.*: Neuronale Netz selbst programmiert, 1. Auflage 2017, S. 8.
[130] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz, 4. Auflage 2016, S. 132, 258, 300, 331, 333.
[131] *Goodfellow*, *I.*; *Bengio*, *Y.*; *Courville*, *A.*:Deep Learning. MIT Press, https://www.deeplearningbook.org/, abgerufen am 11.05.2020.
[132] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz, 4. Auflage 2016, S. 132, 258, 300, 331, 333.
[133] *Goodfellow*, *I.*; *Bengio*, *Y.*; *Courville*, *A.*: Deep Learning. MIT Press, https://www.deeplearningbook.org/, abgerufen am 11.05.2020.
[134] Wikipedia-Stichwort „Künstliches neuronales Netz", abgerufen am 27.04.2020.
[135] *Ertel*, *W.*: Grundkurs Künstliche Intelligenz, 4. Auflage 2016, S. 132, 258, 300, 331, 333. (Kriesel, 2017)

Diese erste Schicht leitet ihre Ausgaben an die nächste Schicht weiter. Diese zweite Schicht verarbeitet die Informationen der vorherigen Schicht und gibt das Ergebnis ebenfalls weiter. Die nächste Schicht nimmt die Informationen der zweiten Schicht entgegen und verarbeitet sie weiter. Diese Schichten werden als versteckte Ebenen (Hidden Layers) bezeichnet.[136] Die in ihnen enthaltenen Merkmale werden zunehmend abstrakt. Ihre Werte sind nicht in den Ursprungsdaten angegeben. Stattdessen muss das Modell bestimmen, welche Konzepte für die Erklärung der Beziehungen in den beobachteten Daten nützlich sind. Dies geht über alle Ebenen des KNN so weiter. Das Ergebnis wird im sichtbaren „Output Layer", der letzten Schicht, ausgegeben. Hierdurch wird die gewünschte, komplizierte Datenverarbeitung in eine Reihe von verschachtelten, einfachen Zuordnungen unterteilt, die jeweils durch eine andere Schicht des Modells beschrieben werden.[137]

Diese Architekturen von KNN, die über mehr als einen Hidden Layer verfügen, machen sich dadurch bemerkbar, dass zwischen den Schichten „neue" Informationen gebildet werden können, die eine Repräsentation der ursprünglichen Informationen darstellen. Wichtig ist hierbei zu verstehen, dass diese Repräsentationen eine Abwandlung bzw. Abstraktion der eigentlichen Eingangssignale sind.[138] Ein solcher Mechanismus, der unter dem Begriff „Feature Learning" bzw. „Representation Learning" zusammengefasst werden kann, sorgt dafür, dass Deep-Learning-Modelle in der Regel sehr effektiv auf neue Datenpunkte abstrahieren können.[139] Die Ursache dafür ist, dass die geschaffenen Abstraktionen der Daten wesentlich generellerer Natur sind als die ursprünglichen Eingangsdaten.[140]

KNN haben nur wenig mit den neuronalen Netzen in Lebewesen zu tun. Denn moderne Deep-Learning-Modelle basieren nur zu einem gewissen Teil aus den Erkenntnissen der Neurowissenschaft.[141] Heute weiß man, dass die Abläufe und Funktionen im menschlichen Gehirn, die zur Verarbeitung von Informationen berechnet werden,

---

[136] *Kriesel*, *D.*: A Brief Introduction to Neural Networks, http://www.dkriesel.com/en/science/neural_networks, abgerufen am 19.02.2017.

[137] Wikipedia-Stichwort „Künstliches neuronales Netz", abgerufen am 27.04.2020.

[138] *Heinz*, *S.*: Deep Learning – Teil 1: Einführung, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, abgerufen am 11.05.2020.

[139] *Bengio*, *Y.*; *Courville*, *A.*; *Vincent*, *P.*: „Representation Learning: A Review and New Perspectives", 2013, https://arxiv.org/abs/1206.5538, abgerufen am 11.05.2020. IEEE Trans. PAMI, special issue Learning Deep Architectures, 35: 1798 – 1828. arXiv:1206.5538. doi:10.1109/tpami.2013.50.

[140] *Heinz*, *S.*: Deep Learning – Teil 1: Einführung, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, abgerufen am 11.05.2020.

[141] *Nielsen*, *M.*: Neural Networks and Deep Learning. Determination Press, http://michaelnielsen.org, abgerufen am 11.05.2020.

wesentlich komplexer sind als in KNNabgebildet.[142] Grundsätzlich kann jedoch die Idee, dass viele einzelne „Recheneinheiten“ (Neuronen) durch eine Vernetzung untereinander Informationen intelligent verarbeiten, als Grundprinzip anerkannt werden.[143]

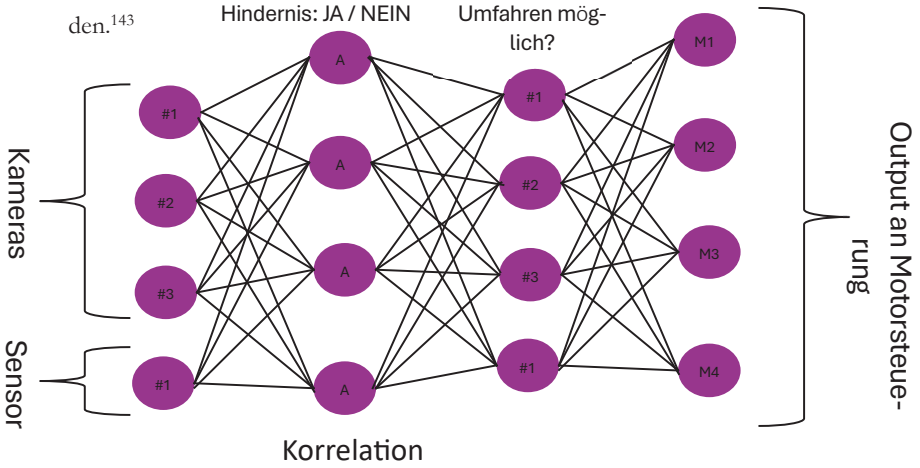


Abbildung 3

Am Anfang dieses Textes wurde ein selbstlernender Saugroboter als Beispiel für ein KNN erwähnt. Doch wie arbeitet dieser Saugroboter konkret, wie schafft er es, Tischbeine, Stühle, Schränke und Kinderspielzeug, welches immer wieder an unterschiedlichen Orten liegen kann, zu umfahren? Diese Frage lässt sich relativ einfach beantworten: Der Saugroboter verfügt über Berührungssensoren und Kameras. Die Kameras können mittels einfacher Bilderkennung registrieren, ob ein Hindernis vor ihnen liegt. Aber auch Gefühlsensoren bekommen eine Information, wenn der Saugroboter aneckt. Diese unterschiedlich gewonnenen Informationen bilden zusammen den oben abstrakt erläuternden Input Layer, also die erste Schicht des KNN. Was macht die KI mit der aus dem Input Layer gewonnenen Information? Es operationalisiert diese Information im zweiten Layer, einem Hidden Layer. Konkret fragt sich

[142] *Schreiber*, *S. B.*: Natürliche Intelligenz. Neuronen und Synapsen – alles nur ein organischer Computer? (Teil 1), c't – Magazin für Computertechnik, 1987 (4), S. 98 ff.

[143] *Heinz*, *S.*: Deep Learning – Teil 1: Einführung, https://www.statworx.com/de/blog/deep-learning-teil-1-einfuehrung/, abgerufen am 11.05.2020.

die KI des Saugroboters: „Liegt vor mir ein Hindernis?“ und vergleicht dabei die unterschiedlichen Informationen von den Sensoren. Das Operationalisieren erfolgt dann nach dem oben beschriebenen Beispiel, wo zwischen Raupen und Marienkäfern unterschieden wurde. Im dritten Layer, ebenfalls ein Hidden Layer, fragt sich die KI des Saugroboters, ob ein Umfahren des Hindernisses möglich ist und im vierten Layer (Output Layer) steuert nach diesen Daten die KI die einzelnen Motoren des Saugroboters.[144]

Die Funktionsweise von intelligenten Saugrobotern unterscheidet sich methodisch nicht sehr von einem KNN für den Handel mit Wertpapieren (sog. „Algotrading“), siehe Abbildung 4. An die Stelle von Berührungssensoren und Kameras treten unterschiedliche, aus legalen Quellen gewonnene Finanzinformationen, so z. B. vom Kapitalmarkt, von globalen Wertpapierbörsen, von Newsanbietern (z. B. Reuters) oder auch Jahresberichte von Unternehmen. Ähnlich wie beim Saugroboter bildet diese Erfassung von relevanten Informationen den Input Layer. In den folgenden Hidden Layers werden die Informationen normativiert, also gewichtet und bewertet. Im Output Layer werden dann Entscheidungen gefällt, wie „Kaufen“, „Verkaufen“, „Kaufen ab Wert x“ und „Verkaufen bis Wert y“.[145]

[144] *Zweig*, *K.*: Ein Algorithmus kennt kein Taktgefühl, 1. Auflage 2019, S. 140 ff.
[145] *Zweig*, *K.*: Ein Algorithmus kennt kein Taktgefühl, 1. Auflage 2019, S. 140 ff.

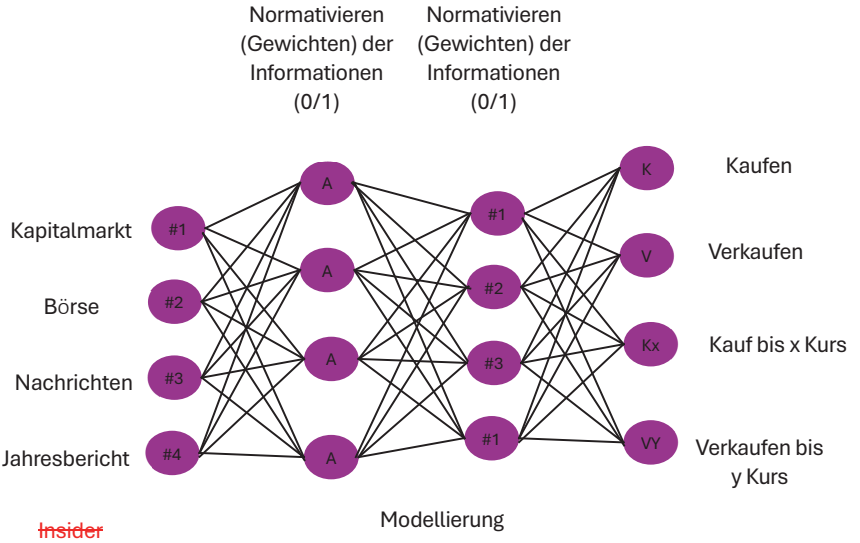


Abbildung 4

VI. Rechtsschutz für Maschinelles Lernen

Die Rechtsfragen bei den oben beschriebenen KNN lassen sich in zwei Grundfragen aufteilen: Zum einen den Schutz für die Erschaffung der KNN und zum anderen den Schutz der durch die KNN erhaltenen Informationen.

1. Schutz für die Schaffung eines künstlichen neuronalen Netzwerkes

Der Schutz für die Schaffung eines KNN als Anwendungsfeld von ML kann sich aus dem Patentrecht, aus dem Urheberrecht und aus dem Geschäftsgeheimnisgesetz ergeben.

a) Patentschutz für KNN

Leider fehlt es bei der alleinigen Schaffung von KNN an den für das Patentrecht gem. § 1 Abs. 2 und 3 PatG und Art. 52 Abs. 2 und 3 EPÜ so notwendigen technischen Verfahren, um einen wirksamen Patentschutz zu entfalten. So würde es für das KNN für den Handel mit Wertpapieren („Algotrading“) wahrscheinlich keinen Patenschutz geben. Denn kommt eine an und für sich nicht technische Methode, z. B. eine mathematische Methode, in einem technischen Verfahren zum Einsatz, das mit Hilfe von technischen Mitteln zur Ausführung der Methode auf eine physikalische

Erscheinung angewandt wird und bei dieser eine Veränderung hervorruft, so trägt diese Methode zum technischen Charakter der Erfindung als Ganzes bei. Ein grundlegender Unterschied zwischen einer mathematischen Methode und einem technischen Verfahren ist darin zu sehen, dass eine mathematische Methode oder ein mathematischer Algorithmus mit Zahlen (die etwas Beliebiges darstellen können) ausgeführt wird und zu einem in Zahlen ausgedrückten Ergebnis führt. Denn die mathematische Methode oder der Algorithmus ist nur ein abstraktes Konzept, das beschreibt, wie mit Zahlen zu verfahren ist.[146] Das betreffende Merkmal ist daher bei der Beurteilung der erfinderischen Tätigkeit zu berücksichtigen.[147] Daher die Erschaffung von KNN nicht patentierbar.

Dies ist natürlich im Zusammenhang mit dem Saugroboter anders zu sehen, da hier ein technisches Verfahren vorliegen dürfe, da der Roboter an sich über ein technisches Verfahren verfügt. Wahrscheinlich wäre das KNN in der Steuerungssoftware des Saugroboters integriert und diese Steuerungssoftware würde als sog. Embedded Software mit patentiert, werden können. Denn bei Hardware, die von einer Software gesteuert wird, geht es nicht um Patentschutz für die Software als solche, sondern für die technische Erfindung (Hardware). In der BGH-Entscheidung „Sprachanalyseeinrichtung“[148] wurde die Frage der Technizität von Computerprogrammen mittels der Verbindung von Hard- und Software zu einer Einheit beantwortet.[149] Diese sich vermeintlich abzeichnende weitere Öffnung des Patentschutzes für Computerprogramme wurde vom BGH in der Entscheidung „Suche fehlerhafter Zeichenketten“[150] erheblich eingeschränkt,[151] so dass heute keine eindeutigen Kriterien für die Patentfähigkeit von Software bestehen.[152] Grundsätzlich ist nicht von Patentfähigkeit auszugehen, wenn eine Software als solche, ohne zusätzliche technische Erfindung, angemeldet werden soll. Anders liegt der Fall natürlich, wenn die Software eine Maschine steuert.

[146] T 208/84, ABl. 1987, S. 14.
[147] T 208/84, ABl. 1987, S. 14; T 641/00; T 258/03; T 1814/07, ABl. 2003, S. 352.
[148] BGH, 11.05.2000 – X ZB 15/98, BGHZ 144, S. 282 = MDR 2000, S. 1447.
[149] *Marly*, *J.*: Praxishandbuch Softwarerecht, 5. Aufl. 2009, Rn. 398.
[150] BGH, 17.10.200 – X ZB 16/00, BGHZ 149, S. 68 = GRUR 2002, S. 143.
[151] *Marly*, *J.*: Praxishandbuch Softwarerecht, 5. Aufl. 2009, Rn. 398.
[152] *Marly*, *J.*: Praxishandbuch Softwarerecht, 5. Aufl. 2009, Rn. 398.

b) Urheberrechtlicher Schutz als Werk

Die Frage, ob sich ein urheberrechtlicher Schutz als Werk für die Schaffung eines KNN ergibt, richtet sich danach, in welchem Status sich das KNN befindet.[153] Somit wird die Darstellung eines KNN analog zum Algorithmus in der Form eines einfachen Entscheidungsbaums bzw. der einfachen Darstellung des KNN wie in Abbildung 1 bis Abbildung 4 i. d. R. keinen urheberrechtlichen Schutz nach § 69a BGB genießen. Anders verhält es sich, wenn der Entscheidungsbaum schon die Qualität eines Programmablaufplanes erreicht. Dann könnte dieser Programmablaufplan den Schutz als Entwurfsmaterial eines Computerprogrammes nach § 69a Abs. 2 UrhG entsprechenden urheberrechtlichen Schutz genießen.[154]

Bei einem mathematisch dargestellten Algorithmus bzw. KNN, wie z. B. dem euklidischen Algorithmus, ist kein urheberrechtlicher Schutz anzunehmen. Dagegen kann bei der Darstellung eines KNN in einem Pseudocode durchaus von einem urheberrechtlichen Schutz angenommen werden, auch wenn dieser nicht aus der Vergleichbarkeit zum Quellcode zu entnehmen ist, sondern als Entwurfsmaterial eines Computerprogrammes nach § 69a Abs. 2 UrhG entsprechenden urheberrechtlichen Schutz genießt.[155]

Wurde das KNN als Code, z. B. bei der Programmiersprache Python, aufgebaut, so kann durchaus von einem urheberrechtlichen Schutz, vergleichbar mit dem eines Softwareprogramms nach § 69a Abs. 1 UrhG ausgegangen werden.[156]

c) Urheberrechtlicher Schutz als Datenbank

Fraglich ist, ob die oben dargestellte Struktur eines KNN der Struktur einer Datenbank entspricht und deshalb einen Urheberrechtlicher Schutz nach §§ 87a ff. UrhG genießen könnte. Nach § 87 a Abs. 1 Nr. 1 UrhG ist eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen geschützt, wenn sie systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere

[153] Siehe hierzu ausführlich *Söbbing*, *T*. in: CR 2020, S. 223-228.
[154] *Hoeren*, *T*.; *Wehkamp*, *N*. in: CR 2018, S. 1-7.
[155] *Hoeren*, *T*.; *Wehkamp*, *N*. in: CR 2018, S. 1-7.
[156] Siehe hierzu ausführlich *Söbbing*, *T*. in: CR 2020, S. 223-228.

Weise zugänglich ist und ihre Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Lösungen im Big-Data-Umfeld leben gerade davon, dass Daten zu groß, zu komplex, zu schnelllebig oder zu schwach strukturiert sind und erst Datenbanken es ermöglichen, diese Daten zu beherrschen.[157]

Gegebenenfalls könnte man in einzelnen Fällen zu der Ansicht kommen, dass die Schaffung eines KNN unter die Subsumption einer Datenbank i. S. v. § 87a Abs. 1 S. 1 UrhG fällt, auch wenn diese Daten nicht lange gespeichert werden, weil sie, wie im Falle des Saugroboters oder des Algotradings, extrem schnell veralten. Aber grundsätzlich sammelt das KNN Daten, ordnet diese systematisch oder methodisch an, bevor es diese Dritten zur Verfügung stellt. Dass dies eine wesentliche Investition erfordert, dürfte unterstellt werden können. Diese durch KNN gesammelten Daten werden systematisch und methodisch angeordnet i. S. v. § 87a UrhG.[158] Zwar wird bei einer Big-Data-Analyse, bei der die Auswertung unstrukturierter Datenmengen vorgenommen wird, der Datenbankbegriff in Frage gestellt, weil die Daten nicht voneinander unabhängig sind,[159] dies ist bei KNN aber i. d. R. anders zu sehen. Grundsätzlich müssen Daten, die ausgetauscht werden sollen, aus technischen Gründen systematisch und methodisch angeordnet werden.[160] Dabei sieht der EuGH die Voraussetzung der Unabhängigkeit weniger eng, sondern legt diese Voraussetzung sehr großzügig aus,[161] was gerade die Betrachtung im Rahmen der KNN sehr erleichtert.

Im Zusammenhang der Erschaffung eines KNN stellt sich die Frage nach der Erfordernis der Unabhängigkeit der einzelnen Elemente der Datenbank.[162] Nach der Rechtsprechung des EuGH kommt ein Datenbankherstellerrecht nur in Betracht, wenn sich die einzelnen Elemente voneinander trennen lassen, ohne dass der Wert ihres informativen, literarischen, künstlerischen, musikalischen oder sonstigen Inhalts

---

[157] *Bachmann*, *R.*; *Kemper*, *G.*; *Gerzer*, *T.*: Big Data – Fluch oder Segen? Unternehmen im Spiegel gesellschaftlichen Wandels, 2014, S. 2.
[158] *Grützmacher*, *M.* in: CR 2016, S. 485-495 (487).
[159] *Hoeren*, *T.*; *Völkel*, *J.* in: *Hoeren, T.*: Big Data und Recht, 2014, S. 22.
[160] *Peschel*, *C.*; *Rockstroh ,S.* in: MMR 2015, S. 571 ff. (572).
[161] EuGH, 29.10.2015 – C-490/14 = GRUR 2015, S. 1187; MMR 2016, S. 51; K&R 2015, S. 790; afp 2016, S. 33; EuGH, 09.11.2004 – C-444/02 = Slg. 2004, I-10549, GRUR 2005, S. 254, GRUR Int. 2005, S. 239; CR 2005, S. 412.
[162] *Hetmank*, *S.*; *Lauber-Rönsberg*, *A.* in: GRUR 2018, S. 574.

dadurch beeinträchtigt wird.[163] Diese Frage gewinnt daher an Bedeutung, da bei KNN Ergebnisse erzeugt werden, die aus unterschiedlichen Quellen generiert werden und zusammen eine Einheit bilden, z. B. der Saugroboter, der mittels Kameras und Tastsensoren einen Raum analysiert. Der EuGH legt bei der Beurteilung des selbstständigen Informationswerts eines aus einer Sammlung herausgelösten Elements nicht auf die Perspektive des typischen Nutzers der betreffenden Sammlung, sondern auf einen beliebigen Dritten, der sich für das herausgelöste Element interessiert.[164] Der EuGH nennt als Beispiel einzelne geografischen Daten einer topografischen Karte.[165] Somit dürfte das Erfordernis der Unabhängigkeit der Elemente angesichts der durch die technischen Entwicklungen zunehmenden Möglichkeiten, den Informationsgehalt von Daten in verschiedenen Kontexten auszuwerten, keine allzu große Hürde darstellen, da ihnen nicht selten nach deren Herauslösung ein hinreichender und selbstständiger, aus Sicht eines Dritten zu beurteilender Wert verbleiben wird.[166]

Gem. § 87b Abs. 1 S. 1 UrhG hat der Datenbankhersteller das ausschließliche Recht, die Datenbank insgesamt oder einen nach Art oder Umfang wesentlichen Teil der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Damit ergibt sich grundsätzlich kein Schutz, wenn Einzeldaten von weniger als 10 % entnommen werden.[167] Hierbei ist aber zu berücksichtigen, dass auch sukzessive Vervielfältigungen, Verbreitungen oder öffentliche Wiedergaben, wenn sie nur unwesentliche Teile der Datenbank betreffen, in der Summe einem wesentlichen Teil gleichstehen, vgl. § 87b Abs. 1 S. 2 UrhG. Dennoch muss berücksichtigt werden, dass in der horizontalen Vernetzung auch geringe Datenmengen als schutzbedürftig zu betrachten sind, insbesondere auch dann, wenn Einzeldaten einen erheblichen Einfluss auf Prozessabläufe haben können bzw. die Systeme durch die Veränderung der Einzeldaten manipuliert werden.[168] Es geht dabei vor allem um den Schutz der

[163] EuGH, 29.10.2015 – C-490/14 = GRUR 2015, S. 1187 Rn. 17 – Freistaat Bayern/Verlag Esterbauer.
[164] *Hetmank*, *S.*; *Lauber-Rönsberg*, *A.* in: GRUR 2018, S. 574.
[165] BGH, 20.11.2008 - I ZR 112/06 = GRUR 2009, S. 403 – Metall auf Metall I; BGH, 13.12.2012 - I ZR 182/11 GRUR 2013, S. 614 – Metall auf Metall II; GRUR 2017, S. 895 – Metall auf Metall III.
[166] *Hetmank*, *S.*; *Lauber-Rönsberg*, *A.* in: GRUR 2018, S. 574.
[167] BGH, 21.07.2005 - I ZR 290/02 = BGHZ 164, S. 37; NJW 2005, S. 3216 (Ls); MDR 2006, S. 104 (Ls.); GRUR 2005, S. 857; MMR 2005, S. 754; K&R 2006, S. 38; ZUM 2005, S. 731; afp 2005, S. 470; CR 2005, S. 849.
[168] *Grützmacher*, *M.* in: CR 2016, S. 485-495 (488).

Unversehrtheit von Daten, da bereits leichteste Veränderungen zur Unbrauchbarkeit von Datenstämmen führen können.

2. Schutz für die Ergebnisse des Maschinellen Lernens

Nun mag der Schutz für die Ergebnisse des Maschinellen Lernens durch das KNN in vielen Fällen gar nicht so bedeutsam sein. Sicherlich wird der Hersteller und auch der Nutzer des Saugroboters kein Interesse daran haben, dass der Weg, den der Saugroboter zurückgelegt hat, geschützt wird. Aber in vielen Fällen erzeugt das KNN Daten, die es lohnen, geschützt zu werden. Unabhängig vom Datenschutz stellt sich daher die Frage, ob diese durch KNN gesammelten Daten rechtlich geschützt und übertragen werden können.

a) Daten

Fraglich ist, ob eine Art Eigentum an den gesammelten Daten begründet werden kann.[169] Dabei werden Daten „auch" als Informationen verstanden, die nicht oder nicht ausreichend derart bearbeitet wurden, dass sie in den Schutzbereich von Immaterialgüterrechten, wie insbesondere das Patent- oder Urheberrecht, fallen.[170] Solche Informationen sind i. S. d. Immaterialgüterrechts „gemeinfrei" und können unter der Berücksichtigung des Datenschutzrechts von jedermann genutzt werden. Der EuGH hat in mittlerweile zwei Entscheidungen einen Leistungsschutz für künftig zu generierende Daten nicht anerkannt; geschützt werden soll nach Ansicht des EuGH nur die Investition in bereits vorhandenen Daten.[171]

Schuldrechtlich stellt sich die Frage, ob die durch das KNN gesammelten Daten i. S. v. § 433 BGB verkauft werden oder ob hier auf der Basis einer Sui-generis-Vereinbarung die Daten weitergegeben werden können. Beim Verkauf stellt sich die Frage nach der Sacheigenschaft von Daten, was einen Verkauf i. S. v. § 433 BGB erheblich erschwert. Eine originäre Anwendung der §§ 433 ff. BGB beim Datenhandel kann aber nur dort stattfinden, wo sich die Daten mittelbar einer Sache (z. B. einem

[169] *Heymann*, *T.* in: CR 2016, S. 650-657 (650). (Ensthaler, 2016)
[170] *Ensthaler*, *J.* in: NJW 2016, S. 3473-3552, (3473).
[171] EuGH, 09.11.2004 – C-203/02 = Slg. 2004, I-10415; NJW 2005, S. 1263 (Ls.); GRUR 2005, S. 244; GRUR Int. 2005, S. 247; EuZW 2004, S. 757; MMR 2005, S. 29; ZUM 2005, S. 1 und EuGH, 09.11.2004 – C-444/02 = Slg. 2004, I-10549; GRUR 2005, S. 254; GRUR Int. 2005, S. 239.

Datenträger) zuordnen lassen.[172] In den allermeisten Fällen – z. B. bei der rein elektronischen Datenübertragung per FTP, E-Mail etc. – scheitert es an der fehlenden Sacheigenschaft der Daten selbst.[173] Durch § 453 Abs. 1, Alt. 2 BGB können Daten als sonstige Gegenstände aufgefasst werden[174], womit der Weg zu den §§ 433 ff. BGB über den Rechtskauf eröffnet ist. Entscheidend ist dabei allein die zu bejahende translative Übertragbarkeit von Daten in Abgrenzung zur konstitutiven Übertragung beispielsweise von Urheberrechten (vgl. § 29 Abs. 1 UrhG),[175] unabhängig davon, ob die Daten tatsächlich nur kopiert oder unter gleichzeitiger Löschung übertragen werden.[176] Der Datenverkäufer ist folglich gem. §§ 453, 433 Abs. 1 S. 2 BGB verpflichtet, dem Datenkäufer das Datum beziehungsweise die Daten frei von Sach- und Rechtsmängeln zu verschaffen. [177]

Noch nicht abschließend geklärt ist, auf welcher Rechtsgrundlage die Weitergabe der Daten im Rahmen der DSGVO gerechtfertigt ist.[178] Dabei wird vertreten, dass die Verarbeitung in diesem Kontext auf Grundlage der allgemeinen Rechtfertigungstatbestände, insbesondere Art. 6 Abs. 1 S. 1 lit. f DSGVO, zulässig ist.[179] Nach anderer Ansicht genügt es bereits, dass die Voraussetzungen des Art. 28 DSGVO für eine Auftragsdatenverarbeitung erfüllt sind.[180] Mit Blick darauf, dass die Auftragsverarbeitung eine Form der Privilegierung darstellt, ist es überzeugend, allein auf die Vorgaben des Art. 28 DSGVO abzustellen.[181] Der Betreiber der KI-Technologie kann für seinen Kunden dann aber nur im engen Rahmen des Art. 28 DSGVO tätig werden, also

[172] *Beckmann*, *R. M.* in: Staudinger, BGB, 2014, § 453 BGB, Rn. 37; *Patzak*, *A.*; *Beyerlein*, *T.* in: MMR 2007, S.687 (688); vgl. auch *Hieke*, *R.* in: InTeR 2017, S. 10, 11 f.; zu §§ 377, 381 Abs. 2 HGB ebenso BGH, 14.07.1993 – VIII ZR 147/92, NJW 1993, S. 2436, 2437 f.; BGH, 15.11.2006 - XII ZR 120/04, NJW 2007, S. 2394, 2394 – Software.

[173] *Kirchner*, *G.* in: InTeR 2018, S. 19-24.

[174] *Berger*, *C.* in: Jauernig, BGB, 14. Aufl. 2011, § 453, Rn. 11; *Hauck*, *R.* in: NJW 2014, S. 3616 (3616); *Grosskopf*, *L.* in: IPRB 2011, S. 259 (259); OLG Düsseldorf, 17.02.2010 - 17 U 167/09, BeckRS 2010, 09514 – zu Adressdaten; LG München I, 10.12.2008 - 16 HK O 10382/08, BeckRS 2009, 88429 – zu E-Mailadressen; vgl. auch RegE, BT-Drucks. 14/6040, S. 242, wo aber ausdrücklich nur die Software als sonstiger Gegenstand aufgeführt wurde; dagegen offen gelassen von: OLG Düsseldorf, 30.07.2004 - I-23 U 186/03, BeckRS 2004, 08836 – präferierter Werklieferungs- oder Werkvertrag; BGH, 30.06.1976 - VIII ZR 267/75, NJW 1976, 1886, 1887 – Kauf- oder Mietvertrag.

[175] *Pahlow*, *L.* in: JA 2006, S. 385 (385), allgemein zum Rechtskauf.

[176] Vgl. hierzu *Hoppen*, *P.* in: CR 2015, S. 802 (803), wobei dessen Aussage, dass jede Datenübertragung ein Kopiervorgang sei, beispielsweise auf die datenträgergebundene Übertragung nicht zutreffen kann.

[177] *Kirchner*, *G.* in: InTeR 2018, 19-24.

[178] *Heckmann*, *D.* in: *Heckmann*, *D.*: jurisPK-Internetrecht, 5. Aufl. 2017, Kap. 9 1. Überarbeitung Rn. 214.

[179] *Spoerr*, *W.* in: Wolff/Brink, Beck'scher Onlinekommentar, Stand 01.11.2017, Art. 28 DSGVO, Rn. 30 f.

[180] *Schmidt*, *B.*; *Freund*, *B.* in: ZD 2017, S. 14 (16); a. A. *Hartung*, *J.* in: *Kühling*, *J.*; *Buchner*, *B.*: DS-GVO/BDSG, 2. Aufl. 2018, Art. 28, Rn. 22.

[181] So auch *Thomale*, *P.-C.* in: Auernhammer, DS-GVO/BDSG, 5. Aufl. 2017, Art. 28, Rn. 8.

auf Weisung des Kunden, und er muss die nach Art. 28 Abs. 1 DSGVO entsprechenden Garantien abgeben, dass die geeigneten technischen und organisatorischen Maßnahmen i. S. v. Art. 32 DSGVO so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

b) Geschäftsgeheimnisse

Eine andere Möglichkeit, einen rechtlichen Schutz für die durch das KNN gesammelten Daten zu genieren, wäre über das Geschäftsgeheimnisgesetz (GeschGehG). Als Geschäftsgeheimnis i. S. d. GeschGehG ist eine Information schon dann geschützt, wenn sie die Anforderungen nach § 2 Abs. 1 GeschGehG erfüllt. Ein Geschäftsgeheimnis ist danach eine Information,

- die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist, und
- die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und
- bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Inhaber eines Geschäftsgeheimnisses jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat, vgl. § 2 Abs. 2 GeschGehG. Rechtsverletzer ist gem. § 2 Abs. 3 GeschGehG jede natürliche oder juristische Person, die entgegen § 4 ein Geschäftsgeheimnis rechtswidrig erlangt, nutzt oder offenlegt; Rechtsverletzer ist nicht, wer sich auf eine Ausnahme nach § 5 berufen kann;

Eine wichtige Voraussetzung ist, dass gem. § 2 Nr. 1 lit. b GeschGehG die Information kommerziellen Wert haben muss, da sie geheim ist. Dabei ist wichtig zu erwähnen, dass das Geheimhaltungsinteresse im Vergleich zu einem kommerziellen Wert der allgemeinere Begriff ist. Er erfasst nicht nur Informationen, die einen positiven Wert haben, sondern auch solche Geheimnisse, die zwar keinen Wert vermitteln, deren Bekanntwerden umgekehrt aber Schaden verursachen könnte.[182] Zu denken ist

[182] BGH, 27.04.2006 – I ZR 126/03, GRUR 2006, S. 1044, Rn. 19 – Kundendatenprogramm; BGH, 10.05.1995 – 1 StR 764/94, NJW 1995, S. 2301 – Angebotsunterlagen.

etwa an potenziell imageschädigende Informationen oder gar Informationen über rechtswidrige Vorgänge im Unternehmen, etwa Kartellrechtsverstöße. Zweifelsohne kann ein Bekanntwerden solcher Informationen zu erheblichen Vermögensnachteilen – seien es Geldbußen oder ein Absatzrückgang – führen.[183] Allerdings wird man solche Informationen (anders als beispielsweise produktiv einsetzbares Know-how) nicht als Vermögenswerte des Unternehmens bezeichnen können.[184] Dies dürfte beim Schutz von Deep Learning aber weniger eine Rolle spielen. Hierfür spielt mehr der Erwägungsgrund 14 der Geschäftsgeheimnis-RL eine Rolle, der davon spricht, dass die zu schützenden Informationen einen realen oder potenziellen Handelswert verkörpern sollten.[185] Dies kann i. d. R. bei komplexen KNN bejaht werden. Denn niemand würde bestreiten, dass die gesammelten Informationen, z. B. bei der Gesichtserkennung, einen größeren Wert darstellen. Eine Veröffentlichung der Information aus KNN würde wahrscheinlich dem Unternehmen in erheblichem Maße Schaden zufügen.

Der § 2 GeschGehG führt dazu, dass KI-Hersteller bestimmte Schutzmaßnahmen umsetzen können. Diese Maßnahmen müssen zudem „angemessen" und „den Umständen entsprechend" sein. Je nach Art und Bedeutung der geheimen Information können sich Grad und Intensität der erforderlichen Sicherungsmaßnahmen im Einzelfall also unterscheiden.[186] Die Verwertung des Geschäftsgeheimnisses steht somit dem Inhaber zu.[187]

Dabei muss natürlich auch der Datenschutz berücksichtigt werden, da eine KI nicht so ohne Weiteres personenbezogene Informationen sammeln darf, da sie den Anforderungen der DSGVO unterliegt.

[183] *Kalbfus*, *B.*: GRUR 2016, S. 1009.
[184] Stellungnahme der GRUR vom 19.03.2014, S. 4, abrufbar unter http://www.grur.org/de/stellungnahmen.html; a. A. *Redeker*, *S. S.*; *Pres*, *S.*; *Gittinger*, *C.*: WRP 2015, S. 681, Rn. 7.
[185] *Scheja*, *K.* in: CR 2018, S. 485.
[186] *Frisse*, *F.*; *Glaßl*, R.; *Baranowski*, A.; *Duwald*, *L.* in: BKR 2018, S. 177.
[187] *Scheja*, *K.* in: CR 2018, S. 485.

c) Resümee

Der Schutz von KNN fällt in das Rechtsgebiet des sehr neuen und gar nicht richtig erfassten Artificial Intelligence Law (AI-Law).[188] Dabei kann man nicht wirklich von einem Rechtsgebiet sprechen, da die Forschung über diese Rechtsfragen sehr am Anfang steht und sich zudem neue rechtliche Erkenntnisse ergeben. Derzeit, und hoffentlich gilt das nicht für die Ewigkeit, kann kein Patentschutz für ein reines, also nicht in einer Hardware eingebettetes KNN unterstellt werden. Denkbar ist aber ein urheberrechtlicher Schutz, der sich aber, wie oben dargestellt, herleiten muss. Der Schutz für die Ergebnisse des KNN lässt sich ggf. über die Rechtsprechung des EuGH zum Investitionsschutz bei der Erfassung von Daten generieren und über das Geschäftsgeheimnisgesetz.

V. Urheberrechtliche Grenzen für Maschinelles Lernen[189]

Ein fundamentales Anwendungsfeld von künstlicher Intelligenz (KI) ist das Machine Learning. Damit eine KI, z. B. ChatGPT für Text oder Stability AI für Bilder, lernen kann, braucht sie Rohmaterial in der Form von Informationen, welche vorwiegend aus dem Internet stammen. Die rechtlichen Rahmenbedingungen für das Text und Data Mining wurden in bereits 2021 in Deutschland mit dem § 44b UrhG geschaffen. Dies hat Bedeutung auch für die Gestaltung von Bildern, sofern hierfür Data Mining betrieben wird.

1. Einleitung

Maschinelles Lernen benötigt sehr große Mengen an authentischen Trainingsdaten, um seine Möglichkeiten stets weiterzuentwickeln und zu verbessern zu können. Neben den bekannten Textgeneratoren wie das bereits genannte ChatGPT von OpenAI benötigen vor allem Bildgeneratoren große Mengen an Vergleichsdaten für das Training ihrer KI. Trainingsdaten für Bildgeneratoren werden u. a. von kommerziell agierenden Firmen, wie Stability AI[190] oder Mindverse[191], genutzt, um ihre

[188] „KI" – künstliche Intelligenz, englisch: artificial intelligence, „AI" und Gesetz englisch law = „AI Law". *Söbbing*, *T.*: Fundamentale Rechtsfragen Künstlicher Intelligenz, 1. Auflage 2019, S. 4.

[189] ***Urheberrechtliche Grenzen für lernende Künstliche Intelligenz" zu den Fragen des Text und Data Mining (§ 44b UrhG)*** Söbbing/Schwarz, RDi 5/ 2023, 415

[190] Pick-a-Pic: An Open Dataset of User Preferences for Text-to-Image Generation – Stability AI.

[191] https://www.mind-verse.de (abgerufen am 06.07.2023).

bildgenerierende KIs zu trainieren.[192] Hierzu werden u. a. Websites im Internet analysiert, um Texte und Bilder zu vergleichen.[193] Das hierbei verwendete Deep Learning ist ein selbstadaptiver Algorithmus, der ein künstliches neuronales Netz (KNN) nutzt. Diese KNN sind bei der Bilderkennung auf sog. Bilderkennungs-Algorithmen angewiesen, mithin verschiedene Techniken, um Bilder im Internet zu analysieren. Ein dazu eingesetztes Mittel sind Webcrawler[194], welche u. a. das World Wide Web durchsuchen, nicht anders als bislang auch die bekannten Suchmaschinen.

Im Bereich der KI-Anwendungen wird in einem ersten Schritt ein gefundenes/r Bild/Text analysiert und die darin enthaltenen (visuellen) Merkmale extrahiert. Dazu werden maschinelle Lernalgorithmen eingesetzt, z. B. Convolutional Neural Networks (CNN oder ConvNet).[195] Alle eingesetzten Algorithmen sind darauf trainiert, bestimme visuelle Muster und Merkmale in Bildern, wie Formen, Linien, Farben oder Texturen, zu erkennen. Nachdem das Bild analysiert wurde, werden bestimmte Merkmale extrahiert, die der Identifizierung des Inhalts oder der Kategorisierung des Bildes dienen (sog. Merkmalsextraktion). Dies kann beispielsweise die Erkennung von Objekten, Gesichtern, Text oder bestimmten Mustern sein. Basierend auf den extrahierten Merkmalen wird das Bild in verschiedene Kategorien oder Klassen eingeordnet, die sog. Klassifizierung und das Labeling. Dies kann beispielsweise bedeuten, dass das Bild als Landschaft, Tier, Mensch oder Gegenstand identifiziert wird. Diese Klassifizierung kann auf vordefinierten Kategorien basieren oder durch maschinelles Lernen ermöglicht werden, indem der Algorithmus zuvor mit einer großen Menge gelabelter Bilder trainiert wurde oder sich selbst trainiert hat. Dabei kann der Webcrawler auch zusätzliche Metadaten zum Bild sammeln, wie den Titel der Website, die Bildquelle, den Autor oder andere Informationen, die dem Bild zugeordnet sind. Diese Metadaten können dabei helfen, das Bild weiter zu beschreiben und zu kategorisieren.[196]

---

[192] https://www.alltageinesfotoproduzenten.de/2023/04/24/laion-e-v-macht-ernst-schadensersatzforderung-an-urheber-fuer-ki-trainingsdaten/ (abgerufen am 06.07.2023).

[193] *Steiner* in C't 7/2023, 16-17 (16).

[194] auch Spider, Searchbot oder Robot genannt.

[195] siehe hierzu u. a. *Fukushima*, Bio.Cybernetics 36, 193-202 (1980); *LeCun* et al, Gradient-Based Learning Applied to Document Recognition, Proc. of the IEEE, November 1998.

[196] Es ist wichtig anzumerken, dass die genaue Funktionsweise eines Webcrawlers zur Bildanalyse von den verwendeten Algorithmen und Technologien abhängt. Es gibt verschiedene Ansätze und Methoden, um Bilder zu analysieren und die Entwicklung in diesem Bereich schreitet stetig fort. Die dargestellte Methode kann daher nicht als abschließend bezeichnet werden.

2. Rechtsgrundlage

Fraglich ist, ob in der oben dargestellten Arbeitsweise eines Bilderkennungs-Algorithmus eine Urheberrechtsverletzung zu sehen ist. Gerade Medienanbieter und Verlage fühlen sich durch die Arbeitsweise von Bilderkennungs-Algorithmen in ihren Urheberrechten verletzt.[197] Die Hoffnung von *Spindler*, mit der Verwirklichung des Vorschlags der EU-Kommission bestünden gute Chancen, dass die schon zuvor Jahre dauernde Diskussion um das Text und Daten Mining ein vernünftiges Ende nehmen könnte, indem auch kommerzielle Verwertungen zugelassen werden, hat sich erkennbar (noch) nicht ganz bewahrheitet.[198] Zwar sind mit der Reform der Urheberrechtslinie 2019[199] neue, besondere Regelungen aufgenommen worden, die die Entwicklung von KI-Technologien im Bereich der EU nicht behindern, vielmehr fördern sollen. So ist nach Artikel 4 der RL das Text Mining grundsätzlich zulässig, vgl. § 60d UrhG.

Art. 4 Abs. 1 der RL sieht eine Ausnahme oder Beschränkung der Rechte vor, die in Artikel 5 Buchstabe a und Art. 7 Abs. 1 der Richtlinie 96/9/EG,[200] Art. 2 der Richtlinie 2001/29/EG, Art. 4 Abs. 1 Buchstaben a und b der Richtlinie 2009/24/EG[201] und Art. 15 Abs. 1[202] der Richtlinie niedergelegt sind, für die zum Zwecke des Text und Data Mining vorgenommene Vervielfältigungen und Entnahmen von rechtmäßig zugänglichen Werken und sonstigen Schutzgegenständen vor. Die Regelungen wurde in § 44b und § 60d UrhG umgesetzt[203]. Damit gibt es im deutschen UrhG nun zwei, sich in Einzelheiten unterscheidende Schrankenvorschriften für das Text und Data Mining – § 44b im Allgemeinen und § 60d für nicht kommerzielle, wissenschaftliche Zwecke.[204] Ein Data Mining soll nach dem Willen des Verordnungsgebers grundsätzlich rechtlich möglich sein. So wird in einem der Erwägungsgründe ausgeführt[205], das Text und Data Mining könne auch für reine, nicht urheberrechtlich geschützte Fakten oder Daten erfolgen, und in diesen Fällen sei nach dem Urheberrecht keine Erlaubnis

---

[197] *Steiner* in C't 7/2023 16-17 (16).
[198] *Spindler*, GRUR 2016, 1112, beck-online.
[199] 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.
[200] https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31996L0009 (abgerufen am 06.07.2023).
[201] https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32001L0029 (abgerufen am 06.07.2023).
[202] https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32001L0029 (abgerufen am 06.07.2023).
[203] vgl. BT-Drs. 19/27426, 87.
[204] BeckOK UrhR/Hagemeier, 38. Ed. 01.02.2023, UrhG § 44b Rn. 1.
[205] Erwägungsgrund 9 der Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019

erforderlich. Zu beachten ist weiter, dass es auch Fälle des Text und Data Minings geben kann, in denen bereits keine Vervielfältigungshandlung erfolgt oder die Vervielfältigungen unter die in Art. 5 Abs. 1 der Richtlinie 2001/29/EG vorgesehene verbindliche Ausnahme für vorübergehende Vervielfältigungshandlungen fallen, die auch künftig auf Verfahren des Text und Data Mining angewandt werden sollte, die nicht die Anfertigung von Kopien in einem über diese Ausnahme hinausgehenden Umfang einschließen.

Forscher können sich nach der erfolgten Umsetzung der EU-Richtlinie alternativ auf § 60d oder auf § 44b UrhG berufen, sofern er die Voraussetzungen der jeweiligen Schranke erfüllt[206]. Auch wenn § 60d UrhG die allgemeinen Regelungen des § 44b Abs. 1 UrhG im Hinblick auf den Zweck für die wissenschaftliche Forschung modifiziert, verdrängen sich die Vorschriften somit nicht, sondern bleiben nebeneinander anwendbar.[207] Indem für kommerzielle Nutzungen eine weitere Rechtsgrundlage geschaffen wurde, soll dies der Wirtschaft mehr Rechtssicherheit bei der Innovationsförderung und bei dem weiteren Ausbau der Digitalisierung von Services bieten.[208]

Dagegen wenden sich jedoch ausdrücklich der Bundesverband der Digitalpublisher und Zeitungsverleger (BDZV) in seiner „Wiener Erklärung“[209] wie auch der Medienverband der Freien Presse (MVFP)[210] in einer gemeinsamen Erklärung mit dem BDZV: „Eine Verwertung von Verlagsanboten durch KI-Sprachmodule für die Veröffentlichung konkurrierender Inhalte ist unseres Erachtens nur mit einer Lizenz des Verlages zulässig“[211]. Damit wird die Tür zu den §§ 51 ff. VVG aufgestoßen[212].

[206] BReg-Drs. 19/27426, 95.
[207] BeckOK UrhR/Hagemeier, 38. Ed. 01.02.2023, UrhG § 44b, Rn. 1.
[208] vgl. Erwägungsgrund 18 UAbs. 1 Satz 4 DSM-RL; BT-Drs. 19/27426, 87.
[209] https://www.bdzv.de/service/presse/branchennachrichten/2023/wiener-erklaerung-deutschsprachige-verlegerverbaende-verabschieden-gemeinsamen-forderungskatalog?sword_list%5B0%5D=Lizenz&no_cache=1 (abgerufen am 06.07.2023).
[210] https://www.mvfp.de/nachricht/artikel/tagesspiegel-verlage-fordern-lizenzgebuehren-wegen-chatbot-suchmaschinen (abgerufen am 06.07.2023).
[211] *Steiner* in C't 7/2023, 16–17 (17).
[212] siehe hierzu *Pukas*, GRUR 2023, 614.

3. Stock-Fotografie und KI – LG Hamburg

Die besondere wirtschaftliche Bedeutung des § 44b UrhG wird schlaglichtartig deutlich im Bereich der sog. Stock-Fotografie. Hier werden vorproduzierte Aufnahmen („on stock“) lizenzfrei oder gegen Lizenzzahlungen vertrieben und verkauft. Zur Verdeutlichung sei beispielhaft auf einige Zahlen verwiesen. Getty Images, eine der weltweit führenden Bildagenturen, hält 6.206.547 „Stock Photos & High Res Pictures“ bereit.[213] Ein auf die Stockfotografie spezialisiertes britisches Unternehmen verweist auf das Angebot von „339,800,165 stock photos, 360° panoramic images, vectors and videos“[214].

Am 27.04.2023 reichte ein Stock-Fotograf beim Landgericht Hamburg Klage auf Unterlassung der von ihm behaupteten Urheberrechtsverletzung, gegen den gemeinnützigen Verein LAION e. V. ein.[215] Der Stock-Fotograf möchte Klarheit für die gesamte Branche der Stock-Fotografie erreichen, inwieweit Webcrawler seine Bilder oder die seiner Kollegen analysieren dürfen. Darüber hinaus möchte er auf eine Vergütung der Urheber der Bilder hinwirken, die zum Training großer Machine-Learning-Modelle herangezogen werden. [216]

LAION („Large-scale Artificial Intelligence Open Network“) ist eine deutsche Non-Profit-Gesellschaft, die quelloffene KI-Modelle und Datensätze entwickelt. LAION versteht sich dabei als gemeinnützige Organisation mit Mitgliedern aus der ganzen Welt, deren Ziel es sei, groß angelegte Modelle, Datensätze und zugehörigen Codes für maschinelles Lernen der breiten Öffentlichkeit zugänglich [zu] machen.[217] LAIONs Datenbanken enthalten nach Angaben des Vereins keine Pixeldaten, sondern reine Textdaten, Metadaten und URLs. Laut LAION e. V. seien in den bereitgestellten Datensätzen LAION-400M und LAION-5B keine pixelierten Daten enthalten, lediglich Textdaten, Text Embeddings und URL-Verweise auf Bild-Text-Paare, die im freien Internet verfügbar sind.[218] Bei den Datensätzen handelt es sich danach um einen

[213] https://www.gettyimages.com/photos/holding (abgerufen am 06.07.2023).
[214] https://www.alamy.com/enterprise/ (abgerufen am 06.07.2023).
[215] LG Hamburg, 27.09.2024 - 310 O 227/23 = GRUR 2024, 1710
[216] https://www.profifoto.de/szene/notizen/2023/02/21/laion-droht-kneschke/ (abgerufen am 06.07.2023).
[217] https://laion.ai/about/ (abgerufen am 06.07.2023).
[218] Quelle: LAION e. V.

Katalog mit Indexverweisen auf jeweils 400 Millionen oder im Falle von LAION-5B fünf Milliarden frei zugänglicher Bilder.[219]

Gegenstand des Rechtsstreits[220] war die Klage eines Fotografen gegen das gemeinnützige Forschungsnetzwerk Laion (Large-scale Artificial Intelligence Open Network). Laion stellt eine umfangreiche, öffentlich zugängliche Datenbank zur Verfügung, die rund sechs Milliarden Bild-Text-Paare umfasst. Diese Datenbank dient dem Training von KI-Systemen, insbesondere zur Entwicklung von Bild- und Texterkennungsalgorithmen. In der Datenbank befand sich unter anderem ein Bild des klagenden Fotografen, der gerichtlich die Löschung des Fotos sowie ein Verbot der weiteren Nutzung verlangte. Der Fotograf argumentierte, dass durch die Aufnahme seines Bildes in die Datenbank seine Urheberrechte verletzt worden seien. Insbesondere stellte er in Frage, ob Laion berechtigt war, das Bild herunterzuladen und für den Abgleich mit der dazugehörigen Bildbeschreibung zu verwenden.

Fraglich ist, ob die oben dargestellte Arbeitsweise eines Bilderkennungs-Algorithmus eine Urheberrechtsverletzung zusehen ist. Gerade Medienanbieter und Verlage fühlen sich durch die Arbeitsweise von Bilderkennungs-Algorithmen in Ihren Urheber-rechten verletzt. Die Rechtswicklung der EU geht aber in eine andere Richtung, da die EU die Entwicklung von KI nicht behindern möchte. So wurde mit der Reform der Urheberrechtslinie 2019 hierzu besondere Regelungen aufgenommen. So ist es durch Art. 4 der RL ist Textmining grundsätzlich zulässig, vgl. § 60d UrhG. Art. 4 Abs. 1 der Richtlinie bestimmt, dass die Mitgliedstaaten für zum Zwecke des Text und Data Mining vorgenommene Vervielfältigungen und Entnahmen aus rechtmäßig zugänglichen Werken und sonstigen Schutzgegenständen eine Ausnahme oder Beschränkung vorsehen. Dies betrifft die in Art. 5 Buchst. a und Art. 7 Abs. 1 der RL 96/9/EG, Art. 2 der RL 2001/29/EG, Art. 4 Abs. 1 Buchst. a und b der RL 2009/24/EG sowie Art. 15 Abs. 1 der vorliegenden Richtlinie niedergelegten Rechte. Diese Regelung wurde in § 44b UrhG umgesetzt, und somit gibt es nun im deutschen UrhG gibt es damit nun zwei Schranken-vorschriften für das Text und Data Mining – § 44b im

[219] *Hahn*, Was darf KI? Stockfotograf und KI-Verein streiten um das Copyright in https://www.heise.de/hintergrund/Was-darf-KI-Stockfotograf-und-KI-Verein-streiten-um-das-Copyright-8984836.html (abgerufen am 06.07.2023).

[220] LG Hamburg (Urt. v. 27.09.2024, Az. 310 O 227/23 siehe Anmerkungen Söbbing ITRB 2024, xx

Allgemeinen und den spezielleren § 60d für nicht kommerzielle, wissenschaftliche Zwecke. Somit ist grundsätzlich ein Data Mining rechtlich möglich. Hierzu wird ausgeführt, dass das Text- und Data Mining kann auch für reine, nicht urheberrechtlich geschützte Fakten oder Daten erfolgen, und in diesen Fällen ist nach dem Urheberrecht keine Erlaubnis erforderlich. Es kann auch Fälle des Text und Data Mining geben, in denen keine Vervielfältigungshandlung erfolgt oder die Vervielfältigungen unter die in Artikel 5 Absatz 1 der Richtlinie 2001/29/EG vorgesehene verbindliche Ausnahme für vorübergehende Vervielfältigungshand-lungen fallen, die auch künftig auf Verfahren des Text und Data Mining angewandt werden sollte, die nicht die Anfertigung von Kopien in einem über diese Ausnahme hinausgehenden Umfang einschließen. Dagegen erklärte der Bundesanzeiger der Digitalpublisher und Zeitungsverleger (BDZV) und der Medienverband der freien Presse (MVFP) gemeinsam „Eine Verwertung von Verlagsanboten durch KI-Sprachmodule für die Veröffentlichung konkurrierender Inhalte ist unseren Erachtens nur mit einer Lizenz des Verlages zulässig".

Forscher können sich nunmehr alternativ auf § 60d oder auf § 44b berufen, sofern er die Vorausset-zungen der jeweiligen Schranke erfüllt. Nach § 44b Abs. 2 S.1 UrhG sind Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining Zulässig. Dabei sind Nutzungen nach Absatz 2 Satz 1 nur zulässig, wenn der Rechtsinhaber sich diese nicht vorbehalten hat, vgl. § 44b Abs. 3 S. 1 UrhG. Ein Nutzungsvorbehalt bei online zugänglichen Werken ist nur dann wirksam, wenn er in maschinenlesbarer Form erfolgt, vgl. § 44b Abs. 3 S. 1 UrhG. Was mit einer maschinenlesbaren Form gemeint ist, ist dabei nicht ganz unumstritten. Auf Websites finden Suchmaschinen die Datei „ro-bot.txt" die wesentlichen Informationen über die Website für Suchmaschinen enthält. Es wäre also naheliegend, in dieser Datei dem KI-Webcrawler mitzuteilen, dass der Betreiber Website von seinem Recht nach § 44b Abs. 3 S. 1 UrhG gebraucht macht. Denkbar wäre auch eine Mitteilung im Impressum der jeweiligen Website, wie bereits geschildert, muss die Information nach § 44b Abs. 3 S. 1 UrhG nur in einer maschinenlesbaren Form sein.

Auch wenn § 60d UrhG die allgemeinen Regelungen des § 44b Absatz 1 UrhG im Hinblick auf den Zweck für die wissenschaftliche Forschung modifiziert, verdrängen sich die Vorschriften somit nicht, sondern bleiben nebeneinander anwendbar. Indem

für kommerzielle Nutzungen eine klare Rechts-grundlage geschaffen wurde, soll dies der Wirtschaft mehr Rechtssicherheit bei der Innovations-förderung und bei dem weiteren Ausbau der Digitalisierung von Services bieten.

In erster Instanz hat der Kläger nun vor dem Landgericht Hamburg verloren (Urteil vom 27.09.2024 – 310 O 227/23). Die Urteilsbegründung liegt zwar noch nicht vor, jedoch ist bereits bekannt, dass das Gericht die Nutzung des Bildes durch Laion im Hinblick auf die Text- und Data-Mining-Schranke des § 60d UrhG für gerechtfertigt hält. § 60d UrhG gestattet die Nutzung urheberrechtlich geschützter Werke für wissenschaftliche Zwecke, insbesondere für das sogenannte Text- und Data-Mining (TDM), ohne dass eine Verletzung der Urheberrechte vorliegt. TDM bezeichnet den Prozess, bei dem große Mengen von Daten – oft unstrukturierte Texte oder andere Daten – systematisch analysiert werden, um Muster oder Zusammenhänge zu erkennen und daraus neue Erkenntnisse zu gewinnen.

Im vorliegenden Fall sah das Gericht den Abgleich des Bildes mit der zugehörigen Bildbeschreibung durch Laion als einen solchen wissenschaftlichen Zweck an. Laion hatte das Bild heruntergeladen, um es mit der textlichen Beschreibung abzugleichen und daraus Korrelationen zwischen Bildinhalt und Bildbeschreibung zu ermitteln. Dieser Prozess fiel nach Ansicht des Gerichts unter die Schrankenregelung des § 60d UrhG, da es sich um eine wissenschaftliche Analyse handelte. Dass die Datenbank später für das Training von KI-Systemen verwendet wurde, änderte an dieser Beurteilung nichts. Entscheidend war für das Gericht, dass der ursprüngliche Zweck des Datenabgleichs im wissenschaftlichen Bereich lag und somit die Nutzung als privilegiert angesehen werden konnte.

Die Entscheidung ist insbesondere deshalb von Bedeutung, weil sie den Anwendungsbereich der Schrankenregelung des § 60d UrhG in einem bisher noch wenig geklärten Bereich konkretisiert. Das Gericht hat klargestellt, dass der Abgleich von Bild- und Textdaten im Rahmen wissenschaftlicher Forschung unter den Begriff des TDM fällt, auch wenn die Datensätze später für kommerzielle Zwecke genutzt werden könnten. Diese Auslegung ist von erheblichem Interesse für Forschungseinrichtungen und Unternehmen, die im Bereich der künstlichen Intelligenz tätig sind, da sie

Rechtssicherheit hinsichtlich der Verwendung urheberrechtlich geschützter Werke im Rahmen von KI-Trainingsprozessen schafft.

Dabei warf das Gericht auch in einem obiter dictum die Frage auf, ob ein in „natürlicher Sprache" auf einer Webseite formulierter Nutzungsvorbehalt – wie im vorliegenden Fall durch die Fotoagentur – als maschinenlesbar im Sinne der einschlägigen urheberrechtlichen Bestimmungen anzusehen ist. Diese Frage wurde nicht abschließend beantwortet, jedoch ließ das Gericht erkennen, dass Nutzungsvorbehalte, die in natürlicher Sprache verfasst sind, unter Umständen als maschinenlesbar gelten könnten, sofern moderne KI-Technologien in der Lage sind, diese inhaltlich zu erfassen und zu verarbeiten.

4. Sich daraus ergebende rechtliche Fragestellung

Dies wirft offenkundig die Frage auf, ob die Voraussetzungen der §§ 44b oder 60d UrhG vorliegen und somit eine zulässige urheberrechtliche Nutzung durch den Verein vorliegt. Wie bereits oben ausgeführt, ist eine Nutzung gem. § 44b Abs. 3 Satz 1 UrhG möglich, wenn der Rechtsinhaber sich diese nicht vorbehalten hat und dieser Vorbehalt gem. § 44b Abs. 3 Satz 2 UrhG maschinenlesbar hinterlegt ist. Hierzu finden sich aber keine Hinweise.

LAION e. V. vertritt, soweit veröffentlicht, die Ansicht, ihre Verarbeitung könne sich auf § 60d UrhG, dem Text und Data Mining für Zwecke der wissenschaftlichen Forschung, berufen.[221] Hierzu stellt der Fotograf aber die Gemeinnützigkeit und den Forschungszweck des Vereins infrage.[222] So führt er in seinem Blog dazu aus, Stability AI hätte den Verein finanziell mit einer Spende unterstützt (Angaben des Vereins und Stability AI zufolge „einmalig in geringer Höhe") sowie Rechenkraft zur Verfügung gestellt. Laut notariell beglaubigten Auszügen aus dem Vereinsregister wurde LAION im Februar 2022 offiziell als Verein eingetragen – das Erstellen der Datensätze LAION-400M und LAION-5B fand bereits im Laufe des Jahres 2021 statt. Somit könne – so die Argumentation des Fotografen – der Verein für die Zeit vor der

[221] Quelle: LAION e.V.
[222] https://www.alltageinesfotoproduzenten.de (abgerufen am 06.07.2023).

Vereinseintragung Ausnahmen vom Urheberrechtsgesetz nicht in Anspruch nehmen. Der Fotograf bezweifelt, dass der Verein vor Februar 2022 bereits bestanden habe.[223]

Letztlich dürfte könnte dies aber aus mehreren Gründen irrelevant sein. Denn zum einen sollen Public Private Partnerships sich gerade – unabhängig von § 60d UrhG – auf einen bevorzugten Zugang berufen können[224] (dazu b). Zum anderen stellt sich aber schon grundsätzlich die Frage, ob durch den Einsatz eines Webcrawlers Urheberrechte berührt sein können (dazu a).

a) Urheberrechtliche relevante Handlung

Übersehen wird in der allgemeinen Diskussion häufig, dass beim Text und Data Mining nur die schlichten Daten, nicht aber der geistige Inhalt der analysierten Werke genutzt werden[225]. Bei einer generativen KI besteht der (revolutionäre) Unterschied zu einem Chatbot bisheriger Art gerade darin, dass dieser nicht mit vorgefertigten Antworten operiert, sondern durch das Deep Learning in die Lage versetzt wurde, eine eigenständige, jeweils neue Antwort auf eine Anfrage zu generieren. Der denklogische Ansatz, durch die Aufforderung an einen Bildgenerator, ein Bild in der Stilrichtung eines bestimmten Künstlers zu verfassen, vervielfältige das Programm bei ihm vorhandene Daten schlicht, ist bereits falsch. Vielmehr handelt „erschafft" das Programm jeweils eigenständig ein neues, eigenes Werk. Das vorher erfolgende Text und Data Mining ist nichts anderes als ein Lernprozess und Inspiration seitens eines Künstlers vor der Schaffung seines Werks. Sollte das sich aus diesem Lern- und Schaffensprozess ergebende Werk eine zu große Nähe zu einem der Originale das Recht des Urhebers aufweisen, ergäbe sich ein urheberrechtlicher Verstoß nach §§ 15, 16 UrhG. So ist bei der Beurteilung, ob „nur" eine Bearbeitung i. S. d. § 23 UrhG vorliegt, durch Vergleich der sich gegenüberstehenden Werke zu ermitteln, ob und gegebenenfalls in welchem Umfang eigenschöpferische Züge des älteren Werks übernommen worden sind. Maßgebend für die Entscheidung ist letztlich ein Vergleich des jeweiligen Gesamteindrucks der Gestaltungen, in dessen Rahmen sämtliche

[223] https://www.alltageinesfotoproduzenten.de (abgerufen am 06.07.2023).
[224] *Dreier*/*Schulze*/*Dreier*, 7. Aufl. 2022, UrhG § 44b, Rn. 7.
[225] Darauf hat schon *Schack*, GRUR 2021, 904, 907 zutreffend hingewiesen; in diese Richtung auch *Raue*/*Hegemann*, MAH UrhR, § 3 Urheberrechtliche Schranken, Rn. 40.

übernommenen schöpferischen Züge in einer Gesamtschau zu berücksichtigen sind[226]. Die abgestufte Prüfungsreihenfolge[227] des BGH im Rahmen des § 23 UrhG illustriert auch für den Bereich der generativen KI sehr anschaulich, worum es in der Sache geht: „Zunächst ist im Einzelnen festzustellen, welche objektiven Merkmale die schöpferische Eigentümlichkeit des benutzten Werks bestimmen. Sodann ist durch Vergleich der einander gegenüberstehenden Gestaltungen zu ermitteln, ob und gegebenenfalls in welchem Umfang in der neuen Gestaltung eigenschöpferische Züge des älteren Werks übernommen worden sind. Maßgebend für die Entscheidung ist letztlich ein Vergleich des jeweiligen Gesamteindrucks der Gestaltungen, in dessen Rahmen sämtliche übernommenen schöpferischen Züge in einer Gesamtschau zu berücksichtigen sind. Stimmt danach der jeweilige Gesamteindruck überein, handelt es sich bei der neuen Gestaltung um eine Vervielfältigung des älteren Werks. Es ist dann – soweit erforderlich – weiter zu prüfen, ob die neue Gestaltung gleichwohl so wesentliche Veränderungen aufweist, dass sie nicht als reine Vervielfältigung, sondern als (unfreie) Bearbeitung oder andere Umgestaltung des benutzten Werks anzusehen ist. Weicht der jeweilige Gesamteindruck voneinander ab, liegt jedenfalls weder eine Vervielfältigung noch eine Bearbeitung, sondern möglicherweise eine freie Benutzung vor. Um eine freie Benutzung im Sinne von § 24 Abs. 1 UrhG a. F. handelt es sich, wenn ein selbstständiges Werk geschaffen wurde und das ältere Werk als Grundlage für die Schöpfung des neuen Werks diente“.[228] Diese zutreffenden Gedanken der sog. *Porsche*-Entscheidung[229] zeigen deutlich auf, dass jedenfalls bei generativen KI nicht das Text und Data Mining problematisch ist, sondern in Einzelfällen das gefundene Ergebnis. In diesen Fällen stehen dem Urheber aber genügende rechtliche Mittel zur Verfügung.

[226] BGH GRUR 2004, 855 – Hundefigur.
[227] vgl. BeckOK UrhR/Ahlberg/Lauber-Rönsberg, 38. Ed. 01.05.2023, UrhG § 23, Rn. 10.
[228] BGH ZUM 2022, 547, 553.
[229] BGH ZUM 2022, 547, 553.

b) § 44b UrhG Text und Data Mining

Wie schon oben ausgeführt, soll nach dem Willen des Verordnungsgebers die Arbeit mit und durch künstliche Intelligenz im Bereich der Europäischen Union nicht behindert, sondern gefördert werden. Deshalb sollen nach Umsetzung in § 44b Abs. 2 Satz 1 UrhG Vervielfältigungen von rechtmäßig zugänglichen Werken für das Text und Data Mining zulässig sein. Dabei sind Nutzungen nach Abs. 2 Satz 1 nur zulässig, wenn der Rechtsinhaber sich diese nicht vorbehalten hat, vgl. § 44b Abs. 3 Satz 1 UrhG. Ein Nutzungsvorbehalt bei online zugänglichen Werken ist nur dann wirksam, wenn er in maschinenlesbarer Form erfolgt, vgl. § 44b Abs. 3 Satz 1 UrhG. Was im Einzelnen mit einer maschinenlesbaren Form gemeint ist, ist dabei nicht ganz unumstritten. Eine eindeutige und einfache Möglichkeit ist jedenfalls der Hinweis mittels der sog. „robot.txt"-Information. Es handelt sich dabei um eine Textdatei, in der man hinterlegen kann, welche Verzeichnisse von Suchmaschinen gelesen werden dürfen[230]. Mit dieser im Hauptverzeichnis hinterlegten Datei kann der Website-Betreiber gegenüber dem Webcrawler mitteilen, dass er von seinem Recht nach § 44b Abs. 3 Satz 1 UrhG gebraucht macht.[231]

Denkbar wäre auch eine Mitteilung im Impressum der jeweiligen Website (oder den dort hinterlegten AGB). Wie bereits ausgeführt, muss die Information nach § 44b Abs. 3 Satz 1 UrhG nur in einer maschinenlesbaren Form erfolgt sein[232].

Hier zeigt sich, dass dem Urheber ein einfaches Instrument an die Hand gegeben wurde, um sein Werk schon im Ansatz zu schützen. Die entsprechende Programmierung kann einen Zugriff eines Webcrawlers leicht verhindern. Mit diesem Opt-Out-Modell kann der Urheber sicherstellen, dass er seine Werke nicht einer generativen KI zur Verfügung stellt.

[230] https://developers.google.com/search/docs/crawling-indexing/robots/intro?hl=de (abgerufen am 06.07.2023).
[231] *Steiner* in c't 7/2023, 16-17 (17).
[232] so auch *Pukas*, GRUR 2023, 614, 615.

c) Text und Data Mining für Zwecke der wiss. Forschung (§ 60d UrhG)

Damit kann dahinstehen, ob sich eine Organisation wie die LAION e. V. auf § 60d UrhG mit den erweiterten Möglichkeiten einer Speichermöglichkeit der erlangten Daten berufen könnte. So stellt sich der Bundestag berechtigterweise die Frage, ob eine wissenschaftliche Forschung auch noch mit nicht kommerziellen Zwecken verknüpft werden kann, wenn ein Prototyp eines Modells oder Algorithmus für die Finalisierung und Einbettung in Anwendungssoftware in einem ausgegründeten Spin-off finalisiert oder an gewerbliche Entwickler veräußert wird, also ein Citizen-Science-Ansatz verfolgt wird.[233]

Exemplarisch zeigt sich dies an Open AI: Gegründet 2015 als Nonprofit Group, um künstliche Intelligenz zu entwickeln „in the way that is most likely to benefit humanity as a whole", war Open AI in der Folge in einer „Partnerschaft" mit Microsoft verbunden (mit einer Investition von einer Milliarde US-Dollar Ende 2019) und ist seit 2020 nach eigenen Angaben als „a 'capped-profit' company"[234].

d) Resümee

Wie so oft stehen hier widerstreitende Interessen gegenüber: auf der einen Seite die Interessen der Urheber, z. B. die Stock-Fotografen, und auf der anderen Seite die Entwickler von KI. So verständlich die Sorgen der Urheber auf den ersten Blick sein mögen, zeigen die obigen Ausführungen jedoch auf, dass Webcrawler schon nicht den geistigen Inhalt „schürfen". Denn um eine freie Benutzung im Sinne von § 24 Abs. 1 UrhG a. F. handelt es sich, wenn ein selbstständiges Werk geschaffen wurde und das ältere Werk als Grundlage für die Schöpfung des neuen Werks diente. Ob dies immer der Fall ist, wenn Webcrawler Daten sammeln, ist mehr als fraglich.

Die neue Regelung in § 44b UrhG zeigt aber Möglichkeiten auf, wie man verhindern kann, dass Webcrawler die eigenen Werke analysieren, vgl. § 44b Abs. 3 Satz 1 UrhG. Fraglich ist, ob dies die Entwicklung von KI bremst oder verhindert und einen Wettbewerbsnachteil für Deutschland und die EU darstellt.

Die Regelung in § 60d Abs. 1 UrhG sieht vor, dass Vervielfältigungen für Text und Data Mining (§ 44b Abs. 1 und 2 Satz 1 UrhG) zum Zwecke der wissenschaftlichen

[233] Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung (18. Ausschuss) gemäß § 56a der Geschäftsordnung, Drucksache 20/5149, 224 (Vorabfassung vom 09.01.2023).

[234] www.openai.com (abgerufen am 06.07.2023); www.businessinsider.com (abgerufen am 06.07.2023)

Forschung nach Maßgabe der nachfolgenden Bestimmungen zulässig sind. Dies lässt aber die Frage offen, was passiert, wenn die Ergebnisse wissenschaftlicher Forschung kommerziell verwertet werden.

Zusammenfassend lässt sich festhalten, dass mit den oben dargestellten Fragen und möglichen Antworten nichts weniger als die Zukunft der künstlichen Intelligenz in Deutschland und in der EU einhergeht.

C. Generative KI[235]

Einer der großen rechtlichen Fragen dieser Zeit ist die Frage, ob der Output von Generativen Chatbots wie ChatGPT von OpenAI, Gemini von Google oder andere einen rechtlichen Schutz genießt. Hier spielt vor allem die Frage, ob der Output von Generativen Chatbots urheberrechtlich geschützt ist und wenn das nicht, ob der Output ggf. ein Geschäftsgeheimnis darstellen könnte und somit einen rechtlichen Schutz genießen könnte. Immerhin setzen eine Reihe von Unternehmen Generative Chatbots für tägliche Arbeit ein und solche Technologien finden immer mehr Anklang in alltäglichen Arbeiten.

I. Einleitung

ChatGPT und Gemini zählt zur Gruppe der Generative vortrainierte Transformer (englisch Generative pre-trained transformers, GPT) und ist somit ein Large Language Models (Kurzform „LLM“).[236] Solche LLMs zählen sind bedeutende Frameworks für generative künstliche Intelligenz (GenAI).[237]

ChatGPT ist, anders als Internetsuchmaschen wie Google, eine recht neue Technologie und wurde vom US-amerikanischen Unternehmen OpenAI mit Sitz in San Franzisco entwickelt. Nachdem OpenAI die Software-Version GPT-3 am 30. November 2022 online gestellt wurde, meldeten sich innerhalb von fünf Tagen weltweit eine Million Nutzer an.[238] Im Januar 2023 erreichte ChatGPT über 100 Millionen Nutzer.

Die aktuelle Version 4.0 von GPT schien am 14. März 2023 und verfügt über erhebliche Erweiterung ggü. der Version 3.5.[239] So ermöglicht die kostenpflichtige Version GPT-4 eine Bildeingabe und die Analyse und Beschreibung von Skizzen und Fotos. Es ist möglich, abfotografierte Aufgaben aus Büchern lösen zu lassen. Wissenschaftliche Arbeiten können hochgeladen werden, um eine Zusammenfassung generieren

---

[235] *Söbbing* Möglicher Rechtsschutz von KI-Output nach dem UrhG oder GeschGehG – Genießt der Output von Generativen Chatbots wie ChatGPT einen rechtlichen Schutz? ITRB 2024, 184 - 188

[236] Generative AI: a game-changer society needs to be ready for. In: World Economic Forum.

[237] Luhui Hu: Generative AI and Future. In: Medium. 15. November 2022.

[238] Krystal Hu, Krystal Hu: ChatGPT sets record for fastest-growing user base - analyst note. In: Reuters. 2. Februar 2023 (reuters.com [abgerufen am 12. Juli 2023]).

[239] Silke Hahn: OpenAI stellt GPT-4 vor: Sprachmodell versteht jetzt auch Bilder. In: heise online (heise.de). 14. März 2023, abgerufen am 15. März 2023.

zu lassen. Examensprüfungen konnte GPT-4 bei Tests in den USA mit Auszeichnung erledigen. Komplizierte Steuerfragen werden beantwortet.[240]

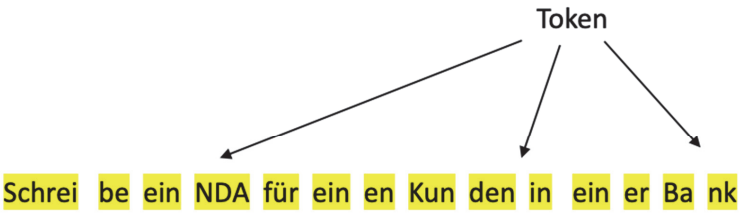
II. Arbeitsweise von generativer KI in Textform

Ein LLM (Large Language Model) wie ChatGPT arbeitet ähnlich wie ein riesiges, sehr komplexes Vorhersagesystem, das darauf trainiert ist, Text basierend auf den Eingaben, die es erhält, zu generieren. Um die Bedeutung eines Wortes zu erfassen, beobachten LLMs es zunächst im Kontext anhand riesiger Trainingsdatensätze, wobei sie auf nahe gelegene Wörter achten. Diese Datensätze basieren auf der Zusammenstellung von im Internet veröffentlichten Texten, wobei neue LLMs mit Milliarden von Wörtern trainiert werden

Beispiel:

Prompt (Eingabe): „Schreibe ein NDA für ein Kunden in einer Bank“

Schritt 1:



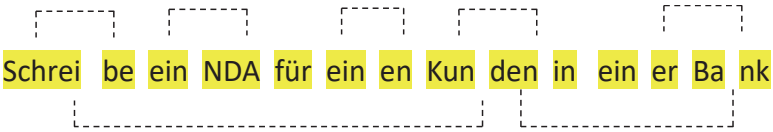
Das unterteilt den Satz in Token

Das LLM unterteilt den Satz in Token.[241] Ein Token kann aus einem Wort, eine Abkürzung eine Silbe, einem Satzzeichenbestehen. Ein Token ist wie ein Teil aus einem Puzzle zu verstehen.

Schritt 2:

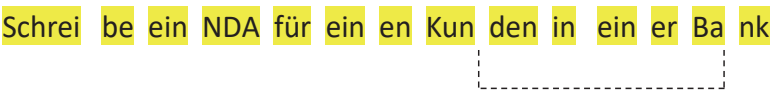
[240] Laurin Meyer: ChatGPT erreicht die nächste Entwicklungsstufe. Die Welt, 17. März 2023. Seite 10.

[241] Ein "Token" ist die grundlegende Einheit der Verarbeitung, die das Modell verwendet, um Text zu verstehen und zu generieren. Siehe hierzu das Original GPT-Papier: "Improving Language Understanding by Generative Pre-Training" von *Alec Radford et al.* Dieses Papier von OpenAI stellt das Konzept und die Implementierung des ursprünglichen GPT-Modells vor, einschließlich einer Diskussion über die Tokenisierung und wie sie die Fähigkeit des Modells beeinflusst, Sprache zu verstehen und zu generieren.



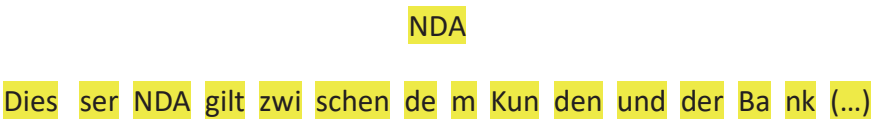
Das LLM analysiert die Token in einem Satz und deren Beziehung zueinander. Die Beziehung zwischen Kunden und Bank weist darauf hin, dass es sich nicht um eine Bank zum Sitzen handelt:

Schritt 3:



Die Antwort auf den Prompt wird durch die häufige Wahrscheinlich von Token zueinander im Internet ein neuer Text erstellt.

Schritt 4:



Ein LLM hat selbst kein Faktenwissen, sondern geht von der Häufigkeit der Information im Internet aus. Daraus können Fehler bzw. Halluzinationen[242] entstehen, so z.B. das „Bettina Wulff“ vor Ihrer Ehe mit dem Bundespräsidenten Christian Wulff “im Rotlichtmilieu gearbeitet“ hätte,[243] was aber nicht der Richtigkeit entspricht oder dass es die Stadt „Bielefeld nicht geben würde“ was ebenfalls falsch ist.[244] Beide Gerüchte haben oder halten sich schon seit längerer Zeit im Internet und eben zu dieser Halluzinationen führen. LLM‘s sind nur so gut, wie seine Trainingsdaten und wie ihr Trainingstool es zu lässt. Es sind nur Wahrscheinlichkeiten.

[242] Halluzinationen bei großen Sprachmodellen (LLMs) wie GPT (Generative Pre-trained Transformer) beziehen sich auf Fälle, in denen das Modell inkorrekte, verfälschte oder vollkommen erfundene Informationen generiert. Diese Phänomene können durch verschiedene Faktoren verursacht werden. "Reducing Hallucination in Language Models" von *Yoav Goldberg,* veröffentlicht auf arXiv.org.

[243] Im September 2012 reichte Bettina Wulff beim Landgericht Hamburg Klagen gegen Günther Jauch und auch gegen Google ein, nachdem in den Monaten zuvor bereits 34 deutsche und ausländische Blogger und Medien Unterlassungserklärungen abgegeben hatten. Damit wehrt sie sich gegen seit 2006 kursierende Gerüchte, sie habe – vor ihrer Ehe mit Christian Wulff – im Rotlichtmilieu gearbeitet, *Hans Leyendecker, Ralf Wiegand*: Bettina Wulff wehrt sich gegen Verleumdungen. In: Süddeutsche Zeitung. 7. September 2012.

[244] Die Bielefeld-Verschwörung ist eine satirische Verschwörungstheorie, die behauptet, die Stadt Bielefeld gebe es nicht, ihre Existenz werde lediglich überzeugend vorgetäuscht. Diese Theorie erschien erstmals 1994 im deutschsprachigen Usenet, kursiert seither als Dauerwitz im Internet und wurde so Teil der Internetfolklore, die zur Netzkultur gehört. *Katharina Miklis:* Aus Bielefeld? Das gibt’s doch nicht! In: der Freitag. 7. April 2010. (Miklis, 2010)

III. Genießt der Output von LLM's urheberrechtlichen Schutz?

Ein Werk genießt urheberrechtlichen Schutz, wenn es sich um eine persönliche geistige Schöpfung handelt, vgl. § 2 Abs. 2 UrhG.

1. Output als Menschliches Werk?

Der zentrale Anknüpfungspunkt für urheberrechtlichen Schutz ist die persönliche Schöpfung. Gemeint ist damit die intellektuelle Leistung eines Menschen. Teleologisch leitet sich dieses Erfordernis aus dem zentralen Schutzgedanken des monistischen Urheberrechts ab. Die Person des Urhebers steht ganz bewusst im Fokus.[245] Allerdings kann der Mensch sich bei seinem schöpferischen Akt Hilfsmitteln bedienen, angefangen von Stift und Pinsel bis hin zur künstlichen Intelligenz.[246] Ausgangspunkt ist dabei technologische Neutralität und Agnostik des Urheberrechts;[247] mit Blick auf die Werknutzung[248] – Drucker und Plotter.[249] Um ein urheberrechtliches Werk i.S.v. § 2 Abs. 2 UrhG zu erschaffen, darf der Urheber Hilfsmittel einsetzen. Die Art des Hilfsmittels ist dabei in wesentlichen unbeachtlich.[250] Das Hilfsmittel darf dabei dem Handelnden nicht den schöpferischen Akt abnehmen.[251] Der fortschreitende Einsatz selbständig lernender Algorithmen erschwert hier in der Praxis bisweilen die rechtliche Einordnung.[252] Dies insbesondere auch deshalb, weil die technischen Abläufe mitunter sehr komplex und wenig transparent sind.[253]

Jedoch bei der Verwendung von Generativen Chatbots wie ChatGPT und der unter Nr. II dargestellten Arbeitsweise liegt der schöpferische Akt eindeutig bei den Generativen Chatbots. Der Handelnde vergibt durch Eingabe eines Promps lediglich eine Aufgabe, das LLM unterteilt den Satz in Token und weist auf bestimmte zusammenhänge hin. Die Antwort auf den Prompt wird durch die häufige Wahrscheinlich von Token zueinander im Internet ein neuer Text erstellt. (siehe Nr. II.). Hierbei liegt der

[245] vgl. Begr. BT-Drs. IV/270, 37
[246] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 47.
[247] Begr. BT-Drs. IV/270, 37.
[248] BVerfG ZUM 2010, 874 Rn. 64.
[249] BGH ZUM 2002, 218, 219 – Scanner.
[250] Wandtke/Bullinger/Bullinger Rn. 16a; Schmoll/Graf Ballestrem/Hellenbrand/Soppe GRUR 2015, 1041 (1042)).
[251] Schricker/Loewenheim/Loewenheim/Leistner Rn. 40
[252] Schricker/Loewenheim/Loewenheim/Leistner Rn. 41; vgl. hierzu auch Olbrich/Bongers/Pampel GRUR 2022, 870 (872 f.)).
[253] Käde, Kreative Maschinen und Urheberrecht, 2021, S. 183

schöpferische Akt bei der Maschine, da nur diese den Output durch die häufige Wahrscheinlich von Token generiert. Der schöpferische Akt muss aber beim Menschen liegen, eine Maschinenschöpfung ist nur dann ein urheberrechtsschutzfähig, wenn die Gestaltung des Erzeugnisses noch auf einen geistigen Schöpfungsakt zurückgeführt werden kann, wenn also die Maschine nur Hilfs- bzw. Ausführungsmittel ist.[254] Hierzu wird zu Recht vertreten, dass ein rein computer-generierten Ergebnissen de lege lata mangels einer geistigen Schöpfung eines Menschen keinen Werkcharakter zubilligen können.[255] Dieser Aspekt wird z.B. in britischen Urheberecht und dort Sec. 178 CDPA[256] oder im Sec. 21 lit. (f) CRRA[257] des irischen Urheberrechts anders gesehen.[258] Denkbar, wäre in diesem Zusammenhang über weitere Auslegung der persönlichen Schöpfung zu denken, die aber nicht gegenwärtig nicht ernsthaft diskutiert wird. Grundsätzlich sollte man aber darüber nachdenken, ob bei KI generierten Ergebnissen, ob die KI als Hilfsmittel eines menschlichen Urhebers zum Einsatz kommt oder ein davon abgehobener, autonomer Erstellungsprozess gegeben ist.[259]

2. Erstellung komplexer Prompts

Zuweilen hört man in der Praxis die Argumentation, dass ein komplexer Prompt doch wesentlich für den Output des kreativen Prozesses von Generativen Chatbots wie ChatGPT sei. Grundsätzlich gilt auch die Abgrenzung, ob das Werk von der KI erschaffen worden ist oder das Werk vom Menschen mittels KI erschaffen wurden".[260] Werke im Sinne des § 2 UrhG sind nur letztere.[261] Denn es besteht die Handlung des Menschen allein darin, bestimmte Kategorien durch Stichworte und Stimmungen vorzugeben und dies reicht im Regelfall nicht aus, um der handelnden Person tatsächlich eine hinreichende Kontrolle über das konkrete Ergebnis zuzuschreiben. Insoweit bleibt der Handelnde nur Initiator eines weitgehend zufälligen Prozesses.[262] Denn auch die Erstellung eines komplexen Prompts dient nur dazu, dass das LLM den

[254] BeckOK UrhR/Ahlberg, 32. Ed. 15.9.2021, UrhG § 2 Rn. 55
[255] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 57.
[256] Britisches Urheberrecht: Designs and Patents Act 1988
[257] Copyright and Related Rights Act 2000
[258] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 57.
[259] vgl. Spindler FS Schack 2022, S. 340 (343); Obergfell FS Windbichler, 2020, S. 1397 (1403 f.)
[260] Olbrich/Bongers/Pampel GRUR 2022, 870
[261] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 57.
[262] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 57.

schöpferischen Akt übernimmt und nicht der Mensch. Zwar können verschiedene Handlungen so zusammenwirken, dass einzelne menschliche Handlungen, die für sich genommen das Endergebnis nicht hinreichend bestimmen, im Zusammenwirken mit anderen Handlungen ausreichend sein können,[263] aber der Prompt hat für sich allein so wenig mit dem schöpferischen Akt zu tun, dass eine Maßgeblichkeit für das spätere Werk nicht vorliegt, denn der Schöpferische Akt muss eine über die bloße Auswahl von KI-generierten Gestaltungen hinausgehende Leistung sein, um ein hinreichendes Maß einer menschlichen Leistung zu erreichen.[264]

In der Literatur wird zu Recht vertreten, dass Tools wie etwa ChatGPT für Texte, Dall-E 2, Midjourney für Bilder oder beatoven für musikalische Gestaltungen, die dem Endnutzer zur Verfügung stehen, man in aller Regel eine Schutzfähigkeit verneinen müssen.[265]

3. Urheberrechtschutz für den Prompts

Davon unabhängig ist natürlich die Frage zu sehen, ob der Promp nicht allein schon einen Urheberrechtlichen Schutz nach § 2 Abs. 2 UrhG zugestehen werden muss. Neben der persönlichen Schöpfung eines Menschen ist ferner „geistige" Leistung zu fordern.[266] Näher umschrieben wird dieses Tatbestandsmerkmal hingegen nicht, es bleibt abstrakt.[267] Gemeinhin wird es weit ausgelegt.[268] In der Literatur wird der geistige Gehalt des Schaffensprozesses als ein „Gedanken- oder Gefühlsinhalt" beschrieben, „der auf den Leser, Hörer oder Betrachter unterhaltend, belehrend, veranschaulichend, erbauend oder sonst wie anregend wirkt.[269]

Im Ergebnis ist es stark Einzelfall abhängig, ob ein Prompt allein schon einen Urheberrechtlichen Schutz nach § 2 Abs. 2 UrhG genießt. Wahrscheinlich hätte diese

[263] Ehinger/Grünberg K&R 2019, 232 (236); Grätz, Künstliche Intelligenz im Urheberrecht, 2021, S. 101; auch auf ein Zusammenwirken abstellend, bei dem das KI-System aufgrund der menschlich-gestalterischen Handlung ein konkretes Vorgehen erwarten lässt Specht-Riemenschneider FS Taeger, S. 711 (717 f.)).

[264] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 57.

[265] v. Welser GRUR-Prax 2023, 2023, 57 (58)); Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 59.

[266] Dreier/Schulze/Schulze Rn. 12; Schricker/Loewenheim/Loewenheim/Leistner Rn. 45

[267] BeckOK UrhR/Rauer/Bibi UrhG § 2 Rn. 61.

[268] vgl. Schricker/Loewenheim/Loewenheim/Leistner Rn. 46

[269] so Dreier/Schulze/Schulze Rn. 12; ähnlich auf eine die Sinne anregende Wirkung abstellend Erdmann FS v. Gamm, 1990, 389 (399 f.)

Frage kaum Bedeutung für die Praxis, da es ja immer um die Beantwortung des Prompts geht.

4. Auswahl von Antworten

Eine weitere Frage ist, dass wenn der LLM lediglich Vorschläge macht und der Handelnde entscheiden darf, welches Werk tatsächlich entsteht, nicht eine solche Mitwirken am Output entsteht, dass der schöpferische Akt beim Menschen liegt.[270] Die Gestaltung des Erzeugnisses könnte auf einen geistigen Schöpfungsakt zurückgeführt werden und die Maschine nur Hilfs- bzw. Ausführungsmittel ist.[271]

Bejaht man im Einzelfall die hinreichende Kontrolle des Menschen, wird es entscheidend sein zu überprüfen, inwieweit sich die restlichen Voraussetzungen des Werkbegriffs, in den von der menschlichen Leistung gesteuerten Elementen bejahen lassen.[272] Insbesondere die Originalität muss sich in diesen Gestaltungselementen hinreichend widerspiegeln.[273] Entscheidend ist hierbei aber nicht die Frage nach der Kontrolle sondern nach dem schöpferischen Akt und diese liegt auch bei der Kontrolle über das herzustellenden Werk immer noch bei dem LLM.[274]

IV. Ist der Output von LLM‘s ein Geschäftsgeheimnis?

Die Frage, ob der Output von Large Language Models (LLMs) wie GPT-3 oder GPT-4 als Geschäftsgeheimnis nach § 2 des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Deutschland angesehen werden kann, hängt von mehreren Faktoren ab.

---

[270] 10. Sinfonie vor seinem Tod 1827 in Wien nicht mehr vollenden können und nur einige Skizzen und Notizen hinterlassen. Auf deren Grundlage hatte ein Experten-Team, zu dem Musikwissenschaftler und Programmierer gehörten, eine Künstliche Intelligenz (KI) entwickelt, um die Leerstellen zu füllen. https://www.zeit.de/news/2021-10/09/von-ki-vollendete-10-sinfonie-von-beethoven-uraufgefuehrt?utm_referrer=https%3A%2F%2Fwww.google.com%2F

[271] BeckOK UrhR/Ahlberg, 32. Ed. 15.9.2021, UrhG § 2 Rn. 55

[272] Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2 Rn. 60.

[273] Kuschel/Asmussen/Golla/Hacker, Intelligente Systeme – Intelligentes Recht, 2021, S. 227 ff.

[274] vgl. zur richtigerweise abzulehnenden Frage, ob ein „KI-Werk“ aufgrund der möglicherweise schöpferischen Auswahlleistung von Trainingsdaten auch dem Schutz eines Datenbankwerks nach § 4 Abs. 2 UrhG unterliegt Leistner FS Dreier 2022, 87 (90 f.)).

1. Voraussetzung § 2 GeschGehG

Laut § 2 GeschGehG ist ein Geschäftsgeheimnis definiert als eine Information,

- die nicht allgemein bekannt oder ohne weiteres zugänglich ist und daher von wirtschaftlichem Wert ist,
- Gegenstand von den Umständen entsprechenden Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist, und
- bei der ein berechtigtes Interesse an der Geheimhaltung besteht.

Um zu beurteilen, ob der Output von LLMs unter diese Definition fällt, müssen folgende Aspekte berücksichtigt werden:

a) Wirtschaftlicher Wert, vgl. § 2 Abs. 1 lit. a GeschGehG

Der Output eines LLM könnte für ein Unternehmen wirtschaftlichen Wert haben, insbesondere wenn er spezifische, maßgeschneiderte Informationen oder Analysen generiert, die für die Geschäftsstrategie oder -operationen des Unternehmens von Nutzen sind. Das wirtschaftliche bzw. kommerzielle Interesse wird vom EU-Gesetzgeber nicht definiert, aber anhand von Beispielen in Erwägungsgrund 14 RL (EU) 2016/943 erläutert.[275] Dort heißt es: „Eine solche Definition sollte daher so beschaffen sein, dass sie Know-how, Geschäftsinformationen und technologische Informationen abdeckt […]. Eindeutig erfasst sind geheime Informationen, die für den Fall eines Verkaufs oder der Lizenzierung positive Erträge erwarten lassen.[276]

b) Geheimhaltungsmaßnahmen, vgl. § 2 Abs. 1 lit. b GeschGehG

Es muss nachgewiesen werden, dass das Unternehmen angemessene Maßnahmen ergriffen hat, um den Output des LLM geheim zu halten. Dies könnte den Einsatz von Verschlüsselung, Zugriffskontrollen oder anderen Sicherheitsmaßnahmen umfassen. Das GeschGehG gibt mit diesem Tatbestandsmerkmal zu erkennen, dass nur derjenige den Schutz der Rechtsordnung genießt, der die geheime Information aktiv schützt.[277] Allerdings gebietet es der Vertrauensschutz und das Verbot unzulässiger unechter Rückwirkung von Gesetzen, das Ergreifen angemessener

[275] Erwägungsgrund 14 RL (EU) 2016/943.
[276] BeckOK GeschGehG/Hiéramente GeschGehG § 2 Rn. 16.
[277] OLG Schleswig GRUR-RS 2022, 9007, Rn. 51 mwN.

Geheimhaltungsmaßnahmen erst ab dem Zeitpunkt des Inkrafttretens des GeschGehG zu verlangen.[278] Die Geheimhaltungsmaßnahmen müssen somit seit dem 26.4.2019 bis heute ununterbrochen vorliegen.[279] Was darunter konkret zu verstehen ist, ist allerdings auch nach mehr als drei Jahren seit Inkrafttreten des Gesetzes noch nicht abschließend bzw. „noch immer wenig geklärt".[280] [281]

c) Berechtigtes Interesse an der Geheimhaltung, vgl. § 2 Abs. 1 lit. c GeschGehG

Das Unternehmen muss ein berechtigtes Interesse daran haben, die Informationen geheim zu halten. Dies könnte der Fall sein, wenn die Veröffentlichung des Outputs die Wettbewerbsposition des Unternehmens beeinträchtigen könnte. Das berechtigte Interesse an der Geheimhaltung dient primär der Klarstellung und erlaubt eine Abgrenzung zu reinen Bagatellfällen, bei denen ein Verstoß nicht die (strafrechtlichen) Sanktionen des GeschGehG nach sich ziehen soll.[282] Da die Offenlegung eines Geschäftsgeheimnisses im deutschen Recht nach § 23 in vielen Fällen strafbewehrt ist, ist das Merkmal des „berechtigten Interesses" auch als Korrektiv zu verstehen, welches den Gerichten eine eigenständige Einstufung als Geschäftsgeheimnis und eine Willkürkontrolle erlaubt.[283] [284]

2. Zusammenfassend mit Bezug zum GeschGehG

Nach der Intention des Gesetzgebers soll der nunmehr verwendete Terminus „Geschäftsgeheimnis" sowohl kaufmännisches als auch technisches Wissen erfassen und damit das Begriffspaar „Betriebs- und Geschäftsgeheimnis" ersetzen.[285] Es ist jedoch zu beachten, dass der Output eines LLM oft auf öffentlich zugänglichen Daten basiert und in vielen Fällen generische Antworten generiert, die möglicherweise nicht als einzigartig oder nicht ohne weiteres zugänglich angesehen werden. In solchen Fällen könnte es schwierig sein, den Output als Geschäftsgeheimnis zu klassifizieren.

---

[278] OLG Düsseldorf GRUR-RS 2021, 17483

[279] auch OLG Stuttgart GRUR-RS 2020, 35613

[280] OLG Schleswig GRUR-RS 2022, 9007, Rn. 52

[281] BeckOK GeschGehG/Hiéramente GeschGehG § 2 Rn. 16.

[282] vgl. auch OLG Schleswig GRUR-RS 2022, 9007, Rn. 91; krit. im Hinblick auf die Fortschreibung der alten Rechtsprechung Köhler/Bornkamm/Feddersen/Alexander Rn. 75 f

[283] vgl. auch OLG Schleswig GRUR-RS 2022, 9007, Rn. 91; krit. im Hinblick auf die Fortschreibung der alten Rechtsprechung Köhler/Bornkamm/Feddersen/Alexander Rn. 75 f

[284] BeckOK GeschGehG/Hiéramente GeschGehG § 2 Rn. 71..

[285] BeckOK GeschGehG/Hiéramente GeschGehG § 2 Rn. 1, 1.1

Zusätzlich könnte die Tatsache, dass der Output reproduzierbar ist – d.h., dass andere mit Zugang zum gleichen oder einem ähnlichen LLM ähnliche Outputs generieren könnten – gegen die Einstufung als Geschäftsgeheimnis sprechen. Letztendlich würde die Einstufung des Outputs von LLMs als Geschäftsgeheimnis von den spezifischen Umständen des Einzelfalls abhängen, einschließlich der Art des Outputs, wie er verwendet wird, und den getroffenen Schutzmaßnahmen.

IV. Resümee

Im Ergebnis lässt sich die Tendenz ableiten, dass der Output von LLM's i.d.R. keinen Urheberrechtlichen noch einen Schutz nach dem GeschGehG vorsieht.

D. Halluzination

Es kann vorkommen, dass KI-Systeme sogenannte ‚Halluzinationen' erzeugen, was rechtliche Fragestellungen aufwirft und bereits Gegenstand einer Entscheidung des AG Köln[286] gewesen ist.

I. Definition

Im Bereich der Künstlichen Intelligenz (KI) ist eine Halluzination (alternativ auch Konfabulation genannt) ein überzeugend formuliertes Resultat einer KI, das nicht durch Trainingsdaten gerechtfertigt zu sein scheint und objektiv falsch sein kann.[287] Der Leiter von Google Search, Prabhakar Raghavan, beschrieb Halluzinationen von Chatbots als überzeugend formulierte, aber weitgehend erfundene Resultate.[288]

Gerade mit der Einführung großer Sprachmodelle (Large Language Models, LLM) wie ChatGPT oder Gemini von Google kam es auch zu Halluzinationen.[289] Die Nutzer beschwerten sich, dass solche Chatbots oft sinnlos plausibel klingende Zufallslügen in ihren generierten Inhalten einbetteten. Als beispielsweise ChatGPT gebeten wurde, einen Artikel über das letzte Finanzquartal eines bestimmten Unternehmens zu generieren, erstellte dieser Chatbot einen kohärenten Artikel, erfand aber darin enthaltene Finanzzahlen.[290] Nach Fragen über astrophysikalische Magnetfelder behauptete ChatGPT fälschlicherweise, dass Magnetfelder von Schwarzen Löchern durch die extrem starken Gravitationskräfte in ihrer Nähe erzeugt würden. In Wirklichkeit hat ein Schwarzes Loch aufgrund des No-Hair-Theorems kein Magnetfeld.[291] Auch im Deutschen Kontext würde es zu Halluzinationen kommen, wenn die Frage nach dem Beruf von Bettina Wulff oder ob es die Stadt Bielefeld wirklich gibt. Das kommt daher, dass im Netz mehr falsche Informationen als richtige Informationen vorhanden sind und dies zu dem entsprechenden mathematisch-statischen

[286] AG Köln, 02.07.2025 - 312 F 130/25 KI-Schriftsatz: Anwalt blamiert sich vor Gericht https://rsw.beck.de/aktuell/daily/meldung/detail/ag-koeln-312f13025-ki-schriftsatz-anwalt-halluzinationen-berufsrecht abgerufen am 16.09.2025.

[287] Craig S. Smith: AI Hallucinations Could Blunt ChatGPT's Success. In: IEEE Spectrum, 24. März 2023. Abgerufen am 24. September 2023 (englisch)

[288] Google cautions against hallucinating chatbots, report says. Reuters, 11. Februar 2023. Abgerufen am 24. Nov. 2024 (englisch)

[289] Christian J. Meier: Warum die KI so gerne lügt. In: Süddeutsche Zeitung, 28. März 2023. Abgerufen am 24. Nov. 2024

[290] Quelle Wikipedia Suchwort „Halluzination (Künstliche Intelligenz) „Abgerufen am 24. Nov. 2024

[291] Ziwie Ji et al.: Survey of hallucination in natural language generation. In: ACM Computing Surveys, 55(12), S. 1-38, 2023 (englisch)

Ergebnissen führen würde. Analysten betrachten häufige Halluzinationen als ein großes Problem der LLM-Technik. [292]

II. Rechtliche Würdigung

Eine Halluzination in den Kontext eines Sachmangels i.S.v § 434, § 633 BGB oder eine eines Produktmangels i.S.v. § 327e BGB zu bringen erscheint mehr als schwierig und wird die Gerichte in der Zukunft vor besonderen Herausforderungen stellen.

1. Sachmangel vs. Produktmangel

Die Abgrenzung zwischen Sachmangel und Produktmangel richtet sich nach der vertraglichen Grundlage. Bei Kaufverträgen über eine physische Sache, die die KI beinhaltet (z. B. ein Gerät mit vorinstallierter KI). Z.B. eine KI-gestützte Diagnosemaschine, die Halluzinationen erzeugt, weist einen Sachmangel auf, sofern die Fehlfunktion bereits bei Gefahrübergang vorliegt. Bei Verträgen über digitale Inhalte oder Dienstleistungen die unter die Anwendung des § 327e BGB fallen, wäre folgender Fall denkbar: Als Beispiel wäre ein KI-System denkbar, welches die Cloud-Dienst oder digitale Lizenz bereitstellt, dann gelten die Maßstäbe des § 327e BGB. Das Halluzinieren, das falsche Ergebnisse erzeugt, ist dann ein Produktmangel, insbesondere wenn die Fehlfunktion durch Updates verschärft wird.

a) Sachmangel im Kaufvertrag

Will ein Hersteller eines KI-Systems, welches z. B. aus einem Roboter oder Algorithmus besteht, dieses gem. § 433 BGB verkaufen, so trifft ihn natürlich auch die Mängelhaftung, wenn ein Mangel i. S. v. § 434 BGB vorliegt. Dem Käufer des KI-Systems stehen dann die Rechte nach §§ 437 ff. BGB zu. In der Robotik können Mängel vor allem in der Mechanik der Maschine vorkommen, Mängel in KI-Algorithmus scheinen schwerer nachweisbar zu sein. Mangels Praxis zur Mängelhaftung für einen KI-Algorithmus kann nur eine Analogie zur Mängelhaftung für Software und dessen Quellcode herhalten. Mit der herrschenden Meinung[293] kommt eine Analogie in Betracht, wenn die „Interessenlage vergleichbar“ ist und das Fehlen einer passenden

[292] Quelle Wikipedia Suchwort „Halluzination (Künstliche Intelligenz) „Abgerufen am 24. Nov. 2024
[293] *Rüthers/Fuscher/Birk,* Rechtstheorie mit Juristischer Methodenlehre, 10. Aufl. 2018.

Rechtsnorm eine „planwidrige Regelungslücke“ darstellt. Handelt es sich um einen nackten Algorithmus als mathematisch-logische Kette, wie z. B. dem BMI-Code, dann wird keine vergleichbare Interessanlage angenommen werden können, da ein Algorithmus keiner Maschine Befehle gibt, was beim Quellcode durchaus der Fall ist. Eine vergleichbare Interessanlage dürfte angenommen werden können, wenn der Quellcode zu einem kleineren Teil auch einen Algorithmus enthält. Einfaches Beispiel wäre eine Handy-App, die einen BMI-Wert berechnet. Der Algorithmus wäre im Verhältnis zum Quellcode relativ klein, weil der Quellcode, der die Benutzeroberfläche der App erzeugt, deutlich umfangreicher sein dürfte als der BMI-Algorithmus. Der BGH[294] ist aber der Ansicht, dass im Einzelfall die konkrete Anwendung und Verknüpfung von Algorithmen in einem Programm sowie die Art und Weise ihrer Implementierung und Zuordnung zueinander urheberschutzfähig sein können, was zu einer vergleichbaren Interessanlage führen dürfte. In einem solchen Fall kann dann auch die Sachmängelhaftung bei einem Algorithmus, der integriert in einer Software ist, angenommen werden. Die Bestimmung eines Mangels für einen reinen Algorithmus dürfte sich über § 475b BGB nach den allgemeinen Grundsätzen von § 434 BGB richten. Grundsätzlich liegt ein Mangel i. S. v. § 434 Abs. 1 BGB bereits dann vor, wenn das KI-System nicht der vertraglichen vereinbarten Beschaffenheit entspricht (§ 434 Abs. 2 Nr. 1 BGB) bzw. sich nicht für die nach dem Vertrag vorausgesetzte Verwendung eignet (§ 434 Abs. 2 Nr. 2 BGB).[295] Was für das Software-Programm gilt, gilt natürlich auch für den zugrundeliegenden Quellcode. Nach der oben beschriebenen Analogie gilt das, was für den Quellcode einer Software gilt, dann auch für einen KI- Algorithmus, wenn er Teil einer Software ist.

Bei der Fehlergruppe der „vertraglich vereinbarten Beschaffenheit“ i. S. v. § 434 Abs. 2 Nr. 1 BGB bedarf es nicht umständlicher Sachverständigengutachten und Auseinandersetzungen zwischen den Parteien. Denn es geht hier nur darum, ob eine bestimmte Leistung entsprechend des Vertrages vorhanden ist oder nicht. In der Praxis wird sich z. B. die Frage nach der Herstellerhaftung danach stellen, ob der Algorithmus richtig rechnet oder nicht, ob er wirklich logisch ist. Weitaus schwerer tun sich

[294] BGH, 04.10.1990 – I ZR 139/89 – "Betriebssystem" = BGHZ 112, 264, NJW 1991, 123; ZIP 1991, 191; MDR 1991, 503, GRUR 1991, 449; BB 1991, 1; BB 1991, 2; DB 1991, 587; ZUM 1991, 246.

[295] *Spindler,* CR 2015, 766 bis 776.

die Gerichte mit der zweiten Kategorie, vgl. § 434 Abs. 2 Nr. 2BGB. Es wird vertreten, dass der vertraglichen Vereinbarung die Sollbestimmungen ausdrücklich vertraglich vorgegeben werden soll.[296] Demgegenüber regelt der Bereich der vertraglich vorausgesetzten Verwendung den Bereich konkludent vereinbarter Kriterien.[297] Dies wäre z. B. der Fall bei der Produktbeschreibung der KI-Technologie. Ähnlich sieht es aus, wenn die gewünschten Funktionen z. B. von Algorithmen im Laufe von Vertragsverhandlungen mit dem Hersteller der KI-Systembesprochen und gemeinsam akzeptiert worden sind.[298] In der Praxis wird man die Anforderungen an den KI-Algorithmus konkret festlegen müssen, was sollen z. B. die Suchergebnisse eines KI-Algorithmus, der z. B. für Deep Learning verwendet wird, bzw. was möchte der Kunde damit erreichen. Gem. § 434 Abs. 3 Nr. 1 BGB kann ein wichtiger Maßstab für die Mangelhaftigkeit eines KI-Algorithmus die gewöhnliche Verwendung sein. Bei der Eignung zur gewöhnlichen Verwendung, die objektiv zu bestimmen ist, ist darauf abzustellen, welche Beschaffenheit der Käufer erwarten kann. Dies bestimmt sich nach dem Erwartungshorizont des Durchschnittskäufers. Bei der Beschaffenheit des Kaufgegenstandes kommen alle tatsächlichen, rechtlichen, wirtschaftlichen und sozialen Umstände in Frage, die nach der Verkehrsauffassung Wert und Brauchbarkeit der Sache unmittelbar beeinflussen.[299] Ein Nachweis der gewöhnlichen Verwendung ist jedoch nicht einfach. Nach § 434 Abs. 5 BGB steht einem Sachmangel die Lieferung einer anderen Sache gleich. Insofern entfällt auch seit der Schuldrechtsreform die früher zentrale Problematik, dass die Lieferung einer Standardsoftware Teil einer Gattungsschuld ist und mangelhafte Software daher gleichzeitig als Aliud anzusehen war. [300]

Ist eine Sache mangelhaft, kann der Käufer, wenn die Voraussetzungen der folgenden Vorschriften vorliegen und soweit nicht etwas anderes bestimmt ist, nach § 439 Abs. 1 BGB Nacherfüllung verlangen, nach § 439 Abs. 2 BGB den §§ 440, 323 und 326

[296] *Hoeren,* IT Vertragsrecht 2018, S. 150.
[297] So auch: *Saenger*, in HK-BGB, 9. Aufl. 2017, § 434 Rn. 11.; *Weidenkaff*, in: Palandt, 76. Aufl. 2017, § 434 Rn. 21; *Matusche-Beckmann,* in: Staudinger, 15. Aufl. 2014, § 434 Rn. 73; a. A. *Westermann,* BGB, 7. Aufl. 2016, § 434 Rn. 18 f.
[298] Vgl. LG Frankfurt, 04.11.1986 – 2/8 S 83/86, IuR 1987, 229.
[299] OLG München, 15.09.2004 – 18 U 2176/04, NJW-RR 2005, 494 = NZV 2005, 309.
[300] *Hoeren,* IT Vertragsrecht, 2018, S. 149.

Abs. 5 von dem Vertrag zurücktreten oder nach § 441 den Kaufpreis mindern und nach § 439 Abs. 3 den §§ 440, 280, 281, 283 und 311a BGB Schadensersatz oder nach § 284 BGB Ersatz vergeblicher Aufwendungen verlangen. Grundsätzlich kann der Nacherfüllungsanspruch auch an eine von vornherein festgelegte Frist gebunden sein.[301] Hierbei weist bereits der Gesetzwortlaut des § 437 BGB daraufhin, dass auch etwas anderes bestimmt sein kann. Hiermit sind natürlich vertragliche Regelungen gemeint, die grundsätzlich von den Regelungen des § 437 ff. BGB abweichen können.[302] Vergleichbares gilt im Werkrecht nach §§ 634 ff. BGB. Nach § 634 BGB kann der Besteller, wenn das Werk mangelhaft ist, und die folgenden Voraussetzungen erfüllt sind und soweit nicht etwas anderes bestimmt ist, gem. Abs. 1 Nacherfüllung verlangt werden, gem. Abs. 2 nach § 637 BGB den Mangel selbst beseitigen und Ersatz der erforderlichen Aufwendungen verlangen, gem. Abs. 3. nach den §§ 636, 323 und 326 Abs. 5 BGB von dem Vertrag zurücktreten oder nach § 638 die Vergütung mindern und gem. Abs. 4 nach den §§ 636, 280, 281, 283 und 311a BGB Schadensersatz oder nach § 284 BGB Ersatz vergeblicher Aufwendungen verlangen.

Nach § 309 Nr. 8b BGB ist bei Formularverträgen eine Bestimmung über Lieferungen neu hergestellter Sachen und über Werkleistungen die Ansprüche gegen den Verwender wegen eines Mangels insgesamt oder bezüglich einzelner Teile ausgeschlossen.[303] Dies zielt insbesondere darauf ab, den Kunden vor einer Aushöhlung seiner ihm kraft Gesetzes zustehenden Mängelrechte zu schützen und sicherzustellen, dass das Äquivalenzverhältnis von Leistungen und Gegenleistung auch bei mangelhafter Leistung des Verwenders durchgesetzt werden kann.[304] Diesem Grundanliegen muss grundsätzlich auch die Vertragsgestaltung im unternehmerischen Geschäftsverkehr Rechnung tragen.[305] Inwieweit der Kunde bereit ist, seine Rechte auf Schadensersatz oder Minderung nach §§ 437 ff. BGB bzw. nach §§ 634 ff. BGB begrenzen zu lassen, ist sicherlich vom Einzelfall abhängig.

Zum Schadensersatz nach §§ 437 Nr. 3, 280 BGB ist der Verkäufer nicht erst dann verpflichtet, wenn er den Sachmangel nach §§ 276, 278 BGB zu vertreten hat, sondern

[301] Palandt/*Putzo*, 77. Aufl. 2017, § 439 Rn. 3.
[302] Ausführlicher hierzu *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 11. Aufl. 2021, Rn. 81 ff.
[303] *Stoffels,* AGB-Recht, 5. Aufl. 2024, Rn. 959 f.
[304] Palandt/*Grüneberg*, 72. Aufl. 2013, § 309 Rn. 72
[305] *Stoffels,* AGB-Recht, 5. Aufl. 2024, Rn. 959 f.

schon dann, wenn er nicht beweist, dass er ihn nicht zu vertreten hat, denn das Gesetz vermutet, dass der Verkäufer den Sachmangel zu vertreten hat.[306] Nach §§ 280 Abs. 1 S. 2, 286 Abs. 4 BGB ist das Verschulden des Verkäufers keine Anspruchsvoraussetzung, vielmehr begründet seine Nichtschuld eine anspruchshindernde Einwendung, die der Verkäufer beweisen muss. Er muss die gesetzliche Verschuldensvermutung widerlegen und das Gegenteil, eben seine Nichtschuld, beweisen (§ 292 ZPO). Die negative Fassung des § 280 Abs. 1 Nr. 2 BGB lautet: „Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat." Sollte sich bei der näheren Untersuchung herausstellen, dass ein Mangel nicht vom Auftragnehmer zu vertreten ist und somit kein Gewährleistungsfall vorliegt, so muss der Auftraggeber die Aufwände für die Mängelsuche dem Auftragnehmer vergüten. Verlangt der Auftraggeber, dass der Auftragnehmer die Mängel behebt, obwohl er die Behebung des Mangels nicht zu vertreten hat, so schließen die Parteien über die Behebung des Mangels einen Werkvertrag gem. §§ 631 ff. BGB ab, der entsprechend dem Auftraggeber zu vergüten ist.

Sobald der Anspruch verjährt ist, darf der Schuldner gem. § 241 Abs. 1 BGB die Leistung auf Dauer verweigern. Dabei erlischt durch die Verjährung der Anspruch nicht, sondern der Anspruch wird lediglich gehemmt.[307] Aber die Hemmung ist dauerhaft, sodass der Anspruch nicht durchgesetzt werden kann, denn gegen den Willen des Schuldners ist der verjährte Anspruch nicht mehr durchsetzbar.[308] Somit muss eine Klage aus einem verjährten Anspruch mit voller Rechtswirkung nach § 322 Abs. 1 ZPO als unbegründet abgewiesen werden, sofern der Schuldner die Einrede der Verjährung geltend macht.[309] Nicht schon der Ablauf der Verjährungsfrist, sondern erst die berechtigte Leistungsverweigerung des Schuldners nach Ablauf der

[306] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1641.

[307] BGH, 02.10.2003 – V ZB 22/03 = BGHZ 156, 269; NJW 2004, 164; MDR 2004, 167; NJ 2004, 225; FamRZ 2004, 176; VersR 2004, 803; WM 2004, 843; BB 2003, 2595; JR 2004, 419; BGH, 19.05.2006 - V ZR 40/05 = NJW 2006, 2773; MDR 2006, 1272; DNotZ 2006, 849; NZBau 2006, 645; WM 2006, 1913; BauR 2006, 1464; IBR 2006, 447.

[308] BGH, 04.12.2007 – XI ZR 144/06 = NJW 2008, 1312; IBR 2008, 189; BauR 2008, 666; BGH, 27.01.2010 - VIII ZR 58/09 = BGHZ 184, 128; NJW 2010, 2422; NJW 2010, 8; MDR 2010, 650; NZM 2010, 511; ZMR 2010, 591; NJ 2010, 343; FamRZ 2010, 887; WM 2010, 986; BB 2010, 1034; JR 2010, 395; IBR 2010, 730.

[309] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 2473.

Verjährungsfrist hemmt den Anspruch dauerhaft.[310] Die §§ 195 bis 198 BGB regeln die gesetzlichen Verjährungsfristen im BGB, dabei verjähren Ansprüche nach 3, 10 oder 30 Jahren. Nach § 195 BGB dauert die regelmäßige Verjährungsfrist drei Jahre. Sachmängelansprüche von Käufern haben dagegen ihre eigenen Verjährungsregelungen, die nach Fristdauer und Beginn von der Regelverjährung der §§ 195, 199 BGB abweicht.[311] Gem. § 438 Abs. 1 BGB verjähren die Mängelansprüche wie folgt: Die in § 437 Nr. 1 und 3 bezeichneten Ansprüche verjähren 1. in 30 Jahren, wenn der Mangel a) in einem dinglichen Recht eines Dritten, aufgrund dessen Herausgabe der Kaufsache verlangt werden kann, oder b) in einem sonstigen Recht, das im Grundbuch eingetragen ist, besteht, 2. in fünf Jahren a) bei einem Bauwerk und b) bei einer Sache, die entsprechend ihrer üblichen Verwendungsweise für ein Bauwerk verwendet worden ist und dessen Mangelhaftigkeit verursacht hat, und 3. im Übrigen in zwei Jahren. I. d. R greift in der IT-Branche (sofern z. B. ein Rechenzentrum als Bauwerk gebaut wird) die gesetzliche Regelung nach Ziffer 3. von 2 Jahren. Die Verlängerung der Gewährleistungsdauer beseitigt gerade für Systeme und Software die Probleme der kurzen Verjährung aus erst in längerer Benutzung erkennbar werdenden Mängeln, bedeutet aber im Ergebnis, dass in vielen Fällen die Gewährleistung als Wartungsersatz auf die gesamte wirtschaftliche Nutzungsdauer ausgedehnt wird. Für einen KI-Algorithmus gilt dies sicherlich nicht, da es i. d. R. keine Wartungsverträge für einen Algorithmus gibt.

Die Verjährung beginnt nach § 438 Abs. 2 BGB mit der Ablieferung der gekauften beweglichen Sache.[312] Auch dann, wenn der Anspruch aus § 281 BGB oder § 284 BGB vor Ablauf der Nachfrist noch gar nicht entstanden ist.[313] Von der Entdeckung des Sachmangels hängt der Verjährungsbeginn nicht ab, auch versteckte Mängel verjähren ab Übergabe oder Ablieferung.[314]

---

[310] BGH, 02.10.2003 – V ZB 22/03 = BGHZ 156, 269; NJW 2004, 164; MDR 2004, 167; NJ 2004, 225; FamRZ 2004, 176; VersR 2004, 803; WM 2004, 843; BB 2003, 2595; JR 2004, 419; BGH, 27.01.2010 - VIII ZR 58/09 = BGHZ 184, 128; NJW 2010, 2422; NJW 2010, 8; MDR 2010, 650; NZM 2010, 511; ZMR 2010, 591; NJ 2010, 343; FamRZ 2010, 887; WM 2010, 986; BB 2010, 1034; JR 2010, 395; IBR 2010, 730.

[311] BGH, 15.11.2006 – VIII ZR 3/06 = BGHZ 170, 31; NJW 2007, 674; ZIP 2007, 131; MDR 2007, 450; DNotZ 2007, 364; WM 2007, 261; BB 2007, 177; IBR 2008, 145; IBR 2008, 20; *Gramer/Thalhofer,* ZGS 2006, 250; *Auktor,* NJW 2003, 120.

[312] BGH, 29.11.1972 – VIII ZR 122/71 = BGHZ 60, 5; NJW 1973, 189; BGH, 04.11.1992 – VIII ZR 165/91 = NJW 1993, 461; MDR 1993, 121; WM 1993, 111; BB 1993, Beil. 13; DB 1993, 424; JR 1993, 406; BGH, Urteil v. 11.10.1995 = NJW 1995, 3381; LM H. 2/1996 § 477 BGB Nr. 62; MDR 1996, 132 ; JZ 1996, 257; BB 1995, 2394; DB 1995, 2520; ZIP 1995, 1822; OLG Celle, 20.06.2006 - 16 U 287/05 = NJW 2006, 2643; MDR 2007, 137; IBR 2006, 492; BauR 2006, 1801 (Ls.).

[313] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 2473.

[314] BGH, 02.06.1980 – VIII ZR 78/79 = BGHZ 77, 215; NJW 1980, 1950; WM 1980, 1035.

b) Sachmangel im Werkvertrag

Die Mängelrechte bei Werkleistungen sieht in § 634a BGB drei verschiedene Verjährungsfristen für die in § 634 BGB aufgelisteten Ansprüche auf Nacherfüllung, Selbstvornahme und Schadensersatz vor. Da es sich bei Rücktritt und Minderung nicht um Ansprüche, sondern um Gestaltungsrechte handelt, unterliegen diese nicht den Verjährungsfristen aus § 634a BGB (vgl. insoweit §§ 218 Abs. 1, 634a Abs. 5 BGB).[315] Nach § 634a Abs. 1 Nr. 1 BGB verjähren Ansprüche bei einem Werk, dessen Erfolg in der Herstellung, Wartung oder Veränderung einer Sache oder in der Erbringung von Planungs- oder Überwachsungsleistungen hierfür bestehen, in zwei Jahren.[316] Nach § 634a Nr. 3 BGB verjähren Ansprüche im Übrigen, d. h. für unkörperliche Werkleistungen, soweit sie nicht aus Planungs- oder Überwachungsleistungen unter § 634a Nr. 1 oder Nr. 2 fallen, nach der regelmäßigen Verjährungsfrist des § 195 BGB in drei Jahren. Fraglich ist, unter was ein KI-Algorithmus fällt. Hierunter fallen z. B. die Erstellung eines Rechtsgutachten, einer Steuerklärung, einer Risikoanalyse.[317] Ob dabei die Erstellung von Software als unkörperliche Werkleistung gem. § 634a Nr. 3 BGB einzustufen ist, ist eine vom BGH noch nicht ausdrücklich entschiedene Frage.[318] Der BGH wendet die Regeln über Sachmängel an, ohne jedoch zu sagen, dass Software eine Sache ist, geschweige denn, ob körperlich oder nicht.[319] Sollte zu einem späteren Zeitpunkt die Rechtsprechung eindeutig der Meinung sein, dass Software keine Sache ist, so würde sich insoweit die Verjährungsfrist auf drei Jahre belaufen.[320] Da die Erstellung eines KI-Algorithmus sicherlich eine unkörperliche Werkleistung ist, dürfte hier die gesetzliche Regelung der regelmäßigen Verjährungsfrist des § 195 BGB von drei Jahren greifen.

[315] *Bonnmann/Erberich,* in: Luther/Knot/Palm, Die Schuldrechtsreform, 2001, S. 106.
[316] Kritisch in der Abgrenzung *Zimmermann/Leenen/Mansell/Ernst*, JZ 2001, 684, 690 f.
[317] *Bonnmann/Erberich,* in: Luther/Knot/Palm, Die Schuldrechtsreform, 2001, S. 106.
[318] Die Rspr. beginnt mit BGH, 11.02.1971, WM 1971, 615, 616 und setzt sich fort u. s. BGH, 05.05.1992, CR 1993, 85, 86; BGH, 24.11.1998, NJW-RR 1999, 347, 348.
[319] *Marly* Praxishandbuch Softwarerecht: Rechtsschutz und Vertragsgestaltung, 7. Auflage 2018, Rn. 101.
[320] *Koch,* CR 2001, 574.

c) Produktmangel

Gegenüber dem Sachmangel im Kauf- oder Werkrecht gilt vorrangig bei Verträgen über digitale Inhalte oder Dienstleistungen, der Produktmangel i. S. v. § 327e BGB.[321] Beispiel: Wird die KI als Cloud-Dienst oder digitale Lizenz bereitgestellt, gelten die Maßstäbe des § 327e BGB. Das Halluzinieren, das falsche Ergebnisse erzeugt, ist dann ein Produktmangel, insbesondere wenn die Fehlfunktion durch Updates verschärft wird.

Der § 327e BGB regelt die Mangelhaftigkeit digitaler Produkte im Rahmen eines Verbrauchervertrags über digitale Inhalte oder digitale Dienstleistungen. Ein digitales Produkt ist mangelhaft, wenn es:[322]

- Nicht die vereinbarte Beschaffenheit aufweist (§ 327e Abs. 2 Satz 1 BGB):
- Die vertraglich festgelegten Eigenschaften müssen erfüllt werden. Beispiele: Funtionsumfang, Kompatibilität oder Sicherheit.
- Nicht für die gewöhnliche Verwendung geeignet ist (§ 327e Abs. 3 Nr. 1 BGB):

Kann ein digitales Produkt nicht die grundlegenden Funktionen erfüllen, die ein Durchschnittsnutzer erwarten darf, liegt ein Mangel vor.

- Nicht mit der aktuellen Version bereitgestellt wird (§ 327e Abs. 3 Nr. 2 BGB):
- Der Anbieter muss bei der Bereitstellung des Produkts sicherstellen, dass die aktuellste Version vorliegt, sofern diese vertraglich geschuldet ist.
- Nicht ordnungsgemäß aktualisiert wird (§ 327e Abs. 3 Nr. 3 BGB):

Anbieter haben die Verpflichtung, Updates bereitzustellen, die für die Funktionalität oder Sicherheit des Produkts erforderlich sind.

- Nicht den objektiven Anforderungen genügt (§ 327e Abs. 4 BGB):
- Ein digitales Produkt muss den üblichen Erwartungen entsprechen, auch wenn keine spezifischen Vereinbarungen getroffen wurden (z. B. Zuverlässigkeit, Kompatibilität).

Als Anwendungsfall sind denkbar, wenn eine KI als „präzises Analysetool" für medizinische Diagnosen überlassen wird und das System wiederholt fehlerhafte oder

[321] Palandt/Grüneberg, BGB, 83. Aufl. 2024, § 327e BGB, Rn. 1 ff.
[322] MüKo/Wendehorst, BGB, 9. Aufl. 2022, § 327e Rn. 10 ff.

ungenaue Diagnosen liefert. Damit weicht es von der vertraglich vereinbarten Beschaffenheit ab.[323] Eine Abgrenzung könnte sein, wenn im Vertrag darauf hingewiesen, dass das KI-System nur als unterstützendes Tool dient und Fehler möglich sind, könnte ein Mangel ausgeschlossen sein.

2. Entscheidung des LG Kiel

Die Rechtsprechung zur Mangelhaftigkeit von KI-basierten Produkten ist bislang sehr überschaubar. So hat das Landgericht Kiel in einem Urteil vom 29. Februar 2024 (Az. 6 O 151/23) die Verantwortung für durch KI generierte Inhalte thematisiert.[324] Dem Gericht lag dabei folgender Sachverhalt vor: Ein mittelständisches Unternehmen klagte gegen eine Plattformbetreiberin, die automatisiert erstellte Wirtschaftsinformationen veröffentlicht hatte. Die Plattformbetreiberin wertet Pflichtveröffentlichungen aus öffentlichen Registern wie dem Handelsregister vollautomatisiert unter Einsatz von Big Data und Künstlicher Intelligenz aus. Die Daten können Nutzer per Suchanfrage abrufen. In seinen Nutzungsbedingungen heißt es, die Daten "werden durch vollständig automatisierte Analyse gewonnen und können teils oder auch weitgehend fehlerbehaftet sein". Eine Haftung für die Richtigkeit der Wirtschaftsdaten schließt er aus. Durch einen fehlerhaften KI-gestützten Zuordnungsprozess wurde fälschlicherweise eine bevorstehende Löschung des Unternehmens wegen Vermögenslosigkeit suggeriert. Die Klägerin verlangte die Unterlassung der Verbreitung unrichtiger Informationen und Ersatz vorgerichtlicher Rechtsanwaltskosten.

Das Gericht stellte fest, dass das allgemeine Persönlichkeitsrecht auch den sozialen Geltungsanspruch eines Unternehmens schützt.[325] Die Verbreitung falscher Informationen durch die Plattform verletzte dieses Recht. Die Beklagte konnte sich nicht auf Haftungsprivilegierungen nach dem Telemediengesetz berufen, da sie sich die KI-generierten Inhalte zu eigen gemacht hatte. Ein in den AGB enthaltener Disclaimer, der die Verantwortung für KI-generierte Inhalte ausschloss, wurde als unwirksam erachtet. Das LG Kiel verurteilte den Wirtschaftsinformationsdienst auf Klage des Familienunternehmens, die Behauptung der beabsichtigten Löschung wegen Vermögenslosigkeit zu unterlassen (Urteil vom

[323] Wendehorst, Christiane: „Regulatorische Herausforderungen für KI-Produkte“, MüKo-Digitalrecht, 2022.

[324] LG Kiel, 29.02.2024 – 6 O 151/23

[325] vgl. BGH, Urteil vom 16.12.2014 – VI ZR 39/14, Rn. 12 = NJW 2015, 773.

29.02.2024 - 6 O 151/23). Es bejahte eine Störerhaftung des Dienstes wegen Verletzung des Unternehmenspersönlichkeitsrechts aus § 1004 BGB analog. Der Dienst sei unmittelbarer Störer, weil er sich zur Beantwortung von Suchanfragen einer eigenen Software bedient, die Informationen aus den veröffentlichten Pflichtmitteilungen extrahiert und aufbereitet veröffentlicht. Er könne sich nicht darauf zurückziehen, an dem automatischen Prozess gar nicht beteiligt gewesen zu sein. Denn er habe bewusst eine KI eingesetzt und die sei fehlerhaft programmiert gewesen.

Außerdem habe der Dienst sich die bereitgestellten Daten zu eigen gemacht und dafür nach außen erkennbar die inhaltliche Verantwortung übernommen. Denn er bündele die Pflichtveröffentlichungen zu einem Unternehmen auf seiner Seite und verknüpfe die Informationen teilweise untereinander.

Das LG bejahte auch eine Wiederholungsgefahr. Dabei sah es eine solche Gefahr gerade durch den Einwand des Dienstes bekräftigt, er veröffentliche nur fremde Daten aus Pflichtveröffentlichungen, ohne sie zu prüfen. Denn laut Dienst seien die Pflichtinformationen im Handelsregister unzuverlässig, sodass es "zu falschen Anzeigen kommt".

Die Beklagte wurde zur Unterlassung der Verbreitung falscher Informationen und zum Ersatz der vorgerichtlichen Rechtsanwaltskosten verurteilt. Das Urteil betont die Verantwortung von Plattformbetreibern für die Inhalte, die durch von ihnen eingesetzte KI-Systeme generiert werden.

Die Entscheidung verdeutlicht, dass der Verweis auf die Automatisierung von Prozessen keinen hinreichenden Entlastungsgrund darstellt, wenn fehlerhafte Systeme rechtlich relevante Schäden verursachen. Unternehmen sind verpflichtet, durch angemessene und wirksame Kontrollmechanismen sicherzustellen, dass die eingesetzten KI-Systeme zuverlässig und rechtskonform funktionieren. Dies gilt natürlich auch dann, wenn in KI-System halluziniert und zu falschen Ergebnis kommt, obwohl die Logik des KI-Systems richtig ist.

Es wird auch sichtbar, dass die Haftung nicht allein auf Betreiber von Plattformen beschränkt ist. Auch Anbieter von KI-Systen können künftig stärker in die Verantwortung genommen werden, insbesondere wenn sich herausstellt, dass durch fehlerhafte Systeme Schäden verursacht wurden. Anbieter sollten daher proaktiv dafür Sorge tragen, dass ihre Produkte den geltenden rechtlichen und technischen Standards entsprechen. Dies gilt selbstverständlich auch für Betreiber von Plattformen, in denen ein KI-System sogenannte

Halluzinationen aufweist und fehlerhafte Ergebnisse liefert, selbst wenn die zugrunde liegende Systemlogik korrekt arbeitet

III. SaaS Modelle für KI

Sofern keine vorrangige Geschäftskonstellation i.S.v. §§ 327 ff BGB vorliegen, insbesondere durch keine B2B Geschäfte bei denen die §§ 327 ff BGB greifen, wäre es für den Betreiber von KI-System rechtlich vorteilhaft seine Leistung als ein SaaS Model anzubieten. Dies würde auch dazu führen, dass Halluzinationen nicht zu einem Haftungsfall für den Betreiber von KI-System führen würde.

1. Definition

Leider wird der Begriff SaaS nicht einheitlich verwendet und häufig mit Application Service Providing (ASP),[326] bei dem die zeitweilige Überlassung einer Software im Vordergrund steht, gleichgestellt. Dabei basiert das SaaS-Modell auf dem Grundsatz, das KI-Systeme als Software und die IT-Infrastruktur bei einem externen KI-Provider betrieben wird und vom Kunden als Dienstleistung (Service) genutzt werden.[327] Daher wird im Folgenden nur vom echten SaaS[328] ausgegangen, bei dem es lediglich um den Service geht, den die Software erbringt, aber nicht um die Überlassung der Software selbst. Daher werden für das echte SaaS-Modell in der Praxis auch keine Softwareüberlassungsverträge genutzt, sondern Abonnentenverträge (engl.: SaaS subscription contracts)[329], in denen der Kunde des SaaS (nachfolgend nur noch „Abonnent“) einen Service über das Internet, meist in monatlichen Perioden, abonniert. Dabei wird beim Abonnenten weder eine Software installiert noch eine Software in den Hauptspeicher des Abonnenten geladen.

Der BGH hat bereits 2004 entschieden, dass ASP in der Form der zeitweiligen Überlassung von Software als Miete zu betrachten ist.[330] So eindeutig ist die Betrachtung von SaaS nicht. Durch Verwendung des Begriffs „Service“ könnte man die Nähe zum Dienstvertrag nach

[326] Der BGH hat bereits in seiner ASP-Entscheidung bestätigt, dass es bei der zeitweiligen Überlassung von Software, auch über das Netz, um Miete handelt: BGH, 15.11.2006 – XII ZR 120/04 = NJW 2007, 2394; MDR 2007, 257; NZM 2007, 379; WM 2007, 467; MMR 2007, 243; K&R 2007, 91; K&R 2007, 385.

[327] http://de.wikipedia.org/wiki/Software_as_a_Service (abgerufen am 28.10.2022).

[328] Zur Abgrenzung zwischen ASP/unechten SaaS- und echten SaaS-Modellen siehe *Söbbing*, ITRB 2021, 168-171.

[329] https://saasoptics.com/saaspedia/saas-subscription-models/ (abgerufen am 28.10.2022).

[330] BGH, MMR 2007, 243 (244).

§§ 611 ff. BGB sehen.[331] Der englische Begriff „service“ ist wesentlich weiter gefasst als der deutsche Begriff „Dienst“ oder „Dienstleistung“. So kann „service“ u. a. mit „Bedienung“, „Kundendienst“, „Gottesdienst“, „Wartung“, „Betrieb“, „Bewirtung“, „Leistung“, „Gebrauch“, „Einsatz“, „Gedenkfeier“ oder „Inspektion“ übersetzt werden.[332] Aber natürlich kommt es immer auf den Charakter der im Vertrag vereinbarten Hauptleistungspflichten an. Wird, wie im idealtypischen SaaS-Vertrag, weder eine Software überlassen (dauerhaft: Kauf; zeitweise: Miete) und auch kein Erfolg (Werkvertrag) versprochen, sollte SaaS Vertrag dennoch dem Dienstrecht zuordenbar sein. Ausgehend von echten SaaS, wäre es möglichweise unnötig, dass der Anbieter von SaaS (im Folgenden „Provider“) seinem Abonnenten grundsätzlich noch Rechte an der Software des Providers einräumt. Denkt man diesen Gedanken zu Ende, würde es zu einem radikalen Umdenken führen, da langwierige Diskussionen um urheberrechtliche Klauseln obsolet werden würden. Davon abzugrenzen ist natürlich Folgendes: Wenn der Output des SaaS/KI-System zu urheberrechtlich geschützten Werken führt und diese ausschließlich von den Abonnenten erstellt worden sind, stehen diese auch nur den Abonnenten zu. Hierzu müsste aber grundsätzlich im SaaS-Vertrag nichts geregelt werden, weil die Urheberschaft generell schon im Gesetz geregelt ist, vgl. § 7 ff. UrhG.

Bei der Einordnung solcher Fernnutzungsrechte in das System der urheberrechtlichen Nutzungs- und Verwertungsrechte ist auf das urheberrechtliche Werk als solches (bzw. gedanklich auf die Softwarekopie) und nicht auf die Nutzung per se abzustellen, dies gilt sowohl bezogen auf das Vervielfältigungsrecht sowie das Verbreitungs- bzw. Vermietrecht als auch auf das Recht der öffentlichen Zugänglichmachung.[333] Somit stellt sich die Frage, ob beim SaaS eine dauerhafte oder vorübergehende Vervielfältigung, ganz oder teilweise, eines Computerprogramms i. S. v. § 69c Abs. 1 UrhG vorliegt. Fragt man sich dabei weiter, inwieweit die Nutzung von Software bei SaaS urheberrechtsrelevant ist, wird man auf § 69c Abs. 4 UrhG stoßen. Danach hat der Rechtsinhaber das ausschließliche Recht, die drahtgebundene oder drahtlose öffentliche Wiedergabe eines Computerprogramms einschließlich der öffentlichen Zugänglichmachung in der Weise, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist, vorzunehmen.

[331] *Pohle/Ammann*, K&R 2009, 625 (626).
[332] *Heydn*, MMR 2020, 435
[333] *Grützmacher*, CR 2015, 779-787.

2. Vervielfältigung

Grundsätzlich stellt die Installation einer Software auf dem IT-System des Kunden[334] sowie auch das Laden der Software in den Arbeitsspeicher des Kunden[335] eine Vervielfältigungshandlung i. S. v. § 69c Nr. 1 UrhG dar.[336] Durch das Laden der Software in den Arbeitsspeicher des Kunden könnte beim ASP regelmäßig eine Vervielfältigungshandlung i. S. v. § 69c Nr. 1 UrhG stattfinden, auch wenn der Mietvertrag keine Besitzverschaffung, sondern lediglich eine Gebrauchsüberlassung vorsieht.[337] Die Frage,[338] ob für eine Vermietung im Sinne des Urheberrechts eine körperliche Überlassung eines Werkstückes vorhanden sein muss,[339] kann ggf. offen gelassen werden, da beim SaaS erst gar keine Software in den Hauptspeicher des Abonnenten geladen wird.

Grundsätzlich muss man sich fragen, inwieweit Vervielfältigungshandlungen entweder dem Provider oder dem Kunden zuzurechnen sind. Der BGH hat hierzu in seiner Internet-Videorekorder-Entscheidung[340] ausgeführt, dass es für die Frage, wer Hersteller einer Vervielfältigung ist, zunächst allein auf eine technische Betrachtung ankommt, nicht auf wertende Überlegungen. Danach vervielfältigt derjenige, der die körperliche Festlegung technisch bewerkstelligt und kontrolliert.[341] Soweit in einer SaaS-Infrastruktur der Nutzer das Laden in den Arbeitsspeicher eines bestimmten Rechners anstößt, ist diese Vervielfältigung ihm zuzurechnen.[342] In der Praxis des SaaS ist dem Abonnenten der Vervielfältigungsvorgang im Sinne des BGH (Bewerkstelligen und Kontrollieren) nicht zuzuweisen, da dieser weder bewerkstelligt noch kontrollieren kann bzw. nicht festlegt, wie und wo gespeichert wird. Daher können die Vervielfältigungen (in vielen Fällen) nur dem Provider zugerechnet werden.[343] Denn Hersteller der Vervielfältigung ist daher derjenige, der diese körperliche

[334] BGH, 20.01.1994, I ZR 267,91 = NJW 1994, 1216, 1217.
[335] BGH, 04.10.1990, I ZR 139/89 = NJW 1991, 1231, 1234.
[336] *Marly*, Softwareüberlassungsverträge, 7. Aufl. 2018, Rn. 1127.
[337] BGH, 15.11.2006 – XII ZR 120/04 = NJW 2007, 2394.
[338] *Marly*, Softwareüberlassungsverträge, 7. Aufl. 2018, Rn. 1128.
[339] Es wird durchaus schon vertreten, dass beim ASP wegen des Mangels der körperlichen Überlassung keine Vermietung vorliegt, siehe z. B. *Wandtke*/*Bullinger*/*Grützmacher*, § 69c Rn. 5; *Bettinger*/*Scheffelt*, CR 2001, 729, 734.; *Alpert*, CR 2000, 345, 347; *Marly*, Softwareüberlassungsverträge, 7. Aufl. 2018, Rn. 1128.
[340] BGH, 22.04.2009 – I ZR 216/06, CR 2009, 598.
[341] Siehe auch *Paul*/*Niemann* in Hilber, Handbuch Cloud-Computing, 1. Aufl. 2014, Teil 3, Rn. 94.
[342] *Niemann*/*Paul,* CR 2009, 661 (662); *Marly*, Softwareüberlassungsverträge, 7. Aufl. 2018, Rn. 1151.
[343] *Niemann*/*Paul*, K&R 2009, 444 (448).

Festlegung technisch bewerkstelligt. Hier ist es ohne Bedeutung, ob er sich dabei technischer Hilfsmittel bedient, selbst wenn diese von Dritten zur Verfügung gestellt werden.[344]

Fraglich ist, ob ein Vervielfältigungsrecht für das vom Provider bereitgestellte Webformular eingeräumt werden muss. Denn auch Benutzeroberflächen, Webformulare und Bildschirmmasken können, wenn sich etwa ihre Darstellung durch besondere Anwenderfreundlichkeit auszeichnet, als wissenschaftlich-technische Darstellung gem. § 2 Nr. 7 UrhG geschützt sein.[345] Der EuGH hat dazu entschieden, dass ein Schutz der grafischen Oberfläche zwar nicht als Computerprogramm, aber nach allgemeinen Grundsätzen in Betracht kommt, ohne sich jedoch zu der in Betracht kommenden Werkart zu äußern.[346] Für die Darstellung der grafischen Oberfläche im Webbrowser des Abonnenten muss diese im Rahmen des Browsings kurzfristig in den Arbeitsspeicher des Kundenrechners kopiert werden. Über die Frage, ob das Laden in den Browser-Cache (ein Pufferspeicher) eine Vervielfältigung darstellt, besteht Uneinigkeit.[347] Erwägungsgrund 33 der InfoSoc-Richtlinie[348] lautet:
„*Eine Ausnahme vom ausschließlichen Vervielfältigungsrecht sollte für bestimmte vorübergehende Vervielfältigungshandlungen gewährt werden, die flüchtige oder begleitende Vervielfältigungen sind, als integraler und wesentlicher Teil eines technischen Verfahrens erfolgen und ausschließlich dem Ziel dienen, entweder die effiziente Übertragung in einem Netz zwischen Dritten durch einen Vermittler oder die rechtmäßige Nutzung eines Werks oder sonstiger Schutzgegenstände zu ermöglichen.*“

Soweit diese Voraussetzungen erfüllt sind, erfasst diese Ausnahme auch Handlungen, die das Browsing sowie Handlungen des Cachings ermöglichen; dies schließt Handlungen ein, die das effiziente Funktionieren der Übertragungssysteme ermöglichen, sofern der Vermittler die Information nicht verändert und nicht die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Information, die von der gewerblichen Wirtschaft weithin anerkannt und verwendet werden, beeinträchtigt.[349] Eine Nutzung sollte als rechtmäßig gelten, soweit sie vom Rechteinhaber zugelassen bzw. nicht durch Gesetze

---

[344] *Grützmacher*, CR 2015, 779-787.

[345] OLG Karlsruhe, 14.04.2010 – 6 U 46/09, GRUR 2010, 533 (Ls.).

[346] EuGH, 22.12.2010 – C-393/09, CR 2011, 220; siehe aber dort: „*Es obliegt dem nationalen Gericht, unter Berücksichtigung insbesondere der Anordnung oder spezifischen Konfiguration aller Komponenten, aus denen sich die grafische Benutzeroberfläche zusammensetzt, zu prüfen, ob dies der Fall ist, um bestimmen zu können, welche das Kriterium der Originalität erfüllen. In diesem Zusammenhang kann dieses Kriterium nicht von Komponenten der grafischen Benutzeroberfläche erfüllt werden, die nur durch ihre technische Funktion gekennzeichnet sind.*“

[347] Der Meinungsstreit ist ausführlich dargestellt bei *Loewenheim* in Schricker/Loewenheim, Urheberrecht, 6. Aufl. 2020, § 16, Rn. 21.

[348] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft

[349] *Söbbing*, ITRB 2021, 168-171.

beschränkt ist.[350] Grundsätzlich muss dabei analysiert werden, welche urheberrechtlichen Inhalte tatsächlich im Browser- oder Client-Cache gespeichert werden. Denn i. d. R. wird nicht die Software, derer sich der Provider bedient, im Cache des Kundenrechners gespeichert, sondern nur die Daten des Abonnenten, an denen der Abonnenten die ausschließlichen Nutzungsrechte und somit auch das Vervielfältigungsrecht besitzt. Das Wesen des SaaS ist gerade, dass die Rechenoperationen beim Provider und somit nicht beim Abonnenten erfolgen.[351] Denn eine reine Wiedergabe der Bildschirmdarstellung beim Abonnenten führt allein noch nicht zu einer Vervielfältigungshandlung i. S. d. § 69c Nr. 1 UrhG.[352] Gegebenenfalls könnten die zu übertragenden Daten ein urheberrechtliches Werk i. S. v. § 87a UrhG sein. Auch ist im Einzelfall zu untersuchen, inwieweit im Rahmen einer SaaS-Anwendung i. S. v. § 87b UrhG unwesentliche Teile einer Datenbank wiederholt und systematisch übertragen werden und damit entweder einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen.[353]

3. Öffentliches Zugänglichmachen

Wenn es zu keiner Vervielfältigungshandlung i. S. v. § 69c Nr. 1 UrhG beim SaaS kommt, stellt sich die Frage nach einer öffentlichen Zugänglichmachung nach §§ 69c Nr. 4, 19a UrhG, welche in der Literatur kontrovers diskutiert wird.[354] Gemäß §§ 69c Nr. 4, 19a UrhG unterliegt die öffentliche Zugänglichmachung eines Computerprogramms der Zustimmung des Inhabers des Urheberrechts am Computerprogramm. Eine öffentliche Wiedergabe liegt vor, wenn das Computerprogramm einer Vielzahl von nicht persönlich verbundenen Nutzern gleichzeitig oder sukzessive in unkörperlicher Form wahrnehmbar oder zugänglich gemacht wird.[355]

---

[350] *Paul*/*Niemann* in Hilber, Handbuch Cloud-Computing, 1. Aufl. 2014, Teil 3, Rn. 95.

[351] siehe *Marly*, Softwareüberlassungsverträge, 7. Aufl. 2018, Rz. 1151: zumindest wird die Vervielfältigung *gemeinsam* mit dem Anbieter vorgenommen. *Paul*/*Niemann* in Hilber, Handbuch Cloud-Computing, 1. Aufl. 2014, Teil 3 Rn. 91.

[352] Dies gilt zumindest solange, wie nur reine Grafikdaten übertragen werden, was bei diesen Angeboten regelmäßig der Fall sein wird. Etwas anders mag es aussehen, wenn auch clientseitig ausgeführte Programme übertragen werden, so etwa Java-Applets oder neuerdings auch HTML-Codes, nämlich in der mit Steuerbefehlen versehenen Version 540. *Grützmacher*, CR 2015, 779-787.

[353] *Wiebe*, CR 2013, 1; *Grützmacher*, Urheber-, Leistungs- und Sui-generis-Schutz von Datenbanken, 1999, 340 f.

[354] So zum ASP: OLG München, 07.02.2008 – 29 U 3520/07, GRUR-RR 2009, 91 – ASP; *Marly*, Praxishandbuch Softwarerecht, 7. Aufl. 2018, Rz. 1087; *Jaeger*, CR 2002, 309 (311); *Lutz*, Softwarelizenzen und die Natur der Sache, München 2009, 164 f.; zum Cloud Computing: *Giedke*, Cloud Computing: Eine wirtschaftliche Analyse mit besonderer Berücksichtigung des Urheberrechts, München 2013, 402 ff.; *Pohle*/*Ammann*, CR 2009, 273 (276); *Niemann*/*Paul*, K&R 2009, 444 (448); differenzierend *Dietrich*, ZUM 2010, 567 ff.

[355] *Grützmacher* in Wandtke/Bullinger, UrhR, 6. Aufl. 2022, § 69c, Rn. 50, 80.

Durch §§ 69c Abs. 4, 19a UrhG werden grundsätzlich alle Formen der öffentlichen Wiedergabe i. S. v. §§ 15 Abs. 2, 19a UrhG erfasst, gleichviel, ob die öffentliche Wiedergabe drahtlos oder drahtgebunden erfolgt.[356] Dennoch machen es sich die Rechtsprechung und die Literatur zu einfach, wenn sie ASP mit SaaS gleichsetzen. So hat das OLG München[357] in einer viel kritisierten Entscheidung[358] verlauten lassen, dass ein ASP-Betrieb auch ohne Übertragung von Programmdaten als ein öffentliches Zugänglichmachen i. S. v. §§ 69c Nr. 4, 19a UrhG zu sehen ist. Der Wortlaut des §§ 69c Nr. 4, 19a UrhG legt nach dem OLG München nicht ohne Weiteres nahe, dass die öffentliche Zugänglichmachung eines Computerprogramms notwendigerweise die Übermittlung von Programmteilen beinhalten müsse. Dem Erstgericht ist laut OLG München darin zuzustimmen, dass auch andere Werkarten (Theaterstücke, Musikwerke) in einer Weise der Öffentlichkeit zugänglich gemacht werden, ohne dass dieser das Werk selbst in körperlicher Form (nämlich durch öffentliche Darbietung und nicht durch Überlassung des Textbuches oder der Partitur) präsentiert wird. Zudem entspricht die Auslegung des §§ 69c Nr. 4 UrhG, wonach als Verwertungshandlung i. S. v. § 69c Nr. 4 UrhG grundsätzlich bereits das Zugänglichmachen eines Computerprogramms zum interaktiven Abruf genüge, dem Willen des Gesetzgebers, einen möglichst frühen Schutz des Rechtsinhabers am Computerprogramm gegen Beeinträchtigungen Dritter zu gewährleisten. Die deutliche Kritik in der Literatur ist berechtigt, da, wie *Grützmacher*[359] zu Recht ausführt, das OLG München die technischen Realitäten verkennt, weil eben beim SaaS keine Applets bzw. kein Code übertragen oder gestreamt wird und, wie bereits oben ausgeführt, lediglich Grafikdaten übertragen werden, was kein Zugänglichmachen eines Computerprogramms i.S.v. §§ 69c Abs. 4, 19a UrhG darstellt.[360]

Spindler[361] vertritt dazu, dass das Recht zur öffentlichen Zugänglichmachung nicht darauf abstellt, ob Vervielfältigungsstücke beim Nutzer angefertigt werden, sondern – als Unterfall des Rechts auf öffentliche Wiedergabe – nur auf die durch die Öffentlichkeit entsprechend

---

[356] *Dreier/Schulze/Dreier*, UrhG § 69c, Rn. 27.

[357] OLG München, 07.02.2008 – 29 U 3520/07, CR 2009, 500 (502).

[358] Siehe z.B. *Grützmacher* CR 2015, 779-787; Nägele/JacobsZUM 2010, 281 (287); Niemann, in Hilber, Handbuch Cloud Computing, Köln 2014, S. 290 und 293: allgemein, bei IaaS und PaaS aber schon wegen der vielen im Hintergrund laufenden Software.

[359] *Grützmacher*, CR 2015, 779-787.

[360] *Loewenheim* in Schricker/Loewenheim, UrhR, 6. Aufl. 2020, § 69a Rz. 2; *Haberstumpf* in Lehmann, Kap. II Rz. 15, 30; *Mestmäcker/Schulze/Haberstumpf*, § 69a Rz. 3; auf DIN 44300 abstellend: OLG Düsseldorf, 12.07.1999 – 20 U 40/99, CR 2000, 742 = NJWE-WettbR 2000, 61 – Add-on CD; zur Gesetzgebungsgeschichte der Richtlinie und den Details dieser Vorschriften ausführlich *Marly*, GRUR 2012, 773, (774 ff.); s. a. EuGH, 02.05.2012 – Rs. C-406/10 , CR 2012, 428 m. Anm. *Heymann* = GRUR 2012, 814 (815 Rz. 39, 42 f.) – SAS Institute; näher *Grützmacher* in Wandtke/Bullinger, UrhR, 6. Aufl. 2022, § 69a, Rz. 3.

[361] *Spindler* in Schricker/Loewenheim, UrhG, 6. Auflage 2020, § 69c, Rn. 41-41c.

gesteigerte Nutzung.[362] Dies gilt auch, wenn es um die Nutzung einer Betriebssystemsoftware im Rahmen des Infrastructure Cloud Services (IaaS) oder des Platform as a Services (PaaS) geht.[363] Werden Vervielfältigungsstücke der Anwendung veranlasst, ist dies aufgrund der Beherrschung des Prozesses durch den Nutzer/Abonnenten diesem zuzurechnen – und nicht dem Anbieter,[364] vergleichbar den Fällen der Erstellung einer Kopie bei einem Dritten. Anders ist dies nur zu sehen, wenn der Nutzer keinen Einfluss darauf hat, ob Vervielfältigungsstücke durch den Provider angefertigt werden, was regelmäßig beim echten SaaS der Fall sein dürfte und dazu führen dürfte, dass der Provider kein zusätzliches Recht nach §§ 69c Abs. 4, 19a UrhG für SaaS benötigt. Hinzu kommt in der Praxis, dass der Provider von SaaS häufig auch der Hersteller der Software und somit der Inhaber aller Rechte ist; dann hat die Frage weniger Bedeutung.

Selbst in dem Fall, dass der Provider ein Recht zur öffentlichen Wiedergabe nach §§ 69c Abs. 4, 19a UrhG benötigt, so bedeutet es nicht, dass der Provider dem Abonnenten Rechte an der zugrunde liegenden Software einräumen muss. Wenn nach § 69c Nr. 4 UrhG das „Computerprogramm" zugänglich gemacht werden muss,[365] so ist hierfür auf die WIPO[366]-Musterbestimmung abzustellen, die nach h. M. auch im Rahmen des § 69a UrhG greifen.[367] Danach reicht es nicht aus, dass lediglich Grafikdaten übertragen werden.[368] Denn entsprechend der WIPO-Definition ist ein Computerprogramm vielmehr die Vielzahl von Steuerbefehlen.[369] Diese werden im Regelfall aber beim echten SaaS gerade nicht übertragen und damit zugänglich gemacht. Insofern steht die Entscheidung des OLG München[370] im

[362] *Grützmacher* in Wandtke/Bullinger, UrhG, 6. Auflage 2022, § 69 c, Rn. 82.

[363] Vgl. BGH, GRUR 2009, 845 Rn. 16 – Internet-Videorekorder; *Bisges*, MMR 2012, 574 (577 f.); *Nägele*/*Jacobs*, ZUM 2010, 281 (286); *Niemann*, CR 2009, 661 (662 f.); *Grützmacher*, CR 2011, 697 (704 f.); *Wandtke*/*Bullinger*/*Grützmacher*, UrhG, § 69 c, Rn. 99; dagegen aber (nur Anbieter) *Schuster*/*Reichl*, CR 2010, 38 (40 f.); *Giedke*, S. 382 ff.; ähnlich *Hilber*/*Paul*/*Niemann*, Teil 3, Rn. 94; nicht ganz eindeutig *Bräutigam*/*Thalhofer* in Bräutigam, Teil 14, Rn. 120, die zu einer Unterlizenzierung raten.

[364] BGH, GRUR 2009, 845 Rn. 16 – Internet-Videorekorder; *Bisges*, MMR 2012, 574 (577 f.); *Nägele*/*Jacobs*, ZUM 2010, 281 (286); *Niemann*, CR 2009, 661 (662 f.); *Grützmacher*, CR 2011, 697 (704 f.).; *Wandtke*/*Bullinger*/*Grützmacher*, UrhG, § 69 c, Rn. 99; dagegen aber (nur Anbieter) *Schuster*/*Reichl*, CR 2010, 38 (40 f.); *Giedke*, S. 382 ff.; ähnlich *Hilber*/*Paul*/*Niemann*, Teil 3, Rn. 94; nicht ganz eindeutig *Bräutigam*/*Thalhofer* in Bräutigam, Teil 14, Rn. 120, die zu einer Unterlizenzierung raten.

[365] OLG München, 07.02.2008 – 29 U 3520/07, CR 2009, 500 (502).

[366] World Intellectual Property Organization, Weltorganisation für geistiges Eigentum

[367] *Loewenheim* in Schricker/Loewenheim, UrhR, 6. Aufl. 2020, § 69a, Rz. 2; *Haberstumpf* in Lehmann, Kap. II, Rz. 15, 30; *Mestmäcker*/*Schulze*/*Haberstumpf* § 69a Rz. 3; auf DIN 44300 abstellend OLG Düsseldorf, 12.07.1999 – 20 U 40/99, CR 2000, 742 = NJWE-WettbR 2000, 61 – Add-on CD; zur Gesetzgebungsgeschichte der Richtlinie und den Details dieser Vorschriften ausführlich *Marly*, GRUR 2012, 773, (774 ff.); s. a. EuGH, 02.05.2012 – Rs. C-406/10, CR 2012, 428 m. Anm. *Heymann* = GRUR 2012, 814 (815 Rz. 39, 42 f.) – SAS Institute; näher *Grützmacher* in Wandtke/Bullinger, UrhR, 6. Aufl. 2022, § 69a, Rz. 3.

[368] *Grützmacher*, CR 2015, 779-787.

[369] *Grützmacher* in Wandtke/Bullinger, UrhR, 6. Aufl. 2022, § 69a, Rz. 3.

[370] OLG München, 07.02.2008 – 29 U 3520/07, CR 2009, 500 (502).

Widerspruch zu der Rechtsprechung zu Bildschirmmasken.[371] Denn diese geht gerade davon aus, dass die übertragenden Bildschirmmasken noch kein Computerprogramm darstellen[372] und somit auch keine Nutzungsrechte eingeräumt werden müssen.[373]

4. Resümee

Zusammenfassend lässt sich festhalten, dass es im Subscription-Vertrag des SaaS-Modells für ein KI-System es nicht notwendig ist, dem Abonnenten Nutzungs- oder Vervielfältigungsrecht einzuräumen. Sollten die Ergebnisse (Services) der Software beim SaaS die Schöpfungshöhe nach § 2 Abs. 2 UrhG erreichen, würde die Urheberschaft nach §§ 7 UrhG ff. auch beim Abonnenten liegen und somit auch keine Haftung des Betreibers für eine Software in der ein KI-System integriert vorliegen. Dies würde auch dazu führen, dass Halluzinationen nicht zu einem Haftungsfall für den Betreiber von KI-System führen würde, da das Dienstleistungsrecht grundsätzlich keine Haftung für Mängel vorsieht. Dies gilt natürlich nur in dem Fall in dem die §§ 327 ff BGB keine Anwendung finden. Ausgenommen hiervon ist natürlich ein Schadenersatzanspruch z.B. nach § 280 Abs. 1 BGB.

[371] EuGH, 22.12.2010 – Rs. C-393/09, CR 2011, 221 = GRUR 2011, 220 (223) – BSA/ Kulturministerium; OLG Karlsruhe, 14.04.2010 – 6 U 46/09, CR 2010, 427 = GRUR-RR 2010, 234.

[372] *Grützmacher*, CR 2015, 779-787.

[373] Siehe oben unter II. Vervielfältigungsrechte.

E. Datenschutz

Der rechtliche Zusammenhang zwischen Künstlicher Intelligenz (KI) und dem Datenschutz ergibt sich aus einigen sehr interessanten Einzelfragen, die aus Platzgründen nicht alle aufgeführt werden können. In folgenden werden aber auf zwei sehr interessanten Einzelfragen eingegangen. Nämlich die Fragen: "Verstößt das Maschine Learning gegen den Datenschutz" und welche Rechtsfragen ergeben sich bei automatisierte (KI-) Entscheidung nach Art. 22 DS-GVO.

I. Verstößt das Maschine Learning gegen die DSGVO[374]

Im Juni 2024 plante der Meta-Konzern die Verwertung von Nutzerdaten aus öffentlichen Beiträgen auf Facebook und Instagram für das Training seiner KI-Modelle. Dies löste datenschutzrechtliche Bedenken aus, da es die Verarbeitung personenbezogener Daten ohne die ausdrückliche Einwilligung der Nutzerinnen und Nutzer umfasste, was bedeutete, dass der Anwendungsbereich der DSGVO eröffnet war.

Erfasst die KI beim Auslesen des Internets (zufällig) personenbezogene Daten, so könnte es hierfür an der Rechtmäßigkeit der Verarbeitung i.S.v. Art. 6 Abs. 1 DSGVO fehlen, was zur Verhängung erheblicher Bußgelder i.S.v. Art. 83 DSGVO führen könnte. Auch unter Geltung der KI-VO wird die DSGVO von dieser nicht verdrängt, vgl. Art. 2 Abs. 7 KI-VO. Beim Kampf um noch nicht gehobene große Datenschätze wird die Frage des Datenschutzes eine bedeutende Rolle spielen.

1. Ausgangssituation

Sog. Large Language Modelle (LLM) wie z.B. ChatGPT oder Gemini, aber auch andere Modelle generativer Künstlicher Intelligenz bedienen sich eines Machine Learning Verfahrens, das Informationen aus dem Internet nutzt. Dabei kann es vorkommen, dass auch personenbezogenen Daten i.S.v. Art. 4 Nr. 1 DSGVO erfasst werden, da der Anwendungsbereich der **Verarbeitung** gem. Art. 4 Nr. 2 DSGVO sehr umfassend ist. Ausdrücklich erfasst Art. 4 Nr. 2 DSGVO das Erheben, das Erfassen, die

[374] ***Verstößt das Maschine Learning beim Auslesen des Internets gegen die DSGVO?*** Söbbing/Schwarz ITRB 2024, 212-217.

Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen und den Abgleich von personenbezogenen Daten.

Das Machine Learning benötigt sehr große Mengen an authentischen Trainingsdaten, um seine Möglichkeiten stets weiterentwickeln und zu verbessern zu können.[375] Maschinelles Lernen bei LLM arbeitet ähnlich wie ein riesiges, sehr komplexes Vorhersagesystem, das darauf trainiert ist, Text basierend auf den erhaltenen Eingaben zu generieren. Um die Bedeutung eines Wortes zu erfassen, beobachten LLM es zunächst im Kontext, nämlich anhand riesiger Trainingsdatensätze, wobei sie auf nahe gelegene Wörter achten. Diese Datensätze basieren auf der Zusammenstellung von im Internet veröffentlichten Texten, wobei neue LLM mit Milliarden von Wörtern trainiert werden. Auf die Suchanfrage eines Nutzers (Prompt) unterteilt das LLM den Satz in sog. Token.[376] Ein Token kann aus einem Wort, einer Abkürzung, eine Silbe, einem Satzzeichen bestehen. Ein Token ist wie ein Teil aus einem Puzzle zu verstehen. Das LLM analysiert die Token in einem Satz und deren Beziehung zueinander. Unter Berücksichtigung der Wahrscheinlichkeit, mit der einzelne Token mit anderen Token gemeinsam im Internet auftreten, wird eine Antwort auf den Prompt erstellt. Ein LLM hat selbst kein Faktenwissen, sondern geht von der **Häufigkeit der Information** im Internet aus. Daraus können Fehler oder sog. Halluzinationen[377] entstehen.

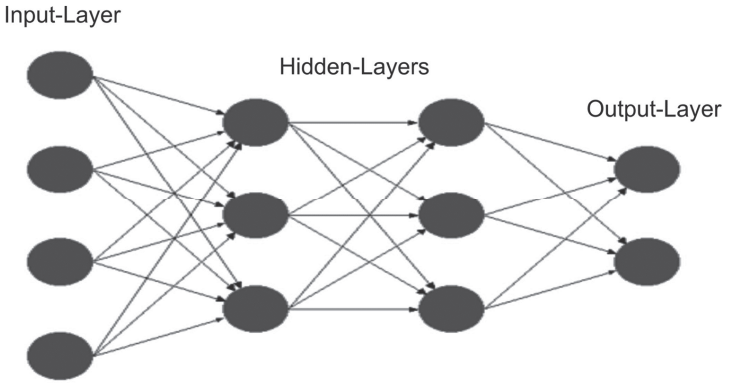
LLM sind nur so gut wie ihre **Trainingsdaten** und ihr Trainingstool, denn sie basieren auf Wahrscheinlichkeiten. Die Trainingsdaten stammen aus verschiedenen Quellen wie Büchern, Artikeln, aber vor allem aus Webseiten. Die Daten werden dann vorbereitet, was bedeutet, dass sie gereinigt, organisiert und manchmal in eine formatierte Struktur gebracht werden, damit sie für das Training des Modells geeignet sind. Für LLM werden häufig neuronale Netzwerke verwendet, speziell solche, die als Transformer-Modelle bekannt sind, sog. **Künstliche Neuronale Netzwerke** (KNN). Diese Modelle sind besonders gut darin, Muster in Sequenzen von Daten

[375] *Söbbing,* ITRB 2024, 184.

[376] Ein Token ist die grundlegende Einheit der Verarbeitung, die das Modell verwendet, um Text zu verstehen und zu generieren. S. hierzu das grundlegende GPT-Papier von *Radford* et al., Improving Language Understanding by Generative Pre-Training. Dieses Papier von OpenAI stellt das Konzept und die Implementierung des ursprünglichen GPT-Modells vor, einschließlich einer Diskussion über die Tokenisierung und wie sie die Fähigkeit des Modells beeinflusst, Sprache zu verstehen und zu generieren.

[377] Halluzinationen bei großen Sprachmodellen wie GPT beziehen sich auf Fälle, in denen das Modell inkorrekte, verfälschte oder vollkommen erfundene Informationen generiert. Diese Phänomene können durch verschiedene Faktoren verursacht werden. Vgl. *Goldberg*, Reducing Hallucination in Language Models, arXiv.org.

(wie Text) zu erkennen und zu lernen, was es ihnen ermöglicht, Sprache effektiv zu verarbeiten. Das Grundelement eines neuronalen Netzes für Deep Learning ist das Neuron, welches ein Knotenpunkt im neuronalen Netzwerk darstellt, an dem also ein oder mehrere Eingangssignale (numerische Daten) zusammentreffen und von der sog. Aktivierungsfunktion des Neurons weiterverarbeitet werden.[378] Dabei kann es sich, je nachdem, an welcher Stelle sich das Neuron im Netzwerk befindet, sowohl um Signale der Eingangsschicht als auch Signale vorhergehender Neuronen handeln. Nach der Verarbeitung der Eingangssignale werden diese als Output an die nachfolgenden Neuronen weitergegeben. Formal gesprochen, ist der Output eines Neurons eine Funktion der Inputs.[379]



Beim Training des Modells werden die gesammelten Textdaten verwendet, um dem Modell beizubringen, wie Sprache funktioniert. Dies geschieht durch ein Verfahren "überwachten Lernens", bei dem das KNN Eingabetexte und die gewünschten Ausgabetexte erhält. Das Ziel ist, dass das Modell lernt, die Eingabe in die gewünschte Ausgabe zu übersetzen. Z.B. könnte das Modell den Anfang eines Satzes sehen und lernen, wie man ihn vervollständigt. Nach dem anfänglichen Training kann das KNN weiter angepasst oder feiner abgestimmt werden, um spezifische Arten von Aufgaben oder Sprachstilen besser zu handhaben. Dies kann durch Training mit spezifischeren Datensätzen oder durch Anpassungen an der Art und Weise, wie das Modell lernt,

[378] *Kriesel*, A Brief Introduction to Neural Networks. http://www.dkriesel.com/en/science/neural_networks (1.7.2024).
[379] *Heinz*, Deep Learning – Teil 1: Einführung, Fn. 11.

erfolgen. Schließlich wird das KNN bewertet, um zu sehen, wie gut es funktioniert. Dies kann durch Tests mit echten Benutzeranfragen oder durch spezielle Evaluationstests erfolgen. Basierend auf diesen Ergebnissen wird das Modell weiter verbessert. Insgesamt basiert maschinelles Lernen bei LLM auf der Analyse und dem Verständnis von Sprache auf einer sehr großen Skala, was es ihnen ermöglicht, menschenähnliche Antworten in einer Vielzahl von Kontexten zu generieren.[380]

2. Verarbeitung i.S.v. Art. 4 Abs. 2 DSGVO

Während für das Urheberrecht mit § 44b UrhG und § 60d UrhG Sonderregeln für das Auslesen von Internetseiten durch eine KI im Weg des Machine Learnings greifen, sieht die DSGVO hierzu keine Sonderregeln vor. Auch wenn sie nicht im Fokus der Suche des KNN stehen, werden personenbezogenen Daten automatisch gesammelt, wenn das KNN das Internet durchforstet.[381]

Eine Verarbeitung i.S.v. Art. 4 Nr. 2 DSGVO wird definiert als jede[r] mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.[382] Die Aufzählung ist nicht abschließend; Ergeben, Erfassen sind Beispiele für Verarbeitung. Bei der Arbeitsweise von LLM durch KNN kommt vor allem das Erheben, das Erfassen, das Organisieren, das Ordnen, das Auslesen, das Abfragen und den Abgleich von personenbezogenen Daten i.S.v. Art. 4 Nr. 2 DSGVO in Betracht. Unter einer ihren Regelungen unterliegenden Verarbeitung versteht die DSGVO jeden Vorgang des **Umgangs mit personenbezogenen Daten**, beginnend mit der Erhebung und endend mit dem Löschen.[383]

[380] Quelle: ChatGPT.
[381] *Herbst* in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, zu den einzelnen Vorgängen.
[382] Dies entspricht der Definition von Art. 2 lit. b Datenschutz-RL.
[383] *Gola* in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 4 Rz. 35.

a) Erheben

Das Erheben i.S.v. Art. 4 Abs. 2 DSGVO ist das **Beschaffen** der personenbezogenen Daten bei dem Betroffenen selbst. An dem von dem Begriff des Beschaffens geforderten aktiven und subjektiven Element fehlt es, wenn die Daten von dem Betroffenen selbst oder von Dritten ohne Aufforderung geliefert werden, d.h. der verantwortlichen Stelle „zuwachsen“;[384] so der Fall bei der ursprünglich geplanten und nun auf die Beschwerden von noyb zurückgenommenen AGB-Änderungen von Meta (Auslesen der von den Nutzern "gelieferten" Daten). Dabei setzt das Erheben zunächst ein **aktives Tun** durch die erhebende Stelle voraus.[385] Ein KNN, welches von seinen Entwicklern als ein Webcrawler/Agent das Internet nach Informationen durchsucht, erfüllt die Voraussetzung des aktiven Tuns. Hier bedarf es eines aktiven Tuns der erhebenden Stelle (des Verantwortlichen), welches ihr zuzurechnen ist.[386] Dabei knüpft das Beschaffen an eine Tätigkeit durch die erhebende Stelle an, welche Kenntnis von den personenbezogenen Daten erhalten möchte.[387] Dies kann durchaus dem Entwickler und Betreiber des KNN unterstellt werden. Denn im Sinne eines ständigen Monitorings wird und muss der Entwickler ein Interesse an der laufenden Überprüfung haben. Ob die Erhebung dann rechtmäßig ist, wird unter Ziff. 3. erläutert.

b) Erfassen

Der Begriff des Erfassens (recording) war gem. § 3 Abs. 4 Nr. 1 BDSG a.F. ein Unterbegriff des Speicherns, der hier gesondert benannt wird, wobei die Abgrenzung letztlich für die Praxis bedeutungslos sein wird. Gemeint ist das **Aufschreiben oder Aufnehmen** der beschafften Daten.[388] Das Erfassen ist, ebenso wie das Aufnehmen, sehr weit gefasst zu verstehen.[389] Damit ist das Durchsuchen durch ein KNN auch ein Erfassen i.S.v. Art. 4 Nr. 2 DSGVO.

[384] *Schild* in BeckOK Datenschutzrecht, 48. Ed. 1.5.2024, Art. 4 DSGVO Rz. 36.
[385] *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46. Ed. 1.11.2023, Art. Rz. 35.
[386] *Simitis* BDSG, 8. Aufl. 2014, § 3 Rz. 102.
[387] *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46. Ed. 1.11.2023, Art. 4 Rz. 35.
[388] *Ernst* in Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 4 Rz. 26.
[389] *Gola*/*Schomerus.* BDSG,11. Aufl. 2012, § 3 Rz. 21, 26.

c) Organisieren und Ordnen

Die Organisation und das Ordnen von Daten überschneiden sich. Gemeint ist das Aufbauen einer wie auch immer gearteten **Struktur** innerhalb der Daten, wobei es keine Rolle spielt, ob diese simpel oder komplex ist.[390] Fragen der Qualität des Strukturierungsvorgangs, ob dieser etwa sinnvoll und vernünftig ist, spielen keine Rolle.[391] Durch den Aufbau des KNN und seiner komplexen Form zur Analyse der gesammelten Daten wird eine Struktur für das Sammeln der Daten geschaffen. Somit kann ein Organisieren i.S.v. Art. 4 Abs. 2 DSGVO bei der Verwendung des KNN unterstellt werden.

d) Auslesen und Abfragen

Das Auslesen unterscheidet sich vom Abfragen insoweit, als beim Auslesen insb. ein vorhandener Datensatz konsultiert wird, während beim Abfragen eine externe Datenbank genutzt wird.[392] In beiden Fällen geht es jedoch um eine Unterform des Erhebens, da **Daten** beschafft werden.[393] Gerade das Auslesen und Abfragen von Daten aus dem Internet kann als die Kernaufgabe des KNN der LLM gesehen werden; es ist die notwendige Aufgabe des Input-Layers für das spätere Organisieren und Ordnen der Daten.

e) Abgleich und Verknüpfung

Ein Abgleich von Daten meint die **Überprüfung**, ob die in mehreren Dateisystemen über einen Betroffenen gespeicherten Daten identisch sind oder, ob bestimmte Daten in zwei unterschiedlichen Dateien vorhanden sind (z.B. um festzustellen, welche Personen an mehreren Sachverhalten beteiligt sind).[394] Ob dies die Aufgabe des KNN eines LLM ist, kann in Frage gestellt werden, dennoch werden die KNN häufig mehrere Informationsquellen nutzen und diese miteinander vergleichen, um eine Richtigkeit (Grundwahrheit) zu bestätigen.

---

[390] *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46. Ed. 1.11.2023, Norm Rz. 43.
[391] *Ernst* in Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Norm Rz. 24.
[392] *Ernst* in Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Norm Rz. 28.
[393] *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46. Ed. 1.11.2023, Norm Rz. 43.
[394] *Ernst* in Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Norm Rz. 31.

Werden Daten aus einem System mit einem anderen **verbunden** oder hinzugefügt, um den anderen Datensatz zu vervollständigen, handelt es sich um eine Verknüpfung. [395] Auch dies wird ein KNN tun, um die Qualität seiner Daten zu verbessern.

3. Rechtmäßigkeit der Verarbeitung

Durch die weite Auslegung des Begriffs der Verarbeitung i.S.v. Art. 4 Nr. 2 DSGVO ist also sehr wahrscheinlich, dass das KNN eines LLM personenbezogene Daten verarbeitet. Von einer wirksamen Einwilligung wird man in der Regel nicht ausgehen können. Denn das Einholen der Einwilligung ist durch die Methodik der Webcrawler faktisch unmöglich.[396] Bei der eigenen Nutzung geben die Chatbots zwar ausdrücklich Hinweise auf die eigene Weiterverarbeitung. So heißt es bei Gemini von Google: "*Deine Unterhaltungen werden von Prüfer*innen verarbeitet, um die für Gemini-Apps verwendeten Technologien zu verbessern. Gib also nichts ein, was von Prüfer*innen nicht gesehen oder von Google nicht verwendet werden soll*".[397] Dies betrifft aber nur die eigenen übermittelten Daten. In die nachfolgende Nutzung hat der Betroffene sicherlich nicht über die zugrunde liegenden AGB-Regelungen zustimmen können. Keine der bekannten AGB-Regelungen sieht derzeit eine einfache Gestaltung eines Opt-out gleich der Abbestellung eines Newsletters vor. Vielmehr hatte der Meta-Konzern für Ende Juni 2024 zunächst eine Opt-out-Lösung über eine individuell zu begründende Widerspruchslösung angedacht [398]. Ziel war es die seitens der Nutzer von Facebook und Instagram geteilten Inhalte - sicherlich vom Umfang und Inhalt ein riesiger und wertvoller Datenschatz - als Trainingsdaten für die eigene KI zu nutzen. Eine Einwilligung sollte ausdrücklich nicht eingeholt werden. Man sah die geplante Änderung durch die berechtigten Interessen von Meta gedeckt. Zwischenzeitlich hat der Konzern (zunächst) von dieser Lösung Abstand genommen und mitgeteilt, "We're disappointed by the request from the Irish Data Protection Commission (DPC), our lead regulator, on behalf of the European DPAs, to delay training our large language models (LLMs) using public content shared by adults on Facebook and Instagram – particularly since

[395] *Wolff/Brink/v. Ungern-Sternberg* in BeckOK Datenschutzrecht, 46. Ed. 1.11.2023, Norm Rz. 52.
[396] Hessel/Dillschneider, RDI 2023, 458, 460.
[397] https://gemini.google.com/app
[398] https://noyb.eu/de/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai

we incorporated regulatory feedback and the European DPAs have been informed since March." [399]. Deshalb ist fraglich, ob Art. 6 Abs. 1 lit f DSGVO eine Rechtsgrundlage für die Verarbeitung sein kann. Gem. Art. 6 Abs. 1 lit. f können die Interessen des Verantwortlichen oder eines oder mehrerer Dritter, in deren Interesse die Daten verarbeitet werden oder an die die Daten übermittelt werden sollen, eine Verarbeitung rechtfertigen, sofern diese zur Wahrung nämlicher Interessen erforderlich ist. Ob ein berechtigtes Interesse vorliegt, ist nur auf den ersten Blick eine Wertungsfrage. Zu bestimmen ist zunächst das Interesse des Verantwortlichen auf Grundlage der Zweckbestimmung.[400] Ist das Interesse ermittelt, ist sodann normativ zu bestimmen, ob dieses Interesse gegen die Rechtsordnung der Union, des jeweiligen Mitgliedstaates oder gegen datenschutzrechtliche Grundsätze (Art. 5) einschließlich des Erforderlichkeitsgrundsatzes[401]Für die Annahme eines berechtigten Interesses spricht schon der Umstand, dass ein auf Dauer funktionsfähiges KI-System des Monitorings bedarf. Die Ergebnisse, die der jeweilige Chatbot – insbesondere auch die multimodalen Chatbots, welche nicht nur Text, sondern auch das gesprochene Wort, Bilder und Videos bedienen - müssen mit der Realität und bestehenden, sich ständig erweiternden Datenbeständen abgeglichen werden, Abzuwägen sind dagegen die Interessen der Nutzer, die sich ihrer (personenbezogenen) Daten zuvor entäußert haben. Wenn dies in einem öffentlich zugänglichen Bereich erfolgt sein sollte, spricht im ersten Zugang Vieles dafür, dass jedenfalls bei einer erfolgenden Anonymisierung die Interessen des Verarbeiters überwiegen.[402] Andererseits sieht der EuGH erhebliche Probleme bei einem Nutzer, „dessen Online-Aktivitäten zum großen Teil, wenn nicht sogar fast vollständig, von Meta Platforms Ireland aufgezeichnet werden, was bei ihm das Gefühl auslösen kann, dass sein Privatleben kontinuierlich überwacht wird".[403] Ob dieser Gedanke vom EuGH auch für Chatbots herangezogen werden wird, scheint offen.

Äußerst problematisch wird es aber, wenn besonders sensible Daten im Sinne des Art. 9 DSGVO betroffen sind. Die dort genannten Kategorien unterliegen

[399] https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/
[400] *Schulz* in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz 3. Auflage 2022 Rn. 61
[401] Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 61.
[402] Hessel/Dillschneider, Datenschutzrechtliche Herausforderungen beim Einsatz von KI, RDI 2023, 459, 461; Dallmann/Busse ZD 2019, 394 (395); Herfurth ZD 2018, 514 (517); Dieker, ZD 2024, 132, beck-online)
[403] EuGH GRUR 2023, 1131 Rn. 115 ff.; BeckOK DatenschutzR/Albers/Veit, 46. Ed. 1.8.2023, DS-GVO Art. 6 Rn. 72

grundsätzlich einem Verarbeitungsverbot (Art. 9 Abs. 1). Nur unter den Voraussetzungen der Abs. 2 und 3 ist eine Verarbeitung zulässig. Wenn nun ein KI-System insbesondere Bilder von Nutzern eines Social-Media-Dienstes durchsucht, werden nahezu zwangsläufig auch sensible Daten umfasst sein. Unabhängig davon, dass regelmäßig bei Lichtbildern, die Personen oder Personengruppen abbilden, eine ethnische Zuordnung möglich sein kann, unterfallen Lichtbilder den „biometrische Daten", „wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen" [404]. Nichts anderes geschieht inzwischen regelmäßig durch die fortschreitende Technik sowohl in den mobilen Endgeräten als auch in den Social-Media-Plattformen, wenn abgebildete Personen über eine Gesichtserkennung identifiziert werden.[405] Schon ein sensibles Datum führt aber dazu, dass es für die Rechtmäßigkeit auf die in Art. 9 Abs. 2 DS-GVO genannten Voraussetzungen ankommt [406]. Es hilft insoweit nicht, dass nach Art. 9 Abs. 2 lit. e Daten, die ein Nutzer selbst öffentlich eingestellt hat, von dem Dienst genutzt werden können. Denn es werden gerade auch Daten verarbeitet, die der Betroffene nicht eingestellt hat. Im Einzelfall wird ein Betroffener zudem keinen Account bei dem Dienst haben, auf welchem das Data-Scraping erfolgt. Man denke nur an die Bilder einer Familienfeier mit einer Vielzahl von Personen. Die jeweilige Plattform mag in dieser Fallgestaltung zwar nicht alle zur Identifizierung erforderlichen Informationen in ihren Händen halten. Dies schließt aber nicht aus, dass die fraglichen Daten als personenbezogene Daten qualifiziert werden können [407]. Auch ist völlig unklar, wie ein Unternehmen technisch eine genügende Unterscheidung zwischen den sensiblen und nicht sensiblen Daten gelingen soll. Zudem liegt der Ausnahmeregelung der Gedanke zu Grunde, dass dort kein Schutz von sensiblen Daten erforderlich ist, wo der Berechtigte freiwillig auf den Schutz verzichtet. Dies ist aber nur dann der Fall, wenn der Betroffene bei voller Kenntnis aller relevanten Umstände veröffentlichte (Nutzer müssten "durch in voller

[404] Erwägungsgrund 51.

[405] vgl. schon Spindler/Schuster/Spindler/Dalby, 4. Aufl. 2019, DS-GVO Art. 9 Rn. 5. Die entsprechende Funktion ist bei dem Dienst von google in Europa zwar nicht verfügbar, die Sperre kann aber über die Nutzung eines VPN leicht umgangen werden.

[406] EuGH GRUR 2023, 1131 Rn. 89; BeckOK DatenschutzR/Albers/Veit, 48. Ed. 1.5.2024, DS-GVO Art.9 Rn. 17a.

[407] EuGH Urt. v. 7.3.2024 – C-479/22 P, BeckRS 2024, 3655 Rn. 49, beck-online.

Kenntnis der Sachlage vorgenommene individuelle Einstellungen klar ihre Entscheidung zum Ausdruck gebracht haben, dass diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden sollen" [408]. Bereits aus der Formulierung des EuGH wird die Notwendigkeit einer restriktiven Auslegung der Ausnahmevorschrift deutlich.

Nach Erwägungsgrund 47 DS-GVO sollen bei der Interessenabwägung unter anderem die vernünftigen Erwartungen der betroffenen Person hinsichtlich der konkreten Verarbeitung berücksichtigt werden [409]. Falls zum Zwecke des KI-Trainings personenbezogene Daten aus öffentlich frei zugänglichen (Internet-)Quellen erhoben werden, stellt sich somit die Frage, ob die betroffene Person vernünftigerweise damit rechnen musste, dass ihre Daten beispielsweise durch Webscraping zu diesem Zwecke weiterverwendet werden. Für die Bestimmung der vernünftigen Erwartung wird grundsätzlich ein gemischt subjektiv-objektiver Maßstab zugrunde gelegt. Entscheidend ist insoweit, ob die in Rede stehende Weiterverarbeitung unter Berücksichtigung des „Wissens der Allgemeinheit" für einen objektiven Dritter erwartbar ist. Hier ist darauf zu verweisen, dass immer mehr Unternehmen – wie oben für den Meta-Konzern beispielhaft dargestellt - die Verwendung von Webscraping- bzw. Webcrawling-Methoden zum Zwecke von KI-Training selbst in ihre Datenschutzerklärungen oder -richtlinien versuchen aufzunehmen. Dadurch können diese Unternehmen die nutzerseitige Erwartungshaltung bis zu einem gewissen Grad zumindest indirekt zu den eigenen Gunsten beeinflussen. In der Literatur wird teilweise die Auffassung vertreten, niederschwellig sei das Wissen um eine Verarbeitung schon vorhanden [410].In einem nächsten Schritt sollen Umstände hervorgehoben werden, die für ein Überwiegen der Interessen von KI-Entwicklern sprechen können. Die Verarbeitungsgrundsätze sowie die konkret umgesetzten technischen und organisatorischen Maßnahmen zur Sicherung der Betroffenenrechte spielen hierbei eine entscheidende Rolle. Nur eine umfassende und effektive Anonymisierung oder Pseudonymisierung, hohe Transparenz-Standards sowie Privacy-by-Design-Anforderungen vermögen nach den vorstehenden Ausführungen eine datenschutzkonforme

[408] EuGH, EuZW 2023, 950 Rn. 82, beck-online.
[409] Erwägungsgrund 47 ber. ABl. 2018 L 127 S. 2.
[410] Dieker ZD 2024, 132, 135, beck-online

Ausgestaltung des KI-Trainings zu ermöglichen. Denn mangels einer praxisnahen Möglichkeit zur Einwilligung in die Datenverarbeitung kann so die individuelle Eingriffsintensität für die betroffenen Personen erheblich verringert werden. Je geringer die Eingriffsintensität infolge der ergriffenen Maßnahmen aufseiten der betroffenen Personen ist, umso eher kann die Interessenabwägung zugunsten der KI-Entwickler ausfallen. Schon seit 2015 sieht die EU-Kommission in Anonymisierung, Pseudonymisierung und Verschlüsselung die zentralen Elemente für eine datenschutzkonforme Erhebung von Daten [411]. Während eine Anonymisierung nach allen vertretenen Auffassungen datenschutzkonform ist[412], wird das Problem bei den anderen technischen Lösungen schwieriger: Nach Erwägungsgrund 26 Satz 2 sollen "*einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, als Informationen über eine identifizierbare natürliche Person betrachtet werden*". Dies führt bei der fortschreitenden technischen Entwicklung zu einem Dilemma: ab wann ist dies gewährleistet? Zutreffend verweist Paal auf das praktische Problem des technischen Fortschritts gerade durch die KI hin [413]. Denn die Anwendung der KI führt zur Mustererkennung, welche wiederum Rückschlüsse zulässt, die man bei der Anonymisierung sowie Pseudonomysierung nicht im Blick hatte.

4. Verantwortlicher

Zum Schluss soll noch die Frage aufgeworfen (wenn auch nicht hier vertieft) werden, wer Verantwortlicher ist (vgl. Art. 26 Abs. 1 Satz 1 DSGVO). Nicht jeder Verwender einer KI, der die KI-Anwendung vom Hersteller erworben hat, wird bei der heute weit verbreiteten arbeitsteiligen Vorgehensweise das genügende Wissen darüber haben, wie der Algorithmus, der ihm von einem Hersteller zur Verfügung gestellten KI funktioniert.[414]

Immer häufiger wird sich ein Unternehmen eine auf sein Unternehmensmodell zugeschnittene KI-Anwendung zukaufen. Den Verantwortlichen zeichnet aber aus, dass

[411] Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 152 mit Hinweis auf die Stellungnahme der EU-Kommission.
[412] Paal, ZfDR 2024, 129, 136, beck-online.
[413] Paal, ZfDR 2024, 129, 137, beck-online.
[414] Hoeren/Sieber/Holznagel MMR-HdB, Teil 29 Rn. 17, beck-online

er in der Lage ist, auf den Verarbeitungsvorgang in der Form des „Warum“ und des „Wie“, steuernd einzuwirken.[415] So könnte man als Unternehmen sich zu sicher sein und zu denken, für den unwissenden Verwender seien die oben genannten datenschutzrechtlichen Vorgänge mangels genügenden Wissens um das “*Wie” rechtlich unproblematisch. Da der schon seit Längerem die Möglichkeit einer “gemeinsamen Verantwortlichkeit” für einen umfassenderen Schutz der Rechte der Verbraucher anerkennt*[416]*, können im Einzelfall für den Verwender einer eingekauften KI-Anwendung zusätzliche und unerwartete Probleme auftauchen. Da sich die Zwecke des Herstellers der KI und des Verwenders hier zudem „wechselseitig ergänzen*” können[417], könnten nach der Rechtsprechung des EuGH beide als Verantwortliche im Sinne des Art. 26 Abs. 1 Satz 1 DSGVO anzusehen sein. Entscheidend dürfte im Sinne des Art. 4 Nr. 7 DSGVO die Entscheidungsmacht auch des Verwenders über die Datenverarbeitung sein (sog. „*decisive influence*“).[418] Eine solche wird man sowohl beim Hersteller als auch dem Verwender des Systems bejahen müssen. Denn in der Regel wird er Verwender „im Eigeninteresse auf die Entscheidung über die Zwecke und Mittel der Verarbeitung Einfluss genommen” haben, was insoweit ausreicht [419]. Ist das Unternehmen danach Verantwortlicher, trifft es zudem noch die Datensicherheitspflicht nach Art. 32 DS-GVO, für deren Einhaltung den Verantwortlichen die Beweislast trifft.[420]

5. Resümee

Die Chancen von – insbesondere multimodalen – Maschine Learning für LLM’s sind faszinierend groß. Aber allein schon wegen den hohen Busgelder des Art. 83 Abs. 5 DSGVO dürfen die bestehenden Regelungen der DSGVO nicht außeracht gelassen werden. Hatte der EuGH in seiner sog. Schufa-Entscheidung[421] noch zugunsten der DSGVO entschieden, wäre es wünschenswert, dass der Gesetzgeber in der DSGVO gleichlaufende Regelung wie in §§ 44b / 60d UrhG etabliert, die eine technologiefreundliche Entwicklung in der EU ermöglicht. Jedoch ist eine mit Augenmaß

[415] Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 26 Rn. 19

[416] EuGH Urt. v. 5.6.2018 – C-210/16, EuZW 2018, 534 - Facebook-Fanpage, beck-online; ergangen ist die Rechtsprechung zur abgelösten DS-RL; sie dürfte aber auch auf die DS-GVO übertragbar sein; so auch Gierschmann, ZD 2020, 69, beck-online

[417] EuGH, ZD 2019, 455 – Fashion-ID; Gierschmann ZD 2020, 69, beck-online

[418] BeckOK DatenschutzR/Spoerr, 46. Ed. 1.5.2022, DS-GVO Art. 26 Rn. 17

[419] EuGH ECLI:EU:C:2023:949 = BeckRS 2023, 34702 Rn. 31ff; Assion NJW 2024, 632 Rn. 3, beck-online.

[420] EuGH ECLI:EU:C:2023:986 = EuZW 2024, 236; EuGH ECLI:EU:C:2024:72 = BeckRS 2024, 530 Rn. 42.

[421] EuGH, Urteile v. 7.12.2023 – C-634/21 „SCHUFA Holding (Scoring)“ sowie C-26/22 und C-64/22 „SCHUFA Holding (Restschuldbefreiung)“) vom 7. Dezember 2023 = Söbbing/Schwarz ZD 2024, 160.

erfolgende Auslegung des "berechtigten Interesses" möglich und nach unserer Meinung auch geboten. Besonders bedauerlich ist, dass bei dem AI-Act die Möglichkeit ausgelassen wurde, eine eigenständige und belastbare Regelung für die Datenerhebung bei KI-Anwendungen zu treffen. Die daraus resultierende Rechtsunsicherheit geht unnötigerweise zu Lasten der Anwender.

Bei der Betrachtung wurde der Aspekt der wissenschaftlichen Forschung, wie er z.B. § 60d UrhG verwendet wird, für die DSGVO nicht berücksichtigt. Dies würde den Umfang des Artikels deutlich überschreiten, aber sicherlich spannende Möglichkeit offenbaren.

II. Welche Datenschutzfragen ergeben sich bei automatisierte (KI-)Entscheidung

Die Ermittlung der Kreditwürdigkeit anhand eines scores basiert laut des Anhang III. der KI-VO auf einer künstlichen Intelligenz und möglicherweise auf der Basis eines Hochrisikosystems. Die DSGVO hat hierzu den Art. 22 DSGVO erschaffen zu dem sich mittlerweile auch der EuGH geäußert hat.[422]

1. Einleitung

In Art. 22 regelt die DSGVO die Besonderheiten für Profiling und automatisierte Entscheidungsfindungen. Der Art. 22 DSGVO normiert ein grundsätzliches Verbot[423] automatisierter Entscheidungen, die gegenüber betroffenen Personen rechtliche Wirkungen entfalten oder sie sonst erheblich beeinträchtigen.[424] Eine automatisierte Einzelentscheidung im Sinne der Verordnung erfolgt unter Ausschluss jeglicher menschlicher Einbindung.[425] Die betroffene Person sollte das Recht haben, keiner Entscheidung – was eine Maßnahme einschließen kann – zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer

[422] Muss die SCHUFA offenlegen, wie sie ihren Score berechnet? Grundsatzentscheidung des EuGH zu Art. 22 DSGVO und § 31 BDSG erwartet; Sichtweise des Generalanwalts am EuGH Fachartikel, Söbbing/Schwarz, in Recht der Datenverarbeitung Beck-Verlag, ZD 2023, 579.

[423] Zum Verbotscharakter der Norm: *Martini* in: Paal/Pauly, DS-GVO BDSG, Art. 22, Rn. 15; Spindler/Schuster/Spindler/Horváth, 4. Aufl. 2019, DS-GVO Art. 22 Rn. 5.

[424] Siehe Erwägungsgrund 71 DSGVO.

[425] *Wendehorst/Gritsch* in: Omlor/Link, Kryptowährungen und Token, II. Datenschutzrechtlicher Befund, 2., aktualisierte und erweiterte Auflage 2023, Rn. 57.

automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder ein Online-Einstellungsverfahren ohne jegliches menschliches Eingreifen.[426] Mit § 31 BDSG soll der Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften geregelt werden.[427] In § 31 BDSG kann aus unionsrechtlichen Gründen nur die der Datenverarbeitung nachgelagerte, weitere Verwendung von Scoring- und Bonitätsauskünften geregelt werden und auch dies nur, soweit dies dem Schutz des Wirtschaftsverkehrs dient.[428] Art. 22 DSGVO regelt nicht direkt das Scoring, wie es in § 31 BDSG verstanden wird. Denn Art. 22 Abs. 1 DSGVO macht Vorgaben dazu, wann eine betroffene Person das Ziel einer Entscheidung sein darf, die auf einer automatisierten Verarbeitung beruht. Regelungsgegenstand von Art. 22 Abs. 1 DSGVO ist die „Entscheidung" (und ihre Auswirkungen) und sind nicht Anforderungen an die Ermittlung eines Scorewerts. § 31 Abs. 1 BDSG betrifft hingegen die Vorbereitung einer Entscheidung („zum Zweck der Entscheidung").[429]

Der BGH[430] hatte bereits 2014 entschieden, dass ein Betroffener einen Anspruch auf Auskunft darüber hat, welche personenbezogenen, insbesondere kreditrelevanten Daten bei der SCHUFA gespeichert sind und in die Berechnung seiner Wahrscheinlichkeitswerte einfließen. Zur Berechnung des Scorewerts nimmt die SCHUFA eine Bonitätseinschätzung vor, wofür aus bestimmten Merkmalen einer Person auf der Grundlage mathematisch-statistischer Verfahren für diese die Wahrscheinlichkeit eines künftigen Verhaltens, z. B. die Rückzahlung eines Kredits, prognostiziert wird. Die Gewichtung der Einzeldaten bei der Ermittlung des Wahrscheinlichkeitswerts und die Bildung etwaiger Vergleichsgruppen seien hingegen als wesentlicher Bestandteil der sogenannten Scoreformel Geschäftsgeheimnis der SCHUFA und deswegen nicht mitzuteilen, so die Sichtweise der SCHUFA im BGH-Verfahren.[431]

---

[426] Artikel-29-Datenschutzgruppe, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251 rev. 01, S. 20.
[427] *Kühling*, NJW 2017, S. 1985, 1988.
[428] BT-Drs. 18/11655, S. 31.
[429] *Kühling/Martini* et al., Die DSGVO und das nationale Recht, 2016, S. 441.
[430] BGH, Urteil vom 28.01.2014 – VI ZR 156/13 = NJW 2014, S. 1235.
[431] *Schade*, ZD 2014, S. 306, 309, Anm. zu BGH, Urteil vom 28.01.2014 – VI ZR 156/13

Nach dem das Verwaltungsgericht Wiesbaden dem EuGH zwei Vorabentscheidungsersuchen zur DSGVO (Rechtssachen C-26/22 und C-64/22) vorgelegt hat, wird nun die Sichtweise des BGH vom Generalanwalt am EuGH in Frage gestellt. In den beiden Schlussanträgen vom 16.03.2023 beschäftigte sich der Generalanwalt mit der Arbeitsweise der SCHUFA und deren Einordnung der Wahrscheinlichkeitswerte (Scoring), vgl. Rs. C-634/21. In den hier nicht besprochenen, aber verbundenen Rs. C-26/22 und C-64/22 geht es um die gerichtliche Überprüfbarkeit von rechtsverbindlichen Beschlüssen von (Datenschutz-)Aufsichtsbehörden und die Speicherung von Daten in privaten Wirtschaftsauskunfteien, wenn diese Daten aus den öffentlichen Registern bereits gelöscht wurden.[432] Der BGH hat hierzu die Aussetzung des Verfahrens bis zu der Entscheidung des EuGH in den dort anhängigen (verbundenen) Verfahren C-26/22 und C-64/22 beschlossen.[433]

2. Verfahren am VG Wiesbaden (Rs. C-634/21)

In dem ursprünglichen Fall vor dem VG Wiesbaden[434] zur Rs. C-634/21 forderte der Betroffene die SCHUFA auf, die ihn betreffenden falschen Eintragungen zu löschen und Auskunft über die der Eintragung zugrunde liegenden gespeicherten Daten zu erteilen. Dabei betrifft das Verfahren einen Rechtsstreit zwischen einem Bürger und dem Land Hessen, vertreten durch den Hessischen Beauftragten für Datenschutz und Informationsfreiheit (im Folgenden: HBDI), hinsichtlich des Schutzes personenbezogener Daten. Im Rahmen ihrer wirtschaftlichen Tätigkeit, die darin besteht, ihre Kunden mit Auskünften über die Kreditwürdigkeit Dritter zu versorgen, lieferte die SCHUFA Holding AG einem Kreditinstitut einen Scorewert in Bezug auf diesen Bürger. Dieser Scorewert diente als Grundlage für die Verweigerung des von diesem Bürger beantragten Kredits.[435] Auf Anfrage des betroffenen Bürgers teilte die SCHUFA (wie üblich) den berechneten Scorewert sowie die grundsätzliche Funktionsweise der Scorewert-Berechnung mit. Was die SCHUFA aber nicht mitteilte, war die

[432] Hierauf hat die SCHUFA bereits reagiert und die Frist für die Löschung der Rechtschuldbefreiung auf sechs Monate reduziert. https://www.schufa.de/ueber-uns/presse/pressemitteilungen/schufa-loescht-restschuldbefreiung-sechs-monaten/ (abgerufen am 07.07.2023).

[433] Beschluss vom 27.03.2023 – VI ZR 225/21 = ZIP 2023, S. 868.

[434] NZI 2023, S. 399.

[435] Pressemitteilung Nr. 49/23 des EuGH vom 16.03.2023.

Berechnungsmethode oder Arbeitsweise ihres Algorithmus. Gestützt auf die oben dargestellte Sichtweise des BGH[436], nahm die SCHUFA den Rechtsstandpunkt ein, die Berechnungsmethode sei ein Betriebs- und Geschäftsgeheimnis.

Die Klägerin hat sich darauf an den HBDI gewandt, dieser argumentierte aber, dass die SCHUFA bei der Berechnung des Bonitätswerts den im Bundesdatenschutzgesetz geregelten Anforderungen „in der Regel (i. S. v. § 31 BDSG) genüge" und im vorliegenden Fall keine Anhaltspunkte vorlägen, dass dem nicht so sei. Gegen diesen Bescheid erhob der Betroffenen Klage beim VG Wiesbaden. Das angerufene Verwaltungsgericht setzte das Verfahren aus und legte dem EuGH Auslegungsfragen zu Art. 22 DSGVO vor.437 Nach Art. 22 Abs. 1 DSGVO hat eine betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Materiellrechtlich geht es in dem EuGH-Vorabentscheidungsverfahren zentral um die Frage, ob die Ermittlung von Scorewerten durch Wirtschaftsauskunfteien im Wege automatisierter Verarbeitung von personenbezogenen Daten datenschutzrechtlich zulässig ist oder nicht.[438] Konkret wurden folgende Fragen vorgelegt:

1. Fällt die Scorewert-Berechnung durch eine Kreditauskunftei unter Art. 22 Abs. 1 DSGVO?
2. Inwieweit stehen nationale Rechtsvorschriften über das Profiling (hier § 31 BDSG) den Art. 6 Abs. 1 und 22 DSGVO entgegen?

[436] BGH, Urteil vom 28.01.2014 – VI ZR 156/13 = NJW 2014, S. 1235.
[437] VG Wiesbaden ZD 2022, S. 121 m. Anm. Qasim.
[438] MMR-Aktuell 2023, 456626.

3. Sichtweise des Generalanwalts

Die Antworten des Generalanwalts auf die oben genannten Fragen waren:

Zu 1. Der von der SCHUFA erstellte Scorewert stellt eine automatisierte Entscheidung i. S. d. Art. 22 Abs. 1 DSGVO dar.

Zu 2. Aufgrund des Vorrangs des Unionsrechts dürfte „eine solche nationale Bestimmung nicht mit der DSGVO vereinbar" und nur dann anwendbar sein, wenn es sich um ein anderes Profiling als das in Art. 22 Abs. 1 DSGVO vorgesehene handelt.

Bereits die automatisierte Erstellung eines Wahrscheinlichkeitswerts über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, ist eine automatisierte Entscheidungsfindung i. S. v. Art. 22 Abs. 1 DSGVO. Wenn dieser mittels personenbezogener Daten ermittelte Wert vom Verantwortlichen an einen dritten Verantwortlichen übermittelt wird und jener Dritte nach ständiger Praxis diesen Wert seiner Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit der betroffenen Person maßgeblich zugrunde legt, stellt dies einen Verstoß gegen Art. 22 Abs. 1 DSGVO dar.[439]
Im Detail führt der Generalanwalt (GA) aus,[440] die von der SCHUFA vorgenommene Ermittlung des Scorewerts stelle ein Profiling nach der Legaldefinition in Art. 4 Nr. 4 DSGVO dar, da der Scorewert automatisiert ermittelt werde und durch Verwendung personenbezogener Daten Rückschlüsse auf die Kreditwürdigkeit einer Person erlaube. Die Auslegungsfragen drehen sich um die weiteren Voraussetzungen von Art. 22 Abs. 1 DSGVO. Dieser setzt voraus, dass die automatisierte Entscheidung rechtliche Wirkung gegenüber den Betroffenen entfaltet oder diesen in ähnlicher Weise erheblich beeinträchtigt.

Die Grundlage der Sichtweise des Generalanwalts liegt im Erwägungsgrund 71, welcher ausdrücklich die „automatische Ablehnung eines Online-Kreditantrags" als typisches Beispiel einer Entscheidung nennt, die die betroffene Person „erheblich" beeinträchtigt. Die Rechtswirkungen entfaltende Entscheidung muss nach Art. 22 Abs.

[439] *Etteldorf*, MMR-Aktuell 2023, 456626.
[440] *Etteldorf*, MMR-Aktuell 2023, 456626.

1 DSGVO aber weiter auch „ausschließlich“ auf einer automatisierten Verarbeitung beruhen.

Darüber hinaus äußert sich der Generalanwalt auch zum Umfang des Auskunftsrechts in solchen Fällen nach Art. 15 Abs. 1 lit. h DSGVO. Danach habe die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen nicht nur die Bestätigung zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht, sondern auch andere Informationen, wie das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.[441] Darunter versteht der GA hinreichend detaillierte Erläuterungen zur Methode für die Berechnung des Scorewerts und zu den Gründen, die zu einem bestimmten Ergebnis geführt haben. Dazu gehören vor allem die bei der Entscheidungsfindung berücksichtigten Faktoren und deren Gewichtung auf aggregierter Ebene, die der betroffenen Person auch für die Anfechtung von automatisierten „Entscheidungen“ i. S. v. Art. 22 Abs. 1 DSGVO nützlich seien.[442]
Sehr interessant im Zusammenhang mit der Ausgangsfrage ist, welche Sichtweise der GA zur Vereinbarkeit von Art. 22 DSGVO und § 31 BDSG einnimmt. Der GA sieht in § 31 BDSG keine Rechtsgrundlage für Ausnahmen von Art. 22 Abs. 1 DSGVO. In der „Ermangelung von Öffnungsklauseln oder Ausnahmen, die die Mitgliedstaaten ermächtigen, genauere Vorschriften zu erlassen oder von den Vorschriften der DSGVO abzuweichen, um diese Tätigkeit zu regeln“ und „unter Berücksichtigung des Harmonisierungsgrads“ der DSGVO hält der GA § 31 BDSG für unionsrechtswidrig.

Bekanntlich lassen sich Scoring-Algorithmen weder patentieren noch urheberrechtlich schützen; wegen § 2 Abs. 1 lit. a GeschGehG wäre der Score nach der Offenlegung auch kein Geschäftsgeheimnis mehr, so dass jede/r andere sich die Algorithmen einer SCHUFA ohne Angst vor rechtlichen Sanktionen zu eigen machen könnte. Denn bisher ist auch nicht rechtlich eindeutig geklärt worden, wie ein Algorithmus

[441] Redaktion beck-aktuell, becklink 2026476.
[442] Redaktion beck-aktuell, becklink 2026476.

geschützt werden kann.[443] Hinzu kommt, dass es sich bei dem Geschäftsmodell der Auskunfteien nicht nur ein von der Rechtsordnung gebilligtes Geschäftsmodell und damit einen legitimen Verarbeitungszweck handelt.[444] Es handelt sich um ein zentrales Element des Wirtschaftslebens. Schon verfassungsrechtlich ist für die Funktionsfähigkeit des Wettbewerbs ein möglichst hohes Maß an Informationen der Marktteilnehmer über marktrelevante Faktoren geboten.[445] Und hierzu zählt jedenfalls auch die Erteilung von zutreffenden Bonitätsauskünften.[446] Diese richtigen Gedanken sollte der GA berücksichtigen und seine Sichtweise nicht allein auf Datenschutzrecht stützen.

4. Entscheidung des EuGH

Der EuGH hatte somit zwei Fragen zu beantworten.[447]

a) Erste Frage

Mit seiner ersten Frage wollte das VG Wiesbaden wissen, ob Art. 22 Abs. 1 DSGVO dahin auszulegen ist, dass eine „automatisierte Entscheidung im Einzelfall" im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet.[448] Bei der Beantwortung dieser Frage wies der EuGH darauf hin, dass bei der Auslegung einer Vorschrift des Unionsrechts nicht nur deren Wortlaut, sondern auch der Zusammenhang, in dem sie steht, sowie die Zwecke und Ziele, die mit dem Rechtsakt, zu dem sie gehört, verfolgt werden, zu berücksichtigen sind.[449] Was den Wortlaut von Art. 22 Abs. 1 DSGVO angeht, so

[443] Siehe *Söbbing*, CR 2020, S. 223-228.
[444] BGH NJW 2020, 1587 Rn. 46; BeckOK DatenschutzR/Krämer, 44. Ed. 01.05.2023, BDSG § 31 Rn. 1c mit weiteren Nachweisen.
[445] BVerfGE 105, 252, 265 f. – Glykol; BGH NJW 2011, 2204 Rn. 20.
[446] BGH NJW 2011, 2204 Rn. 21.
[447] Muss die SCHUFA offenlegen, wie sie ihren Score berechnet? Grundsatzentscheidung des EuGH zu Art. 22 DSGVO und § 31 BDSG erwartet; Sichtweise des Generalanwalts am EuGH Fachartikel, Söbbing/Schwarz, in Recht der Datenverarbeitung Beck-Verlag, ZD 2023, 579.
[448] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 40
[449] Urteil vom 22. Juni 2023, Pankki S, C-579/21, EU:C:2023:501, Rn. 38 und die dort angeführte Rechtsprechung

sieht diese Bestimmung vor, dass eine betroffene Person das Recht hat, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Nach der EuGH-Entscheidung[450] hängt die Anwendung von Art. 22 DSGVO von drei kumulativen Voraussetzungen ab, nämlich davon, dass erstens eine „Entscheidung" vorliegen muss, zweitens diese Entscheidung „ausschließlich auf einer automatisierten Verarbeitung, – einschließlich Profiling – [beruhen]" muss und drittens sie „gegenüber [der betroffenen Person] rechtliche Wirkung" entfalten oder sie „in ähnlicher Weise erheblich" beeinträchtigen muss. [451]
Was die Voraussetzung des Vorliegens einer Entscheidung betrifft, wird durch den EuGH festgestellt, dass der Begriff „Entscheidung" im Sinne von Art. 22 Abs. 1 DSGVO in dieser Verordnung nicht definiert wird. Bereits aus dem Wortlaut dieser Bestimmung ergibt sich jedoch, dass sich dieser Begriff nicht nur auf Handlungen bezieht, die rechtliche Wirkung gegenüber der betroffenen Person entfalten, sondern auch auf Handlungen, die diese Person in ähnlicher Weise erheblich beeinträchtigen.[452]

Laut EuGH wird die weite Bedeutung des Begriffs „Entscheidung" durch den Erwägungsgrund 71. der DSGVO bestätigt, wonach eine Entscheidung zur Bewertung persönlicher Aspekte, die eine Person betreffen, „eine Maßnahme einschließen [kann]", die entweder „rechtliche Wirkung für die betroffene Person" entfaltet oder „sie in ähnlicher Weise erheblich beeinträchtigt", wobei die betroffene Person das Recht haben sollte, einer solchen Entscheidung nicht unterworfen zu werden. Nach diesem Erwägungsgrund umfasst der Begriff „Entscheidung" laut EuGH beispielsweise die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen. [453]

Der EuGH führt weiter aus, dass der Begriff „Entscheidung" im Sinne von Art. 22 Abs. 1 DSGVO somit, wie der Generalanwalt in Nr. 38 seiner Schlussanträge

[450] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 43.
[451] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 43
[452] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 44
[453] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 45

ausgeführt hat, mehrere Handlungen umfassen kann, die die betroffene Person in vielerlei Weise beeinträchtigen können, ist dieser Begriff weit genug, um das Ergebnis der Berechnung der Fähigkeit einer Person zur Erfüllung künftiger Zahlungsverpflichtungen in Form eines Wahrscheinlichkeitswerts mit einzuschließen. [454]

Die zweite Voraussetzung, dass die Entscheidung im Sinne von Art. 22 Abs. 1 DSGVO „ausschließlich auf einer automatisierten Verarbeitung, – einschließlich Profiling – [beruhen]" muss, steht laut EuGH und wie auch der Generalanwalt in Nr. 33 seiner Schlussanträge ausgeführt hat, fest, dass eine Tätigkeit wie die der SCHUFA der Definition des „Profiling" in Art. 4 Nr. 4 DSGVO entspricht und dass diese Voraussetzung somit im vorliegenden Fall erfüllt ist. Laut EuGH bezieht sich der Wortlaut der ersten Vorlagefrage ausdrücklich auf die automatisierte Erstellung eines auf personenbezogene Daten zu einer Person gestützten Wahrscheinlichkeitswerts hinsichtlich deren Fähigkeit, künftig einen Kredit zu bedienen. [455]

Die dritte Voraussetzung, dass die Entscheidung gegenüber der betroffenen Person „rechtliche Wirkung" entfalten oder sie „in ähnlicher Weise erheblich" beeinträchtigen muss, ergibt sich laut EuGH bereits aus dem Inhalt der ersten Vorlagefrage, dass das Handeln des Dritten, dem der Wahrscheinlichkeitswert übermittelt wird, „maßgeblich" von diesem Wert geleitet wird. So führt nach den Sachverhaltsfeststellungen des VG Wiesbaden im Fall eines von einem Verbraucher an eine Bank gerichteten Kreditantrags ein unzureichender Wahrscheinlichkeitswert in nahezu allen Fällen dazu, dass die Bank die Gewährung des beantragten Kredits ablehnt. [456]

Folglich ist laut EuGH davon auszugehen, dass auch die dritte Voraussetzung, von der die Anwendung von Art. 22 Abs. 1 DSGVO abhängt, erfüllt ist, da ein Wahrscheinlichkeitswert wie der im Ausgangsverfahren fragliche die betroffene Person zumindest erheblich beeinträchtigt.[457] Daher ist unter Umständen wie jenen des Ausgangsverfahrens, unter denen der von einer Wirtschaftsauskunftei ermittelte und einer Bank mitgeteilte Wahrscheinlichkeitswert eine maßgebliche Rolle bei der Gewährung

[454] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 46
[455] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 47.
[456] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 48.
[457] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 49.

eines Kredits spielt, die Ermittlung dieses Wertes als solche als Entscheidung einzustufen, die im Sinne von Art. 22 Abs. 1 DSGVO gegenüber einer betroffenen Person „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“.[458] Der EuGH stellt in seiner Entscheidung fest, dass diese Auslegung durch den Zusammenhang, in dem Art. 22 Abs. 1 DSGVO steht, sowie durch die Zwecke und Ziele, die mit dieser Verordnung verfolgt werden, gestützt wird.[459] Insoweit weißt der EuGH weiter darauf hin, dass, wie der Generalanwalt in Nr. 31 seiner Schlussanträge festgestellt hat, Art. 22 Abs. 1 DSGVO der betroffenen Person das „Recht“ verleiht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden. Diese Bestimmung stellt laut EuGH ein grundsätzliches Verbot auf, dessen Verletzung von einer solchen Person nicht individuell geltend gemacht werden braucht.[460]

Da laut EuGH sich aus Art. 22 Abs. 2 DSGVO in Verbindung mit dem 71. Erwägungsgrund dieser Verordnung ergibt, ist der Erlass einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung nur in den in Art. 22 Abs. 2 genannten Fällen zulässig, d. h., wenn sie für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist (Buchst. a), wenn sie aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist (Buchst. b) oder wenn sie mit ausdrücklicher Einwilligung der betroffenen Person erfolgt (Buchst. c).[461]

Außerdem sieht Art. 22 Abs. 2 Buchst. b und Abs. 3 DSGVO laut EuGH vor, dass angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorgesehen werden müssen. In den in Art. 22 Abs. 2 Buchst. a und c dieser Verordnung genannten Fällen gewährt der Verantwortliche der betroffenen Person laut EuGH mindestens das Recht auf Erwirkung des Eingreifens einer Person, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung.[462] Ferner dürfen nach Art. 22 Abs. 4 DSGVO automatisierte Entscheidungen im Einzelfall im Sinne von diesem Art. 22 nur in bestimmten

[458] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 50.
[459] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 51.
[460] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 52.
[461] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 53.
[462] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 54.

Sonderfällen auf besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO beruhen.[463]

Darüber hinaus unterliegt laut EuGH im Fall einer automatisierten Entscheidungsfindung wie jener im Sinne von Art. 22 Abs. 1 DSGVO zum einen der Verantwortliche zusätzlichen Informationspflichten nach Art. 13 Abs. 2 lit. f und Art. 14 Abs. 2 lit. g dieser Verordnung. Zum anderen steht der betroffenen Person nach Art. 15 Abs. 1 lit. h DSGVO ein Auskunftsrecht gegenüber dem für die Verarbeitung Verantwortlichen zu, das insbesondere „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" betrifft.[464] Diese höheren Anforderungen an die Rechtmäßigkeit einer automatisierten Entscheidungsfindung sowie die zusätzlichen Informationspflichten des Verantwortlichen und die damit verbundenen zusätzlichen Auskunftsrechte der betroffenen Person erklären sich aus dem Zweck, den Art. 22 DSGVO verfolgt und der darin besteht, Personen vor den besonderen Risiken für ihre Rechte und Freiheiten zu schützen, die mit der automatisierten Verarbeitung personenbezogener Daten – einschließlich Profiling – verbunden sind.[465] Diese Verarbeitung erfordert nämlich, wie sich aus dem Erwägungsgrund 71.der DSGVO ergibt, die Bewertung persönlicher Aspekte in Bezug auf die von dieser Verarbeitung betroffene natürliche Person, insbesondere zur Analyse oder Prognose von Aspekten bezüglich ihrer Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, Vorlieben oder Interessen, Zuverlässigkeit oder ihres Verhaltens, ihres Aufenthaltsorts oder Ortswechsels.[466]

Diese besonderen Risiken sind nach diesem Erwägungsgrund nach der Sichtweise des EuGH geeignet, die Interessen und Rechte der betroffenen Person zu beeinträchtigen, insbesondere im Hinblick auf etwaige diskriminierende Wirkungen gegenüber natürlichen Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschaftszugehörigkeit, genetischer Anlagen

[463] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 55.
[464] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 56.
[465] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 57.
[466] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 58.

oder Gesundheitszustand sowie sexueller Orientierung. Daher sollte nach der Ansicht des EuGH diesem Erwägungsgrund der betroffenen Person gegenüber eine faire und transparente Verarbeitung gewährleistet werden, insbesondere durch die Verwendung geeigneter mathematischer oder statistischer Verfahren für das Profiling und durch technische und organisatorische Maßnahmen, mit denen in geeigneter Weise sichergestellt wird, dass das Risiko von Fehlern minimiert wird.[467]

Die in den Rn. 42 bis 50 des vorliegenden Urteils dargelegte Auslegung und insbesondere die weite Bedeutung des Begriffs „Entscheidung" im Sinne von Art. 22 Abs. 1 DSGVO verstärkt den wirksamen Schutz, auf den diese Bestimmung abzielt.[468] Hingegen bestünde unter Umständen wie jenen des Ausgangsverfahrens, an denen drei Akteure beteiligt sind, die Gefahr einer Umgehung von Art. 22 DSGVO und folglich eine Rechtsschutzlücke, wenn einer engen Auslegung dieser Bestimmung der Vorzug gegeben würde, nach der die Ermittlung des Wahrscheinlichkeitswerts nur als vorbereitende Handlung anzusehen ist und nur die vom Dritten vorgenommene Handlung gegebenenfalls als „Entscheidung" im Sinne von Art. 22 Abs. 1 dieser Verordnung eingestuft werden kann. [469] In diesem Fall würde nämlich die Ermittlung eines Wahrscheinlichkeitswerts wie des im Ausgangsverfahren in Rede stehenden nicht den besonderen Anforderungen von Art. 22 Abs. 2 bis 4 DSGVO unterliegen, obwohl dieses Verfahren auf einer automatisierten Verarbeitung beruht und Wirkungen entfaltet, welche die betroffene Person erheblich beeinträchtigen, da das Handeln des Dritten, dem dieser Wahrscheinlichkeitswert übermittelt wird, von diesem maßgeblich geleitet ist. [470]

Außerdem könnte die betroffene Person laut EuGH und wie auch der Generalanwalt in Nr. 48 seiner Schlussanträge ausgeführt hat, zum einen bei der Wirtschaftsauskunftei, die den sie betreffenden Wahrscheinlichkeitswert ermittelt, ihr Recht auf Auskunft über die in Art. 15 Abs. 1 Buchst. h DSGVO genannten spezifischen Informationen nicht geltend machen, wenn keine automatisierte Entscheidungsfindung durch dieses Unternehmen vorliegt. Zum anderen wäre der Dritte – unter der Annahme, dass die von ihm vorgenommene Handlung unter Art. 22 Abs. 1 DSGVO fiele, da sie die

[467] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 59.
[468] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 60.
[469] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 61.
[470] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 62.

Voraussetzungen für die Anwendung dieser Bestimmung erfüllte – nicht in der Lage, diese spezifischen Informationen vorzulegen, weil er darüber im Allgemeinen nicht verfügt.[471]

Dass die Ermittlung eines Wahrscheinlichkeitswerts wie des im Ausgangsverfahren in Rede stehenden von Art. 22 Abs. 1 DSGVO erfasst wird, hat, wie in den Rn. 53 bis 55 des vorliegenden Urteils ausgeführt, zur Folge, dass sie verboten ist, es sei denn, eine der in Art. 22 Abs. 2 DSGVO genannten Ausnahmen ist anwendbar und die besonderen Anforderungen von Art. 22 Abs. 3 und 4 DSGVO sind erfüllt.[472] Was insbesondere Art. 22 Abs. 2 Buchst. b DSGVO betrifft, auf den der EuGH Bezug nimmt, ergibt sich bereits aus dem Wortlaut dieser Bestimmung, dass die nationalen Rechtsvorschriften, die den Erlass einer automatisierten Entscheidung im Einzelfall erlauben, angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten müssen.[473]

Im Licht des Erwägungsgrundes 71. der DSGVO müssen laut EuGH solche Maßnahmen insbesondere die Verpflichtung des Verantwortlichen umfassen, geeignete mathematische oder statistische Verfahren zu verwenden, technische und organisatorische Maßnahmen zu treffen, mit denen in geeigneter Weise sichergestellt wird, dass das Risiko von Fehlern minimiert wird und Fehler korrigiert werden, und personenbezogene Daten in einer Weise zu sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird, und insbesondere zu verhindern, dass es ihr gegenüber zu diskriminierenden Wirkungen kommt. Diese Maßnahmen umfassen außerdem mindestens das Recht der betroffenen Person auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der gegen sie erlassenen Entscheidung.[474]

Ferner weist der EuGH in seiner Entscheidung darauf hin, dass nach ständiger Rechtsprechung des EuGHs jede Verarbeitung personenbezogener Daten mit den in Art.

[471] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 63.
[472] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 64.
[473] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 65.
[474] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 66.

5 DSGVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten im Einklang stehen und in Anbetracht des in Art. 5 Abs. 1 Buchst. a vorgesehenen Grundsatzes der Rechtmäßigkeit der Verarbeitung eine der in Art. 6 dieser Verordnung aufgeführten Bedingungen für die Rechtmäßigkeit der Verarbeitung erfüllen muss [*Urteil vom 20. Oktober 2022, Digi, C-77/21, EU:C:2022:805, Rn. 49 und die dort angeführte Rechtsprechung*]. Der Verantwortliche muss die Einhaltung dieser Grundsätze nach dem in Art. 5 Abs. 2 DSGVO niedergelegten Grundsatz der Rechenschaftspflicht nachweisen können.[475]

Ist laut EuGH nach den Rechtsvorschriften eines Mitgliedstaats gemäß Art. 22 Abs. 2 Buchst. b DSGVO der Erlass einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung zulässig, muss diese Verarbeitung somit nicht nur die in der letztgenannten Bestimmung und in Art. 22 Abs. 4 DSGVO aufgestellten Voraussetzungen erfüllen, sondern auch die Anforderungen in den Art. 5 und 6 dieser Verordnung. Folglich dürfen die Mitgliedstaaten keine Rechtsvorschriften nach Art. 22 Abs. 2 Buchst. b DSGVO erlassen, nach denen ein Profiling unter Missachtung der Anforderungen dieser Art. 5 und 6 in deren Auslegung durch die Rechtsprechung des EuGHs zulässig ist. [476] Was insbesondere die in Art. 6 Abs. 1 Buchst. a, b und f DSGVO vorgesehenen Bedingungen für die Rechtmäßigkeit betrifft, die in einem Fall wie jenem des Ausgangsverfahrens Anwendung finden können, sind die Mitgliedstaaten nicht befugt, ergänzende Vorschriften für die Anwendung dieser Bedingungen vorzusehen, da eine solche Befugnis nach Art. 6 Abs. 3 DSGVO auf die in Art. 6 Abs. 1 Buchst. c und e dieser Verordnung genannten Gründe beschränkt ist. [477] Was außerdem im Einzelnen Art. 6 Abs. 1 Buchst. f DSGVO betrifft, dürfen die Mitgliedstaaten nach Art. 22 Abs. 2 Buchst. b DSGVO nicht von den Anforderungen abweichen, die sich aus der Rechtsprechung des EuGH nach dem Urteil vom 7. Dezember 2023, SCHUFA Holding,[478] ergeben, insbesondere nicht dadurch, dass sie das

[475] vgl. in diesem Sinne Urteil vom 20. Oktober 2022, Digi, C-77/21, EU:C:2022:805, Rn. 24EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 67]
[476] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 68.
[477] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 69.
[478] *C-26/22 und C-64/22, EU:C:2023:XXX „Restschuldbefreiung"*

Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen abschließend.[479]

Im vorliegenden Fall weist das VG Wiesbaden darauf hin, dass nur § 31 BDSG eine nationale Rechtsgrundlage im Sinne von Art. 22 Abs. 2 Buchst. b DSGVO darstellen könnte. Bezüglich der Vereinbarkeit dieses § 31 BDSG mit dem Unionsrecht bestehen für dieses Gericht aber durchgreifende Bedenken. Sollte diese Bestimmung als mit dem Unionsrecht unvereinbar angesehen werden, würde die SCHUFA nicht nur ohne Rechtsgrundlage handeln, sondern verstieße ipso iure gegen das in Art. 22 Abs. 1 DSGVO aufgestellte Verbot. [480]

Insoweit ist es laut EuGH Sache des VG Wiesbaden, zu prüfen, ob § 31 BDSG als Rechtsgrundlage im Sinne von Art. 22 Abs. 2 Buchst. b DSGVO qualifiziert werden kann, nach der es zulässig wäre, eine ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung zu erlassen. Sollte das VG Wiesbaden zu dem Schluss kommen, dass § 31 eine solche Rechtsgrundlage darstellt, hätte es noch zu prüfen, ob die in Art. 22 Abs. 2 Buchst. b und Abs. 4 DSGVO und in den Art. 5 und 6 DSGVO aufgestellten Anforderungen im vorliegenden Fall erfüllt sind. [481]

Zusammenfassend beantwortet der EuGH die erste Frage so, dass Art. 22 Abs. 1 DSGVO dahin auszulegen ist, dass eine „automatisierte Entscheidung im Einzelfall" im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet.[482]

[479] vgl. in diesem Sinne Urteil vom 19. Oktober 2016, Breyer, C-582/14, EU:C:2016:779, Rn. 62, EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 70.
[480] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 71.
[481] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 72.
[482] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 25.

b) Zweite Frage

Die zweite Frage lautete, inwieweit stehen nationale Rechtsvorschriften über das Profiling (hier § 31 BDSG) den Art. 6 Abs. 1 und 22 DSGVO entgegen? Nach Auffassung des EuGH brauchte in Anbetracht der Antwort auf die erste Frage die zweite Frage nicht beantwortet zu werden.[483] Denn es „bestünden erhebliche Zweifel an der Vereinbarkeit dieser Bestimmung mit Art. 22 DSGVO, da der deutsche Gesetzgeber nur die „Verwendung" eines Wahrscheinlichkeitswerts wie des im Ausgangsverfahren in Rede stehenden regele, nicht aber die Ermittlung dieses Wertes als solche". [484]

c) Bewertung

Als kritisch muss die Sichtweise des EuGH bewertet werden, dass die Kreditentscheidung erheblich vom Kreditscore der Schufa beeinflusst ist [*Rn. 48*].[485] Denn wäre dies wirklich der Fall, würde die Bank ihr Risiko Management auf die Schufa auslagern, was nach § 25b Abs. 2 KWG in dieser Form gar nicht möglich wäre.[486] Die Schufa erstellt nur einen Kreditscore die jede Bank im Rahmen Ihres Risikomanagement unterschiedlich bewerten kann und wird. Eine risikofreudige Bank würde ggf. einen Kredit bewilligen, während eine eher konservative aufgestellte Bank dem Kunden den Kredit verweigern würde. Das in dem zugrundeliegenden Fall der Kläger keinen Kredit bei keiner Bank erhalten würde, liegt im Zweifel nicht (allein) an seinem (schlechten) Kreditscore. Vielmehr steht zu erwarten, dass er auch ohne den Kreditscore der Schufa kein Darlehen bei einer Bank erhalten hätte. Insoweit ist die Sichtweise des EuGH hier zu einfach und zu kurzgefasst, da die Entscheidung über die Kreditvergabe ausschließlich bei der Bank liegt und der Kreditscore der Schufa lediglich ein Hilfsmittel ist. Mit der Entscheidung des EuGH wird die Kreditvergabe tendenziell und entgegen seiner Intention nicht verbraucherfreundlicher werden. Ein grundlegendes Problem, welches die Entscheidung durchzieht, besteht zum einen in dem fundamentalen Missverständnis, dass die Nachprüfbarkeit eines Computerergebnisses keine binäre Eigenschaft (also die eindeutig „ja" oder „nein") ist.[487] So muss das Austauschen oder Entfernen eines (Kredit-) kriteriums nicht notwendigerweise zu

[483] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 48.
[484] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 25.
[485] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 48.
[486] *Volhard/Jang in W/B/A | KAGB § 36 Rn. 20-24 | 3. Auflage 2021*
[487] *als allgemeinverständliche Einleitung gut geeignet: siehe die Darstellung von Katharina Zweig, Die KI war's, S.149*]

einem besseren oder überhaupt anderen Ergebnis führen. Maschinelles Lernen macht gerade Sinn bei großen Regelmengen. Dort können durch maschinelles Lernen Korrelationen (nicht zwingend Kausalitäten) hergestellt werden. Anders formuliert soll die KI über maschinelles Lernen gerade Beziehungen finden, die der User allein nicht finden könnte. Zentral ist dabei die Auswahl und die Qualität der Eingangsdaten. So erfolgt die Berechnung eines Kreditscores mittels eines Algorithmus – einer Abfolge von Berechnungen. Dessen Komplexität richtet sich nach den ihm vorangestellten Annahmen (der sog. Heuristik). Letzteres stellt über die Auswahl der Eingangsdaten die eigentliche Gefahrenquelle für eine im Ergebnis falsche Bewertung dar. Damit ist die Kritik des EuGH[488] am § 31 BDSG nicht ganz nachzuvollziehen, da sich § 31 BDSG am 71. Erwägungsgrund der DSGVO orientiert und zur Berechnung des Wahrscheinlichkeitswerts sich nach § 31 Abs. 1 Nr. 2. BDSG auf ein wissenschaftlich anerkanntes mathematisch-statistischen Verfahrens bezieht und natürlich, wenn der Score falsche Berechnungen erzeugt, diese schon allein aus wirtschaftlichen Gründen manuell behoben werden. Aus der mangelnden Vereinbarung zur Fehlerbehebung eine Diskrimierungsmöglichkeit zu sehen, erfordern schon eine sehr lange Kette der objektiven Zurechenbarkeit. Anders als im amerikanischen Recht bietet das europäische Recht nicht die Möglichkeit einer rein statistischen Reaktion auf eine Ungleichbehandlung. Die Möglichkeit einer Sanktion allein aufgrund eines „disparate impacts“[489] im Gegensatz zur „disparate treatments“ kennt das europäische Recht nicht.

Die vorliegende Entscheidung des EuGH[490] wie auch die bereits veröffentliche Sichtweise des GA ist eindeutig zu sehr zu Gunsten des Datenschutzes und zu Lasten von Geschäftsgeheimnissen gefällt worden. Nur auf die Interessen von betroffenen Kunden zu schauen und nicht die wirtschaftlichen Interessen von Unternehmen zu berücksichtigen, ist eine einseitige und zu kurz gegriffene Sichtweise. Denn welches Unternehmen wird noch in die Entwicklung von KI investieren, wenn es die Arbeitsweise seiner Algorithmen in der in Art. 15 Abs. 1 lit. h) georderten Form offengelegen werden muss und dadurch die Gefahr besteht, dass die Arbeitsweisen von

[488] EuGH, 07.12.2023 – C-634/21 vom 7.12.2023 Rn. 66.
[489] *Hergeleitet aus dem 14th Amendment to the Unites States, https://www.archives.gov/milestone-documents/14th-amendment*]
[490] *EuGH, 07.12.2023 – C-634/21 vom 7.12.2023*

Algorithmen dadurch keine Geschäftsgeheimnisse i.S.v. § 2 Abs. 1 lit. a) GeschGehG mehr sind. Um es mit den Worten des verstorbenen Wolfgang Schäuble zu sagen: „wir übertreiben es mit dem Datenschutz und es steht bereits in der Inschrift über dem Apollo-Tempel im Delphi „Nichts im Übermaß!".[491]

5. Ausblick

Zunächst einmal könnte man auf den Gedanken kommen, zukünftig könne mit der ausdrücklichen Einwilligung nach Art. 22 Abs. 3 lit. d) i.V.m. Art. 6 Abs. 1 lit. a) DSGVO gearbeitet werden. Der Weg über die Einwilligung ist für die Praxis jedoch ein sehr sperriges Vehikel. Denn die Einwilligung soll sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommene Verarbeitungsvorgänge beziehen [*Erwägungsgrund. 32 S. 4 zur* Datenschutzgrundverordnung]. Erforderlich ist also, dass die Einwilligungserklärung sämtliche Verarbeitungsvorgänge iSv Art. 4 Nr. 2, bezogen auf den jeweiligen Zweck, abdeckt. Bei mehreren Zwecken muss sich die Einwilligung zweifelsfrei auf alle Zwecke beziehen. Vor diesem Hintergrund sind einer Auslegung der Einwilligungserklärung enge Grenzen gesetzt.[492] Zudem kann die Einwilligung jederzeit widerrufen werden, vgl. Art. 7 Abs. 3. S. 1 DSGVO.

Denkbar wäre auch eine Ermächtigungsgrundlage aus Art. 6 Abs. 1 lit. c DSGVO i.V.m. § 505a BGB. Nach Art. 6 Abs. 1 lit. c DSGVO ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Eine solche rechtliche Verpflichtung könnte in § 505a Abs. 1. S. 1 BGB gesehen werden, wonach bei Verbraucherkrediten der Darlehensgeber vor dem Abschluss eines Verbraucherdarlehensvertrags die Kreditwürdigkeit des Darlehensnehmers zu prüfen hat. Dies beinhaltet zwei Problemfelder. Erstens gilt die Ermächtigungsgrundlage nur für Verbraucherkredite und zweitens dürften nach dem Wortlaut des Art. 6 Abs. 1 lit. c DSGVO nur die Darlehensgeber eine solche Prüfung vornehmen, da nur dieser einer Verpflichtung zur Bonitätsprüfung unterliegt und eben nicht die Auskunftei. Fraglich ist, ob die Sichtweise des EuGH [*Rn. 48*], dass die Kreditentscheidung maßgeblich von dem Score Auskunftei abhängig ist und somit die Auskunftei in den Rechtskreis der Bank einbezogen werden muss, im

[491] *In memoriam Gregor Gysi & Wolfgang Schäuble TEIL1 Minute 53:01 https://www.youtube.com/watch?v=Hqb18EkLWSg*].
[492] *Schulz in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz 3. Auflage 2022 Art. 6 Rn. 23.*

Umkehrschluss Anwendung finden würde. Dann nämlich müsste die Auskunftei auch in den Rechtskreis des § 505a Abs. 1. S. 1 BGB einbezogen werden und somit würde die Ermächtigungsgrundlage auch aus Art. 6 Abs. 1 lit. c DSGVO für die Auskunftei greifen, was angesichts der engen Anwendung des Art. 6 Abs. 1 lit. c DSGVO nicht zu erwarten ist.[493]

Grundsätzlich hätte man die Regelung in § 31 BDSG als eine gelungene Abwägung zwischen den Interessen von betroffenen Personen (Art. 22 DSGVO) und dem Schutzinteresse der Geschäftsgeheimnisse (heute § 2 GeschGehG) der SCHUFA ansehen können. Gerade mit Blick auf die Sicherheit einer Investition in die Entwicklung von Algorithmen besaß der § 31 BDSG Modellcharakter auch für andere Bereiche. Leider lässt der EuGH aber nun erhebliche Zweifel an der Vereinbarkeit mit Art. 22 DSGVO erkennen [*Rn. 25.*][494] und es ist davon auszugehen, dass das VG Wiesbaden dies ebenfalls so sehen wird. Daher ist der deutsche Gesetzgeber dringend aufgefordert, den § 31 BDSG schnellstmöglich zu novellieren und klare und eindeutige Regelungen schaffen. So ließe sich auch der Schutzcharakter der Vorschrift sowohl für die Verwendung von Scoring und Bonitätsauskünften als auch deren Erstellung durch Auskunfteien erhalten. Dem Deutschen Gesetzgeber trifft insoweit auch eine Pflicht zur Novellierung, da Art. 22 Abs. 2 lit. b DSGVO vom Gesetzgeber fordert, dass er angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Personen trifft. Dies waren im wesentlich bereits in § 31 BDSG schon enthalten und sollten auch beibehalten werden, um die Investitionen in KI bei der Berücksichtigung der Rechte der Betroffenen Personen (u.a. aus Art. 15 DSGVO) weiterhin zu gewährleisten. Denn der Art. 22 DSGVO gewährt hierzu den notwendigen Freiraum beide Interessen ausreichend zu berücksichtigen. Um den Regelungscharakter von § 31 BDSG zu erhalten, müsste der Anwendungsbereich der Vorschrift auf Art. 22 Abs. 1 DSGVO verweisen. In seinen Schlussanträgen macht der Generalanwalt nämlich deutlich, dass der § 31 BDSG nicht darüber hinausgehen darf. Somit darf der § 31 BDSG nur für automatisierte Entscheidungen im Sinne von Art. 22 Abs.

[493] *Schulz in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz 3. Auflage 2022 Art. 6 Rn. 23*
[494] *EuGH, 07.12.2023 – C-634/21 vom 7.12.2023*

1 DSGVO gelten. Auch müsste dazu in der Gesetzesbegründung erläutern werden, dass sie eine Ausnahme im Sinne von Art. 22 Abs. 2 Buchstabe b DSGVO darstellen soll. Hierbei sollte die Funktion von § 31 BDSG als Hinweis für die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO im Rahmen der Gesetzesbegründung klargestellt werden. Damit wäre sichergestellt, dass die Vereinbarkeit von § 31 BDSG mit der DSGVO vorliegt und die mit Schutzfunktionen verbundene Vorschrift für das Scoring durch Auskunfteien eine sichere und belastbare Arbeitsgrundlage ist niemand in Frage stellt.

F. KI-Verordnung

Am 13.3.2024 haben die Abgeordneten des EU-Parlaments mit 523 zu 46 Stimmen bei 49 Enthaltungen die KI-Verordnung (Kurzform „KI-VO“ bzw. englisch „AI-Act“) angenommen. Damit setzt die EU den Rahmen für den Einsatz von Künstlicher Intelligenz (KI) in Europa.

I. Überblick über die KI-VO[495]

Die KI-Verordnung[496] ist das weltweit erste umfassende Regelwerk für KI. Sie zielt darauf ab, Innovationen zu fördern, gleichzeitig das Vertrauen in KI zu stärken und sicherzustellen, dass diese Technologie in einer Weise genutzt wird, die die Grundrechte und die Sicherheit der Bürgerinnen und Bürger der EU respektiert.

Die Verordnung wird in der Folge von Rechts- und Sprachsachverständigen abschließend überprüft und kann noch dürfte vor Ende der Wahlperiode i. R. d. sog. Berichtigungsverfahrens angenommen werden. Auch der Rat muss die neuen Vorschriften noch förmlich annehmen. Die Verordnung tritt am 20. Tag nach Veröffentlichung im EU-Amtsblatt in Kraft und findet grundsätzlich 24 Monate später Anwendung. Einige Vorschriften sind aber auch schon früher anwendbar: So greifen die Verbote bereits nach sechs Monaten, die Vorschriften zu KI-Modellen mit allgemeinem Verwendungszweck gelten nach 12 Monaten.

1. Anwendungsbereich und Begriffsbestimmungen

Kap. I Art. 1-4 KI-VO nennen den Gegenstand der Verordnung und den Anwendungsbereich der neuen Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen. Außerdem werden die Begriffe bestimmt, die in diesem Rechtsinstrument durchweg verwendet werden. Ziel der Begriffsbestimmung für KI-Systeme ist es, so technologieneutral und zukunftstauglich wie möglich

[495] *Verabschiedung der europäischen KI-Verordnung – Darstellung wesentlicher Punkte der KI-VO und Kritik* Söbbing, ITRB 2024, 108-111.

[496] Gesetz über künstliche Intelligenz, angenommener Text: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_DE.pdf.

zu sein und den rasanten Entwicklungen in der KI-Technologie und auf dem KI-Markt Rechnung zu tragen.[497]

2. Verbotene Praktiken im KI-Bereich

Kap. II Art. 5 KI-VO enthält eine Liste verbotener KI-Praktiken. Die Verordnung verfolgt einen risikobasierten Ansatz, bei dem zwischen Anwendungen von KI unterschieden wird, die ein i) unannehmbares Risiko, ii) ein hohes Risiko und iii) ein geringes oder minimales Risiko darstellen. Die Aufstellung der verbotenen Praktiken umfasst alle KI-Systeme, die als unannehmbar gelten, weil sie Werte der Union, bspw. Grundrechte, verletzen. Die Verbote gelten für Praktiken, die ein erhebliches Potenzial haben, Personen zu manipulieren, indem sie auf Techniken zur unterschwelligen Beeinflussung zurückgreifen, die von diesen Personen nicht bewusst wahrgenommen werden, oder die die Schwächen bestimmter schutzbedürftiger Gruppen wie Kinder oder Personen mit Behinderungen ausnutzen, um deren Verhalten massiv so zu beeinflussen, dass sie selbst oder eine andere Person psychisch oder physisch geschädigt werden könnten. Andere manipulative oder ausbeuterische Praktiken, die Erwachsene betreffen und möglicherweise durch KI-Systeme erleichtert werden, könnten unter die bestehenden Rechtsvorschriften für den Datenschutz, Verbraucherschutz und digitale Dienste fallen, auf deren Grundlage natürliche Personen Anspruch auf angemessene Informationen haben und es ihnen freisteht, Profiling- oder andere Praktiken, die Einfluss auf ihr Verhalten haben könnten, abzulehnen.[498]

3. Hochrisiko-KI-Systeme

Kap. III enthält spezifische Vorschriften für KI-Systeme, die ein hohes Risiko für die Gesundheit und Sicherheit oder für die Grundrechte natürlicher Personen darstellen. Entsprechend dem risikobasierten Ansatz sind solche Hochrisiko-KI-Systeme auf dem europäischen Markt zugelassen, sofern sie bestimmten zwingend vorgeschriebenen Anforderungen genügen und vorab eine Konformitätsbewertung durchgeführt wird. Die Einstufung als Hochrisiko-KI-System beruht auf der Zweckbestimmung des KI-Systems entsprechend den bestehenden EU-Produktsicherheitsvorschriften.

---

[497] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 14 der KI-VO.

[498] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 15 der KI-VO.

Damit hängt die Einstufung als Hochrisiko-KI-System nicht nur von der Funktion dieses Systems ab, sondern auch von seinem konkreten Zweck und seinen Anwendungsmodalitäten.[499]

a) Einstufung als Hochrisiko-Systeme

In Kap. III Abschn. 1 sind die Einstufungsregeln angegeben und zwei Hauptkategorien für Hochrisiko-KI-Systeme festgelegt:

- KI-Systeme, die als Sicherheitskomponenten von Produkten, die einer Vorab-Konformitätsbewertung durch Dritte unterliegen, verwendet werden sollen;
- sonstige eigenständige KI-Systeme, die ausdrücklich in Anh. III genannt werden und sich vor allem auf die Grundrechte auswirken.

b) Anforderungen an Hochrisiko-KI-Systeme

In Kap. III Abschn. 2 ist festgelegt, welche rechtlichen Anforderungen Hochrisiko-KI-Systeme in Bezug auf Daten, Daten-Governance, Dokumentation und das Führen von Aufzeichnungen, Transparenz und Bereitstellung von Informationen für die Nutzer, menschliche Aufsicht, Robustheit, Genauigkeit und Sicherheit erfüllen müssen. Die vorgeschlagenen Mindestanforderungen, die sich aus den von über 350 Organisationen[500] erprobten Ethik-Leitlinien der HEG[501] ableiten, sind bereits gängige Praxis für viele gewissenhaften Akteure und das Ergebnis der Vorarbeiten der letzten zwei Jahre. Sie stimmen auch weitestgehend mit anderen internationalen Empfehlungen und Grundsätzen überein, wodurch sichergestellt wird, dass der vorgeschlagene KI-Rahmen mit den Vorgaben korrespondiert, die von den internationalen Handelspartnern der EU festgelegt wurden. Es liegt im Ermessen des Anbieters des jeweiligen KI-Systems, mit welchen technischen Lösungen er die Einhaltung dieser Anforderungen konkret erreicht – sei es durch Normen oder sonstige technische

[499] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 15 - 17 der KI-VO.

[500] Sie wurden auch von der Kommission in ihrer Mitteilung aus dem Jahr 2019 zu einem auf den Menschen ausgerichteten Ansatz für KI gebilligt.

[501] Hochrangige Expertengruppe für künstliche Intelligenz, Ethics Guidelines for Trustworthy AI (Ethik-Leitlinien für eine vertrauenswürdige KI), 2019.

Spezifikationen oder durch andere Entwicklungen entsprechend dem allgemeinen wissenschaftlich-technischen Know-how.[502]

4. Transparenzpflichten für bestimmte KI-Systeme

Kap. IV Art. 50 befasst sich mit spezifischen Manipulationsrisiken bestimmter KI-Systeme. Transparenzpflichten gelten für Systeme, die i) mit Menschen interagieren, ii) zur Erkennung von Emotionen oder zur Assoziierung (gesellschaftlicher) Kategorien anhand biometrischer Daten eingesetzt werden oder iii) Inhalte erzeugen oder manipulieren („Deepfakes"). Interagieren Personen mit KI-Systemen oder werden deren Emotionen oder Merkmale durch automatisierte Mittel erkannt, müssen die Menschen hierüber informiert werden. Wird ein KI-System eingesetzt, um Bild-, Audio- oder Video-Inhalte zu erzeugen oder zu manipulieren, sodass sie von authentischen Inhalten kaum zu unterscheiden sind, sollte, abgesehen von legitimen Zwecken (wie Strafverfolgung, Meinungsfreiheit), die Pflicht zur Offenlegung der Tatsache vorgeschrieben werden, dass der Inhalt durch automatisierte Mittel erzeugt wurde. So können bewusste Entscheidungen getroffen oder bestimmte Situationen vermieden werden.[503]

5. KI-Modelle mit allgemeinem Verwendungszeck

In Kap. V wird die Einstufung von KI-Modellen mit allgemeinem Verwendungszweck als KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko vorgenommen. So wird in Art. 51 Abs. 1 ein KI-Modell mit allgemeinem Verwendungszweck als KI-Modell mit systemischem Risiko eingestuft, wenn eine der folgenden Bedingungen erfüllt, ist:

b) Es verfügt über Fähigkeiten mit hohem Wirkungsgrad, die mithilfe geeigneter technischer Instrumente und Methoden, einschließlich Indikatoren und Benchmarks, bewertet werden;

c) einem unter Berücksichtigung der in Anhang XIII festgelegten Kriterien von der Kommission von Amts wegen oder aufgrund einer qualifizierten Warnung des

[502] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 15 - 17 der KI-VO.

[503] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 17 der KI-VO.

wissenschaftlichen Gremiums getroffenen Entscheidung zufolge verfügt es über Fähigkeiten oder eine Wirkung, die denen gemäß Buchstabe a entsprechen.

6. Maßnahmen zur Innovationsförderung

Kap. VI wurde im Hinblick auf das Ziel aufgenommen, einen innovationsfreundlichen, zukunftstauglichen und widerstandsfähigen Rechtsrahmen zu schaffen. Hierzu werden die nationalen zuständigen Behörden aufgefordert, Reallabore einzurichten und die grundlegenden Bedingungen für die Leitung, Aufsicht und Haftung festzulegen. KI-Reallabore bieten, auf der Grundlage eines mit den zuständigen Behörden vereinbarten Testplans, für eine begrenzte Zeit kontrollierte Testumgebungen für innovative Technologien. Kap. VI Art. 62 KI-VO enthält zudem Maßnahmen zur Reduzierung des Verwaltungsaufwands für KMU und Start-ups.[504]

7. Governance

Kap. VII Abschn. 1 enthält Vorgaben für die Leitungsstrukturen auf Unionsebene und nationaler Ebene. Der Vorschlag sieht die Einrichtung **eines Europäischen Ausschusses für künstliche Intelligenz auf** Unionsebene **vor, der sich aus Vertretern der Mitgliedstaaten** und der Kommission zusammensetzt. Der Ausschuss soll zu einer wirksamen Zusammenarbeit der nationalen Aufsichtsbehörden und der Kommission beitragen und so eine reibungslose, wirksame und harmonisierte Durchführung der Verordnung erleichtern und darüber hinaus die Kommission fachlich beraten. Ferner soll der Ausschuss bewährte Verfahrensweisen aus den Mitgliedstaaten sammeln und weitergeben.[505]

Auf nationaler Ebene werden die Mitgliedstaaten eine oder mehrere nationale zuständige Behörden (darunter die **nationale Aufsichtsbehörde**) benennen müssen, die die Anwendung und Durchführung der Verordnung überwachen. Der Europäische Datenschutzbeauftragte gilt als zuständige Behörde für die Aufsicht über die Organe,

[504] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 17 der KI-VO

[505] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 17 der KI-VO

Einrichtungen und sonstigen Stellen der Union, die in den Anwendungsbereich dieser Verordnung fallen.[506]

8. EU-Datenbank für Hochrisikosysteme

Kap. VIII Art. 71 KI-VO soll durch die Einrichtung einer unionsweiten Datenbank für eigenständige Hochrisiko-KI-Systeme, die sich vor allem auf die Grundrechte auswirken, der Kommission und den nationalen Behörden die Beobachtungsaufgaben erleichtern. Die Datenbank wird von der Kommission betrieben. Gespeist wird sie durch die Anbieter der KI-Systeme, die ihre Systeme registrieren müssen, bevor sie sie in Verkehr bringen oder anderweitig in Betrieb nehmen können.

9. Beobachtungs- und Meldepflichten

Kap. IX enthält die Beobachtungs- und Meldepflichten für die Anbieter von KI-Systemen im Hinblick auf die Beobachtung nach dem Inverkehrbringen sowie die Meldung und Untersuchung von Vorfällen und Fehlfunktionen im KI-Zusammenhang. Auch die Marktüberwachungsbehörden werden den Markt kontrollieren und die Einhaltung der mit allen bereits in Verkehr gebrachten Hochrisiko-KI-Systemen verbundenen Pflichten und Anforderungen prüfen. Die Marktüberwachungsbehörden werden mit allen in der Verordnung (EU) 2019/1020 über die Marktüberwachung festgelegten Befugnissen ausgestattet. Die **Ex-post-Durchsetzung** soll sicherstellen, dass öffentliche Behörden über die Befugnisse und Ressourcen verfügen, damit sie eingreifen können, sollten sich bei bereits in Verkehr gebrachten KI-Systemen unerwartete Risiken ergeben, die ein rasches Handeln erfordern. Darüber hinaus werden sie darauf achten, dass die Akteure ihren in der Verordnung festgelegten Pflichten nachkommen. Der Vorschlag sieht nicht die automatische Schaffung weiterer Gremien oder Behörden auf Ebene der Mitgliedstaaten vor. Die Mitgliedstaaten können sich daher auf bereits vorhandene sektorspezifische Behörden und deren Fachkenntnisse stützen, denen die Befugnisse zur Beobachtung und Durchsetzung der Bestimmungen dieser Verordnung übertragen werden.[507]

---

[506] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 18 der KI-VO

[507] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 18 der KI-VO

10. Verhaltenskodizes

Kap. X enthält die Grundlagen zur Schaffung von Verhaltenskodizes, die Anbietern von KI- Systemen, die kein hohes Risiko darstellen, Anreize geben sollen, die zwingend vorgeschriebenen Anforderungen an Hochrisiko-KI-Systeme freiwillig anzuwenden. Anbieter von KI-Systemen, die kein hohes Risiko darstellen, können selbst Verhaltenskodizes festlegen und umsetzen. Diese Kodizes können auch freiwillige Verpflichtungen bspw. im Hinblick auf die ökologische Nachhaltigkeit, den Zugang für Personen mit Behinderungen, die Beteiligung von Interessenträgern an Entwurf und Entwicklung von KI-Systemen sowie die Diversität des Entwicklungsteams enthalten.[508]

11. Befugnisübertragung und Ausschlussverfahren

Kap. XI enthält die Regeln für die Ausübung der Befugnisübertragung und des Ausschlussverfahren. In Art. 97 wird die Befugnis zum Erlass delegierter Rechtsakte der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen und in Art. 98 wird geregelt, dass die Kommission wird einem Ausschuss unterstützt wird. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

12. Sanktionen

Das Kap. XII enthält Regelung bei Verstößen gegen die KI-VO. So sieht ist das höchste Bußgeld in Art. 99 Abs. 3 bei Missachtung des Verbots der in Art. 5 genannten KI-Praktiken vor, das Geldbußen von bis zu 35 000 000 EUR oder – im Falle von Unternehmen – von bis zu 7 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist.

13. Schlussbestimmungen

In Kap. 13 finden sich die Schlussbestimmungen wieder.

[508] Vorschlag für eine Verordnung des europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21.04.2021. S. 18 der KI-VO

II. Transparenzverpflichtungen nach Art. 52 KI-VO

Die Transparenzverpflichtungen für Anbieter und Nutzer von Hochrisiko-KI-Systemen nach Art. 52 der europäischen Verordnung über künstliche Intelligenz (KI-VO) sind von erheblicher Bedeutung für die rechtliche und ethische Nutzung von KI-Systemen. In Art. 52 KI-VO sind umfassende Regelungen zur Transparenz geschaffen worden, die Anbieter von Hochrisiko-KI-Systemen zukünftig berücksichtigen müssen. Diese nicht zu berücksichtigen, könnte für die Anbieter von Hochrisiko-KI-Systemen künftig sehr teuer werden und ist daher von erheblicher Bedeutung für die Zukunft.

1. KI-System

Ein KI-System ist nach Art. 3 Nr. 1 KI-VO ein „*maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen* können". Wesentliches Merkmal eines KI-Systems ist die Fähigkeit, Ausgaben (Outputs) abzuleiten aus den Daten, die es erhalten hat. Die Fähigkeit des Ableitens geht auf das Konzept des maschinellen Lernens sowie auf logik- und wissensgestützte Konzepte zurück.[509]

Die Transparenzverpflichtungen für Anbieter und Nutzer von KI-Systemen nach Art. 52 KI-VO sind wesentlich für die Gewährleistung einer verantwortungsvollen Nutzung von KI-Systemen, die als Hochrisiko-KI-System i. S. v. Art. 6 KI-VO klassifiziert werden. Dabei stellt Art. 52 KI-VO spezifische Anforderungen an die Transparenz, die darauf abzielen, die Nutzer in die Lage zu versetzen, fundierte Entscheidungen über den Einsatz von KI-Systemen zu treffen und potenzielle Risiken zu verstehen.

[509] Erwägungsgrund 12 KI-VO.

2. Hochrisiko-KI-Systeme

Für die Anwendung von Art. 52 KI-VO muss ein Hochrisiko-KI-System i. S. v. Art. 6 KI-VO vorliegen. KI-Systeme werden als Hochrisiko-KI-Systeme qualifiziert, wenn diese nach Art. 6 Abs. 1 lit a und b KI-VO als Sicherheitsbauteil oder als Produkt unter die Harmonisierungsvorschriften der Union fallen oder nach Abs. 2 in den Bereichen in Anhang III, Nr. 1-8 eingesetzt werden. Wenn diese Systeme unter Anwendung des Art. 6 KI-VO fallen, müssen diese eine Konformitätsprüfung durchlaufen, bevor diese auf den Unionsmarkt in Verkehr gebracht werden. Die Konformitätsbewertung untersucht Datengovernance, Risikomanagement, Qualitätsmanagement und weitere Faktoren. Hochrisikosysteme müssen den Anforderungen von Art. 8 ff. KI-VO entsprechen. KI-Systeme, die als Hochrisikosysteme nach Art. 6 Abs. 1 i. V. KI-VO i. V. m. Anhang I, Abschnitt B KI-VO klassifiziert werden, müssen keine Konformitätsbewertung durchlaufen, weil durch die Kohärenz mit den Harmonisierungsvorschriften davon auszugehen ist, dass diese konform sind. Die Europäische Kommission näherte sich schon der Definition der Obligations de conformité et de bonne conduite (OCB) an, was auch die letzte Fassung beherbergt.[510] Mit der neuen Definition aus Art. 3 Nr. 1 KI-VO sollen die Merkmale von KI besser beschrieben werden. Die wesentlichen Merkmale von KI sind der Grad der Autonomie, was eine Selbstständigkeit voraussetzt. Der Aspekt der Autonomie ist nicht das einzige Merkmal, auch die Anpassungsfähigkeit findet in der KI-VO Anwendung. Die eigenständige Entwicklung von KI-Systemen findet über das Maschinenlernen statt[511], das durch Parameteranpassung innerhalb des Systems vorgenommen wird, um den optimalen Output zu generieren.[512] Jedoch sind manche der Auffassung, dass sich der Term „Grad an Autonomie" als problematisch herausstellen könnte, da diese Definition zu weit gefasst sein könnte.[513] Die wichtigsten Normen für die Haftung von KI-Systemen sind die Produkthaftungsrichtlinie, die KI-Verordnung und die KI-Haftungsrichtlinie. Die KI-Haftungsrichtline der EU soll dabei Abhilfe schaffen. Sie

[510] *Bomhard/Siglmüller*, RDi 2024, 45, Rn. 1.
[511] *Heine/Frank*, NZA 2023, S. 1281.
[512] *Görgülü* et al., BKR 2024, S. 175.
[513] *Becker/Feuerstack*, MMR 2024, S. 22.

dient zwar nicht als Haftungsgrundlage, allerdings ist sie dafür erdacht worden, notwendige Informationen nach Art. 3 KI-VO zu erhalten, um eine Kausalität zwischen dem KI-System und einem verursachten Schaden zu bilden,[514] was eine Haftungsgrundlage durch andere Gesetze ermöglichen könnte.[515]

Art. 6 KI-VO regelt die Klassifizierung von KI-Systemen, die als Hochrisikosysteme qualifiziert werden. Die Klassifizierung richtet sich nach der Zweckbestimmung des Systems. Nach Art. 3 Nr. 12 KI-VO ist die Zweckbestimmung[516] die vom Anbieter bestimmte Verwendung. Dabei gelten die besonderen Umstände und Bedingungen für die Verwendung, die der Anbieter in der Betriebsanleitung, in Werbe- und Verkaufsmaterialien sowie in den Informationen der technischen Unterlagen zur Verfügung stellt. Hochriskant ist ein KI-System, wenn es bei der Verwendung Risiken für die Gesundheit, die Sicherheit oder die Grundrechte für natürliche Personen in sich birgt. Bei der Klassifizierung solcher Systeme sind sowohl die Schwere des Schadens als auch die Wahrscheinlichkeit des Auftretens des Schadens zu berücksichtigen, ebenso die Einsatzbereiche, die in der KI-VO vordefiniert sind.[517] Der Art. 6 KI-VO kennt zwei Kategorien, um die Systeme als hochrisikoreich einzustufen:[518] einmal nach Art. 6 Abs. 1 KI-VO und einmal nach Art. 6 Abs. 2 KI-VO.

Die KI-VO folgt den Produktsicherheitsvorschriften des „New Legislative Approach" (kurz NLF). Deshalb qualifiziert auch der erste Abschnitt in Artikel 6 Abs.1 lit. a KI-VO Hochrisikosysteme danach, ob sie als Sicherheitsbauteil eines Produkts innerhalb der in Anhang I KI-VO aufgeführten Harmonisierungsvorschriften verbaut oder ein eigenständiges Produkt in diesem Bereich sind. In Anhang I KI-VO aufgeführte Harmonisierungsvorschriften sind z. B. Richtlinien zur Sicherheit von Spielzeug, zu Sicherheitsbauteile von Aufzügen oder zur persönlichen Schutzausrüstung. Zusätzlich muss nach Art. 6 Abs.1 lit. b KI-VO das eigenständige Produkt oder das Produkt, dessen Sicherheitsbauteil ein KI-System ist, einer Konformitätsbewertung durch Dritte unterzogen werden, bevor es auf dem Unionsmarkt in Umlauf gebracht wird.

---

[514] *Görgülü* et al., BKR 2024, S. 175.
[515] *Staudenmayer*, NJW 2023, S. 894, Rn. 8.
[516] *Baumann/Wirtz*, RDi 2024, S. 27.
[517] Erwägungsgrund 52 KI-VO.
[518] *Geminn*, ZD 2021, S. 354.

Schlüsselbegriff für die Klassifizierung nach Art. 6 Abs. 1 KI-VO ist der Begriff „Sicherheitsbauteil". Dabei definiert auch die KI-VO das Sicherheitsbauteil als einen Bestandteil, der die Sicherheitsfunktionen übernehmen kann, oder als Bestandteil, dessen Ausfall eine Gefahr für die Sicherheit und Gesundheit für natürliche Personen darstellt (gemäß Art. 3 Nr. 14 KI-VO). Aus Erwägungsgrund 52[519] geht hervor, dass auch die Zweckbestimmung eine entscheidende Rolle für die Qualifizierung als Hochrisiko-KI-System darstellt. Wenn KI-Systeme nach der Zweckbestimmung ein hohes Risiko für Gesundheit und Sicherheit bergen, sollen diese auch als hochriskant eingestuft werden. Weiterhin sind sowohl die Wahrscheinlichkeit des Auftretens des Schadens als auch die Schwere der Schadensmöglichkeit relevant. Hier werden in Anhang III KI-VO acht Bereiche aufgelistet. Wenn das KI-System in einem solchen Bereich Verwendung findet, wird es per Definition als Hochrisikosystem angesehen. Die Bereiche decken Berührungspunkte zwischen Mensch und Maschine ab, wo ein Schadenseintritt höchstwahrscheinlich ist.

3. Art. 52 KI-VO

Die Regelung des Art. 52 KI-VO wird in Zukunft für viele KI-Unternehmen eine erhebliche Bedeutung haben.

b) Gesetzestext des Art. 52 der KI-VO

Zunächst einmal besagt der Wortlaut des Art. 52 der KI-VO, der sich mit Transparenzverpflichtungen befasst, Folgendes:

„*Anbieter von Hochrisiko-KI-Systemen stellen sicher, dass die KI-Systeme mit hinreichenden Informationen versehen sind, die eine nachvollziehbare und verständliche Beschreibung der KI-Systeme, ihrer Funktionsweise und ihrer möglichen Auswirkungen für die Nutzer und betroffene Personen enthalten.*

Die Informationen umfassen mindestens:

a. die Identität und den Kontakt des Anbieters;

b. die beabsichtigten Zwecke und Anwendungsbereiche der KI-Systeme;

c. die Art der Daten, die für das Training der KI-Systeme verwendet wurden;

d. die Leistung, Genauigkeit und die Robustheit der KI-Systeme;

[519] Erwägungsgrund 52 KI-VO.

e. die Risiken, die mit der Nutzung der KI-Systeme verbunden sind, sowie die Maßnahmen zu deren Minderung;

f. die Art und Weise, wie die Entscheidungen der KI-Systeme nachprüfbar und interpretierbar sind;

g. die Anforderungen an die Nutzung, einschließlich technischer Anforderungen und der notwendigen Qualifikationen der Nutzer;

h. Informationen über das Verfahren zur Meldung und Behebung von Problemen und Risiken."

Die Erwägungsgründe der KI-VO liefern wichtige Hintergrundinformationen und Erläuterungen zu den Bestimmungen der Verordnung, einschließlich Art. 52 KI-VO. Diese Erwägungsgründe bieten Kontext und klären die Absichten des Gesetzgebers. Zu Art. 52 KI-VO, der Transparenzverpflichtungen betrifft, beinhalten die Erwägungsgründe wesentliche Details, warum Transparenz erforderlich ist und welche Zielsetzungen damit verfolgt werden.

c) Erwägungsgründe

So befasst sich der Erwägungsgrund 70[520] mit der Notwendigkeit, dass Nutzer von Hochrisiko-KI-Systemen angemessen über die Funktionsweise, Risiken und Beschränkungen dieser Systeme informiert sind. Hier wird betont, dass Transparenz eine wesentliche Voraussetzung ist, um Vertrauen in Hochrisiko-KI-Systeme aufzubauen und die verantwortungsvolle Nutzung zu fördern. Die Nutzer sollten in die Lage versetzt werden, fundierte Entscheidungen über den Einsatz der Hochrisiko-KI-Systeme zu treffen und deren potenzielle Auswirkungen zu verstehen.

Der Erwägungsgrund 71[521] erläutert, dass die Bereitstellung klarer und verständlicher Informationen über die Hochrisiko-KI-Systeme dazu beitragen soll, Missverständnisse und Fehlanwendungen zu vermeiden. Dies umfasst unter anderem Informationen über die Trainingsdaten, die Leistung der Systeme sowie die Maßnahmen zur Risikominderung. Die Transparenzverpflichtungen sollen sicherstellen, dass die Nutzer die Grenzen und Fähigkeiten der Hochrisiko-KI-Systeme realistisch einschätzen können.

[520] Erwägungsgrund 70 KI-VO.
[521] Erwägungsgrund 71 KI-VO.

Der Erwägungsgrund 72[522] unterstreicht die Bedeutung der Nachvollziehbarkeit und der Möglichkeit, die Entscheidungen von KI-Systemen zu interpretieren. Dies ist besonders wichtig, um die Fairness und Gerechtigkeit der Entscheidungen zu gewährleisten. Der Erwägungsgrund betont, dass Transparenz nicht nur für die Nutzer, sondern auch für die Aufsichtsbehörden entscheidend ist, um die Einhaltung der Vorschriften zu überwachen und durchzusetzen.

Die Erwägungsgründe verdeutlichen, dass die Transparenzverpflichtungen in Art. 52 KI-VO Teil eines umfassenderen Ansatzes sind, um das Vertrauen in KI-Technologien zu stärken und die ethische und rechtliche Verantwortlichkeit der Anbieter und Nutzer sicherzustellen. Durch die Bereitstellung detaillierter Informationen sollen die Nutzer befähigt werden, die Funktionsweise und die potenziellen Risiken der Hochrisiko-KI-Systeme besser zu verstehen und zu bewerten.

Aufgrund der Betonung der Nachvollziehbarkeit und Verständlichkeit der Informationen wird deutlich, dass Transparenz ein zentraler Faktor für die Akzeptanz von Hochrisiko-KI-Systemen ist. Nutzer müssen darauf vertrauen können, dass die Systeme zuverlässig und sicher sind und dass sie bei Bedarf auf klare und verständliche Informationen zugreifen können.

Die Erwägungsgründe legen nahe, dass Transparenz auch ein Mittel ist, um Risiken proaktiv zu managen und die Verantwortlichkeit der Anbieter zu stärken. Durch die Offenlegung von Informationen über die Trainingsdaten, die Leistung und die Risiken der Hochrisiko-KI-Systeme können potenzielle Probleme frühzeitig identifiziert und angegangen werden.

Die Erwägungsgründe unterstreichen, dass Transparenz auch für die regulatorische Überwachung und Durchsetzung von entscheidender Bedeutung ist. Aufsichtsbehörden benötigen klare und umfassende Informationen, um die Einhaltung der gesetzlichen Vorgaben zu überprüfen und gegebenenfalls Maßnahmen zu ergreifen.

Die Erwägungsgründe zu Art. 52 der KI-VO bieten einen klaren Einblick in die Hintergründe und Ziele der Transparenzverpflichtungen. Sie unterstreichen die

[522] Erwägungsgrund 72 KI-VO.

Notwendigkeit, Vertrauen in KI-Systeme aufzubauen, die informierte Nutzung zu fördern und die Verantwortlichkeit der Anbieter zu stärken. Durch die Bereitstellung klarer und verständlicher Informationen sollen die Nutzer in die Lage versetzt werden, fundierte Entscheidungen zu treffen und potenzielle Risiken besser zu managen. Diese Erwägungsgründe bilden die Grundlage für die detaillierten Anforderungen, die in Art. 52 KI-VO festgelegt sind, und verdeutlichen die umfassenden Ziele der Verordnung zur Gewährleistung einer verantwortungsvollen und transparenten Nutzung von KI-Technologien.

4. Analyse der Transparenzverpflichtungen

Hochrisiko-KI-Systeme müssen nach Art. 52 KI-VO die folgenden Punkte berücksichtigen.

a) Nachvollziehbarkeit und Verständlichkeit

Eine der zentralen Anforderungen ist die Nachvollziehbarkeit und Verständlichkeit der bereitgestellten Informationen. Dies impliziert, dass die Dokumentation und Erläuterungen nicht nur für technisch versierte Nutzer, sondern auch für Laien zugänglich sein müssen. Hierdurch soll sichergestellt werden, dass alle betroffenen Stakeholder, einschließlich Endnutzern und Personen, die durch die Entscheidungen der Hochrisiko-KI-Systeme betroffen sind, die Funktionsweise und potenziellen Auswirkungen verstehen können.

b) Identität und Kontakt des Anbieters

Die Transparenz hinsichtlich der Identität und des Kontakts des Anbieters dient der Verantwortlichkeitszuweisung und ermöglicht eine direkte Kommunikation bei Fragen oder Problemen. Dies fördert das Vertrauen der Nutzer in die Hochrisiko-KI-Systeme.

c) Zwecke und Anwendungsbereiche

Die klare Definition der beabsichtigten Zwecke und Anwendungsbereiche hilft, den Rahmen der Nutzung der Hochrisiko-KI-Systeme zu verstehen und Missbrauch oder Fehlanwendungen zu verhindern.

d) Trainingsdaten

Die Offenlegung der Art der für das Training verwendeten Daten adressiert wichtige ethische und rechtliche Bedenken, beispielsweise Bias und Diskriminierung. Transparenz in Bezug auf die Datenquellen und die Art der Daten kann zur Akzeptanz und zum Vertrauen in die Hochrisiko-KI-Systeme beitragen.

e) Leistung, Genauigkeit und Robustheit

Informationen über die Leistung, Genauigkeit und Robustheit der Hochrisiko-KI-Systeme sind entscheidend, um die Zuverlässigkeit und die Grenzen der Systeme zu bewerten. Dies ermöglicht eine realistische Einschätzung der Fähigkeiten und verhindert überzogene Erwartungen.

f) Risikobewertung und -minderung

Die Identifikation und Kommunikation der mit der Nutzung verbundenen Risiken sowie der Maßnahmen zu deren Minderung sind essenziell, um informierte Entscheidungen zu ermöglichen und eine verantwortungsvolle Nutzung zu gewährleisten. Dies umfasst auch ethische Überlegungen und die Berücksichtigung von Datenschutzaspekten.

g) Nachprüfbarkeit und Interpretierbarkeit

Die Nachprüfbarkeit und Interpretierbarkeit von Entscheidungen der Hochrisiko-KI-Systeme sind besonders wichtig, um die Transparenz und Fairness sicherzustellen. Dies erfordert technologische Lösungen und dokumentierte Verfahren, die eine Überprüfung der Entscheidungsprozesse ermöglichen.

h) Nutzungsvoraussetzungen

Die Darstellung der technischen Anforderungen und der notwendigen Qualifikationen der Nutzer sorgt dafür, dass die Hochrisiko-KI-Systeme nur von Personen genutzt werden, die über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um diese sicher und effektiv einzusetzen.

i) Problem- und Risikomanagement

Ein klar definiertes Verfahren zur Meldung und Behebung von Problemen und Risiken unterstützt eine kontinuierliche Verbesserung und Anpassung der Hochrisiko-KI-Systeme an sich ändernde Rahmenbedingungen und neue Erkenntnisse.

5. Resümee

Die Transparenzverpflichtungen nach Art. 52 KI-VO sind darauf ausgerichtet, die informierte Nutzung von Hochrisiko-KI-Systemen zu fördern, ethische und rechtliche Standards zu gewährleisten und das Vertrauen der Nutzer zu stärken. Für Anbieter und Nutzer von Hochrisiko-KI-Systemen bedeutet dies eine umfangreiche Verpflichtung zur Bereitstellung klarer, verständlicher und umfassender Informationen, um die Verantwortlichkeit, Nachvollziehbarkeit und Sicherheit der Hochrisiko-KI-Systeme zu gewährleisten. Ob diese Maßnahmen unerlässlich sind, um die potenziellen Risiken zu minimieren und die positiven Auswirkungen von KI-Technologien zu maximieren, muss die Zukunft beantworten.

III. Die Vertragsgestaltung im Lichte der KI-VO

Die Künstliche-Intelligenz-Verordnung (KI-VO oder englisch AI-Law) der Europäischen Union, die noch im finalen Abstimmungsprozess steht, soll einen umfassenden rechtlichen Rahmen für den Einsatz von KI-Technologien schaffen. Ein zentraler Aspekt der Verordnung ist Ar. 25 Abs. 4, der besondere Verpflichtungen für Anbieter von KI-Systemen gegenüber ihren Nutzern formuliert. Dieser Artikel adressiert insbesondere die Frage, welche vertraglichen Anforderungen Juristen beim Einsatz von KI-Systemen in Zukunft berücksichtigen müssen.

1. Einleitung

Der risikobasierte Ansatz der KI-Verordnung (KI-Verordnung (Vorschlag der Europäischen Kommission), COM(2021) 206 final), insbesondere in Bezug auf Hochrisiko-KI-Systeme, hat nicht nur Auswirkungen auf den Schutz von Sicherheit, Gesundheit und Grundrechten natürlicher Personen, sondern stellt auch neue Anforderungen an die vertragliche Gestaltung im Verhältnis zwischen Anbietern und Nutzern solcher Systeme. Gemäß Art. 25 Abs. 4 KI-VO sind Anbieter verpflichtet, sicherzustellen, dass Nutzer Hochrisiko-KI-Systeme in Übereinstimmung mit den geltenden rechtlichen Anforderungen einsetzen. Dies führt zu spezifischen vertraglichen Verpflichtungen, die in Nutzungsverträgen festgehalten werden müssen.

Art. 25 KI-VO ist die vertragliche Festlegung des Zwecks der Überlassung eines KI-Systems von entscheidender Bedeutung, um eine klare rechtliche Grundlage für den Einsatz und die Nutzung des KI-Systems zu schaffen. Diese Anforderung zielt darauf ab, die Sicherheit, Transparenz und Rechtmäßigkeit der Nutzung von KI-Systemen zu gewährleisten, insbesondere bei Hochrisiko-KI-Systemen, die erhebliche Auswirkungen auf die Rechte und Freiheiten natürlicher Personen haben können. Es lassen sich mehrere zentrale Gründe aus der KI-VO und allgemeinen rechtlichen Prinzipien ableiten, warum der Zweck der Überlassung eines KI-Systems vertraglich festgelegt werden muss.

Für das Vertragsrecht bedeutet dies, dass Anbieter vertraglich verpflichtet werden, den Nutzern wesentliche Informationen über die Funktionsweise, die Risiken und die Sicherheitsvorkehrungen des KI-Systems bereitzustellen. Zudem müssen Verträge Klauseln zur fortlaufenden Überwachung, Wartung und Aktualisierung der Systeme enthalten, um deren Konformität mit der Verordnung zu gewährleisten. Art. 25 Abs. 4 KI-VO bringt damit eine erhebliche Erweiterung der vertraglichen Pflichten im Bereich der Nutzung von Hochrisiko-KI-Systemen mit sich, vergleichbar mit den datenschutzrechtlichen Verpflichtungen nach der DSGVO. Hierdurch wird eine enge Verbindung zwischen der KI-Verordnung und dem Vertragsrecht hergestellt, die in der Praxis bei der Gestaltung und Auslegung von Verträgen berücksichtigt werden muss.

2. Inhalt und Bedeutung von Art. 25 Abs. 4 KI-VO

a) Grundlagen aus Art. 25 Abs. 4 KI-VO

Art. 25 Abs. 4 KI-VO stellt klar, dass Anbieter von Hochrisiko-KI-Systemen (wie in Anhang III der Verordnung definiert, vgl. *Anhang III der KI-VO (Einstufung von Hochrisiko-KI-Systemen* (Art. 25 Abs. 4 KI-VO (Verpflichtungen des Anbieters in Bezug auf den Nutzer)) gegenüber den Nutzern sicherstellen müssen, dass die Systeme in Übereinstimmung mit den in der Verordnung festgelegten Verpflichtungen betrieben werden. Dabei enthält der Anhang III der KI-Verordnung (KI-VO) eine detaillierte Auflistung von KI-Systemen, die als Hochrisiko-KI-Systeme eingestuft werden und damit besonderen regulatorischen Anforderungen unterliegen. Diese Anforderungen betreffen insbesondere den Einsatz solcher Systeme in Bereichen, die für die Rechte und Freiheiten natürlicher Personen von erheblicher Bedeutung sind, darunter etwa die Sicherheit von kritischen Infrastrukturen, Bildungs- und Ausbildungszwecke, Personalverwaltung, Strafverfolgung und Grenzkontrollen.

Bezogen auf Art. 25 Abs. 4 KI-VO „Verpflichtungen des Anbieters in Bezug auf den Nutzer" ergeben sich aus der Hochrisikoeinstufung nach Anhang III wesentliche Implikationen für die vertragliche Gestaltung zwischen Anbietern und Nutzern von Hochrisiko-KI-Systemen. Insbesondere verpflichtet Art. 25 Abs. 4 die Anbieter solcher Systeme, den Nutzern vertraglich sicherzustellen, dass diese in die Lage versetzt werden, die einschlägigen rechtlichen Verpflichtungen in Bezug auf den sicheren und rechtmäßigen Einsatz der KI-Systeme zu erfüllen.

b) Vertragliche Verpflichtungen gemäß Art. 25 Abs. 4 KI-VO

Transparenz und Information: Der Anbieter muss dem Nutzer im Vertrag umfassende Informationen über die Funktionsweise des KI-Systems bereitstellen. Dies umfasst unter anderem Informationen über die Algorithmen, das Trainingsmaterial, die technischen Parameter und die Leistungsfähigkeit des Systems, sowie über die potenziellen Risiken und Nebenwirkungen, die aus dem Einsatz des Systems resultieren könnten. Diese Transparenzanforderungen sind insbesondere bei Hochrisiko-KI-Systemen von besonderer Bedeutung, um den Nutzer in die Lage zu versetzen, seine eigenen rechtlichen Pflichten, etwa im Bereich des Datenschutzes oder der Produktsicherheit, zu erfüllen.

Pflichten zur laufenden Überwachung und Wartung: Art. 25 Abs. 4 in Verbindung mit den Anforderungen aus Anhang III verpflichtet den Anbieter, vertraglich sicherzustellen, dass der Nutzer Zugang zu allen notwendigen Sicherheitsupdates und technischen Wartungen erhält. Hierbei handelt es sich um fortlaufende Verpflichtungen, die gewährleisten sollen, dass das Hochrisiko-KI-System während seiner gesamten Nutzungsdauer den regulatorischen Anforderungen genügt. Diese Verpflichtung betrifft nicht nur technische Aspekte, sondern auch mögliche Veränderungen in der rechtlichen Bewertung des Systems.

Haftungs- und Risikoverteilung: In Verträgen müssen klare Regelungen zur Haftung für etwaige Schäden getroffen werden, die durch den Einsatz von Hochrisiko-KI-Systemen entstehen könnten. Art. 25 Abs. 4 fordert, dass der Anbieter dem Nutzer vertraglich die Möglichkeit gewährt, Maßnahmen zu ergreifen, falls sich herausstellt, dass das System nicht mehr den geltenden Vorschriften entspricht oder Sicherheitsrisiken birgt. Hierzu gehört insbesondere die Pflicht des Anbieters, den Nutzer unverzüglich über sicherheitsrelevante Vorfälle zu informieren, die im Zusammenhang mit dem Betrieb des KI-Systems stehen.

Mitwirkungsrechte und Kontrolle durch den Nutzer: Der Vertrag muss dem Nutzer des Hochrisiko-KI-Systems Kontrollrechte einräumen, die es ihm ermöglichen, den Einsatz des Systems zu überwachen und gegebenenfalls anzupassen oder zu unterbrechen, falls dies zur Einhaltung gesetzlicher Vorschriften erforderlich ist. Dies bedeutet, dass der Nutzer regelmäßig über die Funktionsweise des KI-Systems informiert werden muss und durch den Anbieter entsprechende Kontrollinstrumente erhalten muss, die ihm eine angemessene Überwachung ermöglichen.

c) Berücksichtigung von Anhang III KI-VO

Die Einstufung von KI-Systemen als Hochrisiko-Systeme nach Anhang III setzt umfangreiche vertragliche Anpassungen voraus. Insbesondere müssen Anbieter von Hochrisiko-KI-Systemen in ihren Verträgen sicherstellen, dass die Nutzer in der Lage sind, die gesetzlichen Anforderungen, die durch die Einstufung als Hochrisiko-System bedingt sind, zu erfüllen. Dazu gehören die Bereitstellung ausreichender

Informationen zur Nutzung und Kontrolle des Systems sowie die Einhaltung von Sicherheits- und Transparenzpflichten.

Juristisch gesehen sind diese vertraglichen Verpflichtungen vergleichbar mit den Pflichten in Auftragsverarbeitungsverträgen nach Art. 28 DSGVO, da sie auf eine umfassende Risikoverteilung und Einhaltung regulatorischer Vorgaben abzielen. Während die DSGVO jedoch den Schutz personenbezogener Daten fokussiert, verlangt die KI-VO zusätzlich zur Wahrung der Grundrechte auch umfassende Sicherheitsvorkehrungen und regelmäßige Kontrolle der technischen Integrität des Systems.

3. Vergleich mit Auftragsverarbeitungsverträgen nach Art. 28 DSGVO

a) Auftragsverarbeitung nach Art. 28 DSGVO

Ein wesentlicher Punkt der DSGVO ist die Auftragsverarbeitung nach Art. 28 i.V.m. Art. 32 DSGVO, diese regelt, unter welchen Bedingungen ein Verantwortlicher Datenverarbeitungen an Dritte auslagern kann. Die dort geforderten Auftragsverarbeitungsverträge (AVV) enthalten strenge Anforderungen an den Auftragsverarbeiter, um sicherzustellen, dass personenbezogene Daten in Übereinstimmung mit den Vorschriften der DSGVO verarbeitet werden.

b) Einige zentrale Elemente eines AVV sind:

- Weisungsgebundenheit: Der Auftragsverarbeiter darf die Daten nur auf Grundlage der dokumentierten Weisungen des Verantwortlichen verarbeiten.
- Datensicherheitsmaßnahmen: Der Auftragsverarbeiter muss geeignete technische und organisatorische Maßnahmen treffen, um den Schutz der personenbezogenen Daten zu gewährleisten.
- Überprüfung und Nachweise: Der Auftragsverarbeiter muss dem Verantwortlichen alle Informationen zur Verfügung stellen, die notwendig sind, um die Einhaltung der Pflichten nachzuweisen.

Während der Fokus eines AVV nach Art. 28 DSGVO auf dem Schutz personenbezogener Daten liegt, geht Art. 25 Abs. 4 KI-VO weiter. Hier sind nicht nur Datenschutzaspekte, sondern auch allgemeine Sicherheits- und Transparenzpflichten für die Funktionsweise von KI-Systemen zu berücksichtigen.

c) Einige zentrale Unterschiede und Parallelen:

Im Vergleich zu den vertraglichen Anforderungen der DSGVO, insbesondere Art. 28 DSGVO (Auftragsverarbeitung), ergeben sich sowohl Parallelen als auch Unterschiede. Art. 28 DSGVO regelt die vertraglichen Pflichten zwischen einem Verantwortlichen und einem Auftragsverarbeiter, wenn personenbezogene Daten im Auftrag verarbeitet werden. Die vertraglichen Anforderungen betreffen hier insbesondere:

- **Weisungsgebundenheit**: Der Auftragsverarbeiter darf personenbezogene Daten nur nach den dokumentierten Weisungen des Verantwortlichen verarbeiten (Art. 28 Abs. 3 lit. a DSGVO).
- **Datensicherheitsmaßnahmen**: Der Auftragsverarbeiter muss geeignete technische und organisatorische Maßnahmen treffen, um den Schutz der Daten zu gewährleisten (Art. 28 Abs. 3 lit. c DSGVO).
- **Prüfungsrechte**: Der Verantwortliche hat das Recht, den Auftragsverarbeiter zu überprüfen, um sicherzustellen, dass die datenschutzrechtlichen Anforderungen eingehalten werden (Art. 28 Abs. 3 lit. h DSGVO).

Diese Anforderungen weisen Parallelen zu den vertraglichen Pflichten nach Art. 25 KI-VO auf, insbesondere in Bezug auf die Transparenz-, Überwachungs- und Prüfpflichten. Auch nach Art. 25 KI-VO muss der Anbieter sicherstellen, dass der Nutzer das KI-System rechtmäßig und sicher verwenden kann und der Nutzer entsprechende Kontrollmöglichkeiten über den Einsatz des Systems erhält.

Art. 25 Abs. 4 KI-VO erweitert die Pflichten von Anbietern im Vergleich zur DSGVO, indem er sicherstellt, dass nicht nur der Schutz personenbezogener Daten, sondern auch die Sicherheit und Transparenz von KI-Systemen gewährleistet wird. Juristen sollten bei der Vertragsgestaltung für KI-Systeme diese erweiterten Anforderungen berücksichtigen, insbesondere hinsichtlich Transparenz, Sicherheit und laufender Haftung. Ein Vergleich zu Art. 28 DSGVO zeigt, dass beide Vorschriften ähnliche Verpflichtungen vorsehen, sich jedoch auf unterschiedliche Schutzziele fokussieren: Der AVV schützt personenbezogene Daten, während Art. 25 Abs. 4 KI-VO ein umfassenderes Sicherheits- und Kontrollregime für den Einsatz von KI-

Systemen vorschreibt. Ein Vergleich zwischen Art. 25 Abs. 4 KI-VO und Art. 28 DSGVO erscheint sinnvoll und ergibt folgende Punkte:

- **Informationspflichten**: Beide Normen verpflichten den Anbieter bzw. Auftragsverarbeiter, wesentliche Informationen bereitzustellen. Während es im AVV um Datenverarbeitung geht, fokussiert Art. 25 Abs. 4 KI-VO auf die Funktionsweise und die Risiken des KI-Systems.
- **Sicherheitsverpflichtungen**: In beiden Fällen muss der Anbieter/Verarbeiter technische und organisatorische Maßnahmen ergreifen. In der KI-VO beziehen sich diese jedoch nicht nur auf den Datenschutz, sondern auch auf die Sicherheit der KI-Anwendung insgesamt.
- **Kontrollmöglichkeiten**: Sowohl Art. 28 DSGVO als auch Art. 25 Abs. 4 KI-VO fordern, dass der Nutzer bzw. Verantwortliche Kontrollmöglichkeiten hat. In der KI-VO sind diese auf die Kontrolle über die Nutzung des KI-Systems ausgeweitet.

4. Vertragsgestaltung für KI-Systeme

Folgende Punkte kann als Checkliste bei der Vertragsgestaltung für KI-Systeme gesehen werden, welche aber natürlich nicht abschließend ist.

a) Generelle Anforderungen

Juristen, die Verträge für den Einsatz von Hochrisiko-KI-Systemen gestalten, sollten die folgenden Punkte berücksichtigen:

- **Transparenzklauseln**: Ähnlich wie in einem AVV sollte der Anbieter verpflichtet werden, detaillierte Informationen zur Funktionsweise und den Sicherheitsrisiken des KI-Systems bereitzustellen.
- **Regelungen zur Haftung und Risikoverteilung**: Da Hochrisiko-KI-Systeme potenziell schwerwiegende Folgen haben können, sollten klare Haftungsklauseln aufgenommen werden, die etwaige Fehlfunktionen oder Datenschutzverletzungen abdecken.
- **Fortlaufende Sicherheits- und Updatepflichten:** Anbieter sollten verpflichtet werden, regelmäßig Updates und Patches bereitzustellen, um Sicherheitslücken zu schließen und die ordnungsgemäße Funktion des KI-Systems zu gewährleisten.

- **Kontrollmöglichkeiten des Nutzers:** Nutzer sollten vertraglich das Recht haben, den Einsatz des KI-Systems zu überwachen und bei Bedarf Maßnahmen zu ergreifen, um den Einsatz zu beschränken oder zu beenden, wenn Sicherheitsrisiken festgestellt werden.

b) Anbieter von KI-Systemen

Ist der Vertragsgestalter auf der Anbieterseite von KI-Systemen tätig so sollte er auch darauf achten welche Verpflichtungen er von seinem Subunternehmer verlangen muss, selbst wenn diese selbst keine KI-Systeme i. S. d. Art. 6 KI-VO „Hochrisikosysteme" liefern, so wie z.B. klassische IT-Anbieter.

(1) Auf der Seite der Beschaffung

Hierbei sind auf der Beschaffungsseite folgende Anforderungen nach Art. 25 KI-VO zu beachten:

- Informationen, um die eigenen Anforderungen zum Risikomanagement zu erfüllen, vgl. Art. 9 KI-VO.
- Informationen, um die eigenen Anforderungen zum Qualitätsmanagement zu erfüllen, vgl. Art. 17 KI-VO.
- Technische Informationen und Dokumentationen, um die eigenen Anforderungen zu erfüllen, vgl. Art. 11 KI-VO sowie die Nachvollziehbarkeit und Transparenz, vgl. Art. 13 KI-VO.
- Anforderungen bei einem Dauerhaften Leistungsbezug, wie z.B. Aktualisierungspflichten für:
  - Aktualisierung der technischen Dokumentation, vgl. Art. 11 KI-VO.
  - Fortlaufende Überwachung und Wartung, vgl. Art. 23 KI-VO
  - Meldung wesentlicher Änderungen, vgl. Art. 43 KI-VO.
  - Post-Marketing-Überwachung und Rückmeldungen, vgl. Art. 61 KI-VO.
  - Notwendigkeit eines Konformitätsbewertungsverfahrens bei wesentlichen Änderungen, vgl. Art. 43 KI-VO.
  - Haftung, Kosten, etc.

(2) Auf der Seite des Vertriebes

Auf der Vertriebsseite sind insbesondere folgende Anforderungen nach Art. 25 KI-VO zu beachten:

- Festlegung des Zwecks der Überlassung Beschreibung des KI-Systems, vgl. Art. 6 und Art. 25 Abs. 2 KI-VO:
  - Zur Vermeidung von Zweckentfremdung und Missbrauch
  - Begrenzung der Nutzung auf den festgelegten Zweck
- Einhaltung regulatorischer Vorgaben durch die Zweckbindung
- Transparenz und Nachvollziehbarkeit des Einsatzes
- Risikomanagement und Haftungsverteilung
- Erfüllung der Anforderungen der Aufsichtsbehörden
- Haftungsbeschränkung

c) Betreiber von KI-Systemen

Auf der Seite der Betreiber von KI-Systemen können folgende Punkte relevant für die Vertragsgestaltung sein:

(1) Beschaffung bei Eigennutzung

- Vertragliche Festlegung des Verwendungszwecks, vgl. Art. 6 und Art. 25 Abs. 2 KI-VO
- Gewährleistung der Konformität mit der KI-VO, vgl. Art. 9 bis Art. 15 KI-VO.
- Der Anbieter muss vertraglich zusichern, dass das KI-System den notwendigen Konformitätsbewertungsverfahren nach Art. 43 KI-VO unterzogen wurde und entsprechende Zertifizierungen oder Nachweise vorliegen.
- Technische Dokumentation und Informationspflichten, vgl. Art. 11 KI-VO
- Wartung, Updates und Sicherheitsmaßnahmen, vgl. Art. 23 KI-VO
- Haftung und Gewährleistung, Art. 25 Abs. 2 KI-VO; §§ 434 ff. BGB (Mängelhaftung)
- Sicherstellung der Compliance und Prüfungsrechte, vgl. Art. 23 und Art. 25 Abs. 2 KI-VO
- Datenschutz und DSGVO-Konformität, vgl. Art. 25 Abs. 2 KI-VO

(2) Beschaffung mit Anpassungen

- Anforderungen nach Art. 25 Abs. 1 KI-VO
  - Einrichtung eines Qualitätssicherungssystems
  - Dokumentation des Qualitätssicherungssystems
  - Anforderungen an das Risikomanagementsystem
  - Überprüfung und Validierung des KI-Systems
  - Transparenzanforderungen und Informationspflichten
- Wenn wesentliche Änderungen i.S.v. Art. 25 Abs. 2 lit. b oder lit. c. KI-VO vorgenommen werden:
- Gegenstand und Zweckfestlegung
  - Ausschluss des Hochrisiko-KI-System prüfen, vgl. Art. 25 Abs. 2 S. 3 KI-VO
  - Pflichtenprogramm ggü. Lieferkette anfordern (siehe oben IV. Nr. 2 lit. a)
- Kontinuierliche Informationspflichten
- Unterstützungsleistungen
- Ggf. Lizenzvertrag über IT/KI-System

5. Resümee

Die KI-VO der EU setzt einen regulatorischen Rahmen, der weitreichende Auswirkungen auf die Vertragsgestaltung im Bereich des Einsatzes von Hochrisiko-KI-Systemen hat. Ein Vergleich mit den vertraglichen Anforderungen der Datenschutz-Grundverordnung (DSGVO), insbesondere Art. 28 DSGVO, zeigt sowohl Parallelen als auch Unterschiede auf, die im Rahmen der Vertragsgestaltung Berücksichtigung finden müssen.

Die Anforderungen der KI-VO, insbesondere nach Art. 25, setzen hohe Maßstäbe an die Vertragsgestaltung für Anbieter von Hochrisiko-KI-Systemen. Die Pflichten zur Implementierung von Qualitätssicherungs- und Risikomanagementsystemen, zur Transparenz gegenüber den Nutzern sowie zur Haftung und Risikoverteilung sind zentrale Elemente der vertraglichen Regelungen. Im Vergleich zu den vertraglichen Anforderungen der DSGVO nach Art. 28 zeigen sich deutliche Parallelen,

insbesondere in Bezug auf Transparenz- und Überwachungspflichten, jedoch bestehen auch wesentliche Unterschiede in der Zielsetzung und der Breite der zu berücksichtigenden Risiken. Während Art. 28 DSGVO den Schutz personenbezogener Daten in den Fokus rückt, adressiert Art. 25 KI-VO umfassend die Sicherheit, Zuverlässigkeit und Risikominimierung bei der Nutzung von KI-Systemen, die potenziell erhebliche Auswirkungen auf die Rechte und Freiheiten natürlicher Personen haben können.

Auf die vertragsgestaltenden Parteien kommt einiges zu und die Umsetzung in die Verträge wird sicherlich umfassend sein.

IV. Qualitätsmanagement gem. KI-VO

Mit der Einführung der EU-KI-Verordnung (KI-VO) stellt sich auch die Frage, welche Anforderungen Unternehmen, die KI verwenden, im Bereich des Qualitätsmanagements erfüllen müssen. Die zentrale Norm hierfür ist Art. 17 KI-VO, die konkrete Anforderungen an das Qualitätsmanagement für Hochrisiko-KI-Systeme enthält. Im Bereich des Qualitäts- und Risikomanagements existieren bereits etablierte internationale Normen, insbesondere die ISO 42001 als spezifische Norm für KI-Managementsysteme, die ISO 9001 als allgemeiner Standard für Qualitätsmanagementsysteme sowie die ISO 27001 für Informationssicherheitsmanagementsysteme. Der folgende Abschnitt geht der Frage nach, ob die Befolgung dieser Standards auch ausreichend ist, um die Anforderung nach Art. 17 KI-VO zu erfüllen.[523]

1. Einleitung

Die rasante Entwicklung von Systemen der Künstlichen Intelligenz (KI) und deren zunehmender Einsatz in sicherheitskritischen und gesellschaftlich relevanten Bereichen stellt sowohl die Wirtschaft als auch die Gesetzgeber vor erhebliche Herausforderungen. Insbesondere sogenannte Hochrisiko-KI-Systeme, etwa in der medizinischen Diagnostik, in sicherheitsrelevanten Infrastrukturen oder im Bereich der Beschäftigung, können erhebliche Auswirkungen auf Leben und Rechte von Menschen haben. Vor diesem Hintergrund hat die Europäische Union mit der KI-

[523] Siehe auch *Söbbing* RDi 2025, S. 337 ff.

Verordnung (KI-VO)[524]einen regulatorischen Rahmen geschaffen, der den sicheren und vertrauenswürdigen Einsatz solcher Systeme gewährleisten soll.

Ein zentrales Element dieser Verordnung bildet Art. 17 KI-VO, der die Anbieter hochriskanter KI-Systeme zur Einrichtung und Aufrechterhaltung eines Qualitäts- und Risikomanagementsystems verpflichtet. Ziel ist es, die kontinuierliche Compliance mit den rechtlichen Anforderungen sowie die effektive Risikominimierung über den gesamten Lebenszyklus der KI-Systeme hinweg sicherzustellen. Damit rückt die Frage in den Fokus, wie diese regulatorischen Anforderungen praktisch umgesetzt werden können.[525]

Im Bereich des Qualitäts- und Risikomanagements existieren bereits etablierte internationale Normen, insbesondere die ISO 42001[526] als spezifische Norm für KI-Managementsysteme, die ISO 9001 als allgemeiner Standard für Qualitätsmanagementsysteme sowie die ISO 27001 für Informationssicherheitsmanagementsysteme. Diese Normen bieten strukturierte Vorgehensweisen, um Managementsysteme zu planen, umzusetzen, zu überwachen und kontinuierlich zu verbessern. Dabei stellt sich die Frage, inwieweit diese Normen geeignet sind, die Anforderungen aus Art. 17 KI-VO zu erfüllen oder zumindest zu flankieren. Ziel der Betrachtungen ist es, die Anforderungen des Art. 17 KI-VO detailliert darzustellen, deren praktische Umsetzungsmöglichkeiten im Rahmen der genannten ISO-Normen zu analysieren und aus juristischer Sicht zu bewerten, ob eine Zertifizierung nach diesen Normen als Nachweis für die Erfüllung der gesetzlichen Pflichten ausreicht. Besonderes Augenmerk wird dabei auf die Schnittstellen und möglichen Lücken („Gaps“) zwischen den regulatorischen Anforderungen und den Normvorgaben gelegt.

[524] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828.

[525] Wendt/Wendt Das neue Recht der künstlichen Intelligenz, 1. Aufl. 2024, § 6 Rn. 6 f.

[526] Autor: ISO Technical Committee JTC 1/SC 42, abrufbar unter https://www.iso.org/news/ref2865.html.

2. Die Anforderungen des Art. 17 KI-VO im Überblick

a) Zielsetzung und Systematik

Der europäische Gesetzgeber verfolgt mit Art. 17 KI-VO das Ziel, sicherzustellen, dass Anbieter hochriskanter KI-Systeme über geeignete interne Strukturen und Prozesse verfügen, um die Konformität ihrer Systeme während des gesamten Lebenszyklus zu gewährleisten.[527] Die Vorschrift stellt damit eine Konkretisierung des allgemeinen Konformitätsbewertungsregimes der KI-VO dar und bildet eine Brücke zwischen dem produktspezifischen Risikomanagement und dem organisatorischen Qualitätsmanagement.[528] Während Art. 9 KI-VO das Risikomanagement auf der Ebene des einzelnen KI-Systems regelt, adressiert Art. 17 die dahinterliegende betriebliche Organisation und deren Fähigkeit, Risikomanagementprozesse effektiv zu steuern und zu dokumentieren. Zur Gewährleistung der Konformität der KI-Systeme mit den Anforderungen dieser Verordnung sollten Anbieter von Hochrisiko-KI-Systemen ein Qualitätsmanagementsystem einrichten, das als Teil ihrer internen Governance-Struktur fungiert. Dieses System sollte Verfahren zur Umsetzung der in dieser Verordnung vorgesehenen Anforderungen enthalten.[529]

Die Vorschrift verlangt somit die Einführung, Dokumentation und kontinuierliche Aufrechterhaltung eines Qualitätsmanagementsystems, das geeignet ist, sämtliche Anforderungen der KI-VO – insbesondere in Bezug auf Risikominimierung, Transparenz, Datenqualität und menschliche Aufsicht – systematisch zu adressieren.[530] Damit nimmt Art. 17 eine zentrale Rolle bei der Operationalisierung der regulatorischen Vorgaben ein und hebt die Bedeutung eines strukturierten Managementsystems für die Compliance hervor.[531]

[527] Art. 17 I KI-VO; BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 3.
[528] Wendt/Wendt Das neue Recht der künstlichen Intelligenz, 1. Aufl. 2024, § 6 Rn. 6 f.
[529] KI-VO ErwGr. 48 – Zweck des Qualitätsmanagementsystems.
[530] KI-VO ErwGr. 48 – Zweck des Qualitätsmanagementsystems.
[531] Martini/Wendehorst/Eisenberger, 1. Aufl. 2024, KI-VO Art. 16 Rn. 21.

b) Pflicht zur Einführung eines Qualitäts- und Risikomanagementsystems

Art. 17 KI-VO verpflichtet Anbieter hochriskanter KI-Systeme zur Einführung, Dokumentation und Aufrechterhaltung eines Qualitäts- und Risikomanagementsystems. Diese Verpflichtung ist nicht optional, sondern zwingend ausgestaltet und stellt eine Grundvoraussetzung für die Inverkehrbringung sowie das Inbetriebhalten solcher Systeme dar.[532] Die Norm adressiert damit die organisatorische Sorgfaltspflicht der Anbieter und verlangt, dass nicht nur das Produkt selbst konform ist, sondern auch die zugrunde liegenden betrieblichen Strukturen geeignet sind, um eine dauerhafte Einhaltung der Verordnung sicherzustellen.[533]

Dabei ist zu beachten, dass die KI-VO einen Lebenszyklusansatz verfolgt. Dies bedeutet, dass das Managementsystem alle Phasen des KI-Systems abdecken muss – von der Konzeption über die Entwicklung und Validierung bis hin zur Nutzung, Wartung und gegebenenfalls Außerbetriebnahme.[534] Die Implementierung eines solchen Systems erfordert eine systematische Planung, klare Verantwortlichkeiten, dokumentierte Prozesse und wirksame Kontrollmechanismen, vgl. Art. 17 II KI-VO.

c) Mindestanforderungen an das Managementsystem

Art. 17 II KI-VO konkretisiert die Mindestinhalte des geforderten Managementsystems und nennt dabei explizit folgende Elemente:

- Festlegung einer Strategie zur Einhaltung der rechtlichen Anforderungen,
- Verfahren zur Risikobewertung und -minderung,
- Mechanismen zur Überwachung und Bewertung der Leistung des KI-Systems,
- Dokumentation aller relevanten Prozesse und Maßnahmen,
- Verfahren zur Aufrechterhaltung der Compliance über den gesamten Lebenszyklus.

Diese Anforderungen sind eng mit den Grundsätzen des Qualitätsmanagements verbunden, wie sie etwa in der ISO 9001 niedergelegt sind.[535] Insbesondere das Prinzip des „Plan-Do-Check-Act"-Zyklus (PDCA-Zyklus) spiegelt sich in der Systematik des

[532] Art. 17 I KI-VO; BeckOK KI-Recht/ Henke, KI-VO Art. 17 Rn. 3.
[533] KI-VO ErwGr. 48 – Zweck des Qualitätsmanagementsystems.
[534] BeckOK KI-Recht/ Henke, KI-VO Art. 17 Rn. 4.
[535] ISO 9001:2015, Abschnitt 4 ff.

Art. 17 KI-VO wider.[536] Es ist daher naheliegend, auf bestehende QM-Standards zurückzugreifen, um die Anforderungen der Verordnung in ein funktionierendes Managementsystem zu überführen.

Zugleich geht die KI-VO über die klassischen Qualitätsmanagementaspekte hinaus. Beispielsweise verlangt sie im Bereich der KI-spezifischen Risiken besondere Maßnahmen zur Gewährleistung der Datenqualität, zur Minimierung von Bias[537] und zur Sicherstellung menschlicher Aufsicht, die in allgemeinen QM-Normen bislang nur randständig behandelt werden.[538]

3. Verhältnis zu anderen regulatorischen Pflichten (insbesondere zu Art. 9 KI-VO – Risikomanagement)

Ein zentrales Merkmal des Art. 17 KI-VO ist seine enge Verzahnung mit Art. 9 KI-VO. Während Art. 9 die konkrete Risikobewertung und -minderung für das jeweilige KI-System vorschreibt, stellt Art. 17 die organisatorischen Rahmenbedingungen bereit, um diese Anforderungen systematisch umzusetzen. Das Risikomanagementsystem nach Art. 9 ist damit ein Bestandteil des übergeordneten Qualitätsmanagementsystems im Sinne des Art. 17.[539]

Dies zeigt sich beispielsweise darin, dass Art. 17 ausdrücklich verlangt, Verfahren zur Durchführung und Dokumentation von Risikobewertungen vorzuhalten. Damit wird ein integrativer Ansatz verfolgt, der nicht nur auf ad hoc durchgeführte Risikoprüfungen setzt, sondern auf eine strukturierte und wiederholbare Einbettung des Risikomanagements in die Unternehmensprozesse.[540]

Eine Parallele hierzu besteht im Produktsicherheitsrecht, etwa im Medizinprodukterecht oder in der Maschinenrichtlinie, wo ebenfalls zwischen produktspezifischen

[536] Der „Plan-Do-Check-Act"-Zyklus (PDCA-Zyklus) ist ein iteratives Managementmodell zur kontinuierlichen Verbesserung von Prozessen und Systemen, insbesondere im Rahmen von Qualitätsmanagementsystemen. Er ist zentraler Bestandteil vieler Normen, insbesondere der ISO 9001, ISO 14001 und auch der ISO/IEC 42001:2023, abrufbar unter https://www.iso.org/standard/62085.html.

[537] Die Verzerrung oder auch das Bias oder systematischer Fehler einer Schätzfunktion ist in der Schätztheorie, einem Teilgebiet der mathematischen Statistik, diejenige Kennzahl oder Eigenschaft einer Schätzfunktion, welche die systematische Über- oder Unterschätzung der Schätzfunktion quantifiziert, vgl. Georgii Stochastik, 2009, S. 207.

[538] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 5

[539] Wendt/Wendt Das neue Recht der künstlichen Intelligenz, 1. Aufl. 2024, § 6 Rn. 6 f.

[540] Art. 17 II Buchst. b KI-VO.

Risikobewertungen und den Anforderungen an das Qualitätsmanagementsystem der Hersteller unterschieden wird.[541]

Die KI-VO greift diese Logik auf und überträgt sie auf den Bereich der künstlichen Intelligenz, wobei der Fokus nicht nur auf physischen Gefahren, sondern auch auf algorithmischen Risiken liegt. Dazu zählen insbesondere Probleme wie Diskriminierung durch fehlerhafte Trainingsdaten, Intransparenz algorithmischer Entscheidungen (Black-Box-Problematik) sowie fehlende menschliche Kontrolle.[542]

Diese Besonderheiten machen es erforderlich, dass das Qualitätsmanagementsystem spezifische Maßnahmen zur Risikoerkennung und -minderung für KI-Systeme enthält, die über die allgemeinen Anforderungen herkömmlicher QM-Standards hinausgehen.

4. ISO 42001:2023 – AI Management System

a) Struktur und Zielsetzung der Norm

Mit der Veröffentlichung der ISO 42001 im Dezember 2023 liegt erstmals ein international anerkannter Standard für ein Managementsystem vor, das speziell auf den Einsatz von Künstlicher Intelligenz ausgerichtet ist.[543] Die Norm versteht sich als Leitfaden für Organisationen, die KI-Systeme entwickeln, bereitstellen oder betreiben, und zielt darauf ab, ein systematisches Rahmenwerk zur Steuerung und Kontrolle von KI-bezogenen Risiken zu schaffen. Ihre Struktur orientiert sich an der sogenannten High Level Structure (HLS), die eine einheitliche Grundstruktur für Managementsystemnormen der ISO darstellt und bereits in der ISO 9001 sowie der ISO 27001 Anwendung findet.[544]

Das übergeordnete Ziel der ISO 42001 ist es, Organisationen dabei zu unterstützen, KI-Systeme verantwortungsvoll, sicher und gesetzeskonform zu betreiben. Hierzu definiert die Norm Anforderungen an die Implementierung eines AI Management Systems (AIMS), das alle relevanten Aspekte des Lebenszyklus von KI-Systemen

[541] Vgl. zB § 30 MPG aF, Art. 10 MDR (EU) 2017/745.
[542] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 5.
[543] ISO 42001:2023, Introduction.
[544] ISO 42001:2023, Introduction; vgl. auch ISO 9001:2015 und ISO 27001:2022, Einleitung.

abdeckt, einschließlich Planung, Implementierung, Überwachung, Bewertung und Verbesserung.[545]

b) Anforderungen an Planung, Umsetzung, Monitoring und kontinuierliche Verbesserung

Die ISO 42001 verlangt von Organisationen die Festlegung einer KI-spezifischen Politik, die auf die Einhaltung gesetzlicher und regulatorischer Vorgaben sowie ethischer Grundsätze ausgerichtet ist. Dabei betont die Norm ausdrücklich die Notwendigkeit einer Risikoanalyse, die sowohl technische als auch ethische und soziale Aspekte umfasst.[546]

Konkret enthält die Norm Anforderungen an folgende Elemente:

- Definition der KI-bezogenen Ziele und Verpflichtungen,
- Risikoidentifikation und -bewertung hinsichtlich der Entwicklung und Anwendung von KI-Systemen,
- Festlegung angemessener Kontrollen und Maßnahmen zur Risikobehandlung,
- Durchführung interner Audits zur Überprüfung der Systemwirksamkeit,
- Management-Reviews zur systematischen Bewertung der Leistung des AIMS,
- Implementierung von Maßnahmen zur kontinuierlichen Verbesserung.

Der PDCA-Zyklus bildet dabei das methodische Rückgrat der Norm. Die Planung („Plan“) umfasst die Definition von Zielen und Prozessen, die Durchführung („Do“) bezieht sich auf die Umsetzung der geplanten Maßnahmen, die Überprüfung („Check“) erfolgt über Monitoring und interne Audits, und die Verbesserung („Act“) umfasst die Ableitung und Umsetzung von Optimierungsmaßnahmen aus den Ergebnissen der Überprüfung.[547]

Ein besonderer Fokus der ISO 42001 liegt auf der Berücksichtigung von sogenannten Impact Assessments, die eine Bewertung potenzieller Auswirkungen eines KI-Systems auf Betroffene, Gesellschaft und Umwelt vorsehen. Damit knüpft die Norm an international geführte Diskurse zur menschenzentrierten KI an und unterstützt

[545] ISO/IEC 42001:2023, Managementsysteme für künstliche Intelligenz. Verweist mehrfach auf den PDCA-Zyklus als konzeptionelle Grundlage, abrufbar unter https://www.iso.org/standard/81230.html.
[546] ISO 42001:2023, Abschnitt 4 ff.
[547] ISO 42001:2023, Abschnitt 4 ff.; zum PDCA-Zyklus vgl. auch ISO 9001:2015, Anhang A.

Anbieter dabei, über die rein technische Perspektive hinausgehende Risiken zu adressieren.[548]

c) Konformitätspotential zu Art. 17 KI-VO

in Bezug auf die Anforderungen des Art. 17 KI-VO weist die ISO 42001 eine hohe Kompatibilität auf. Insbesondere die systematische Verankerung von Risikomanagementprozessen, die Dokumentationspflichten und die Pflicht zur kontinuierlichen Überprüfung und Verbesserung decken sich mit den Mindestanforderungen der Verordnung. Dies betrifft insbesondere die Anforderungen an:

- Lebenszyklusorientiertes Risikomanagement,
- Festlegung klarer Verantwortlichkeiten und Zuständigkeiten,
- Dokumentation und Nachvollziehbarkeit der Entscheidungsfindung,
- Monitoring und Anpassung bei veränderten Rahmenbedingungen.

Allerdings bleibt festzuhalten, dass auch die ISO 42001 kein unmittelbares regulatorisches Konformitätsversprechen in Bezug auf die KI-VO abgibt. Die Norm stellt vielmehr ein flexibles Rahmenwerk zur Verfügung, das von den Anwendern entsprechend angepasst und konkretisiert werden muss, um die spezifischen Anforderungen des europäischen Rechtsrahmens – etwa hinsichtlich Bias Detection, Transparenz und Human Oversight – vollständig abzubilden.[549]

Gleichwohl ist die ISO 42001 aufgrund ihres dezidierten KI-Fokus und ihrer systematischen Ausrichtung auf Risikomanagement und Compliance ein geeignetes Instrument, um die Anforderungen des Art. 17 KI-VO zumindest weitgehend operativ umzusetzen und zu flankieren. Eine vollständige Compliance-Prüfung erfordert jedoch in jedem Fall eine ergänzende rechtliche Bewertung und gegebenenfalls zusätzliche Maßnahmen außerhalb des Rahmens der Norm.

[548] ISO 42001:2023, Abschnitt 6.1.3.
[549] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 6

5. ISO 9001:2015 – Qualitätsmanagementsysteme

a) Grundlagen und Anwendungsbereich

Die ISO 9001:2015 stellt den weltweit am weitesten verbreiteten Standard für Qualitätsmanagementsysteme (QMS) dar. Ihr Ziel ist es, Organisationen bei der Fähigkeit zu unterstützen, konsistent Produkte und Dienstleistungen bereitzustellen, die den Anforderungen der Kunden sowie anwendbaren rechtlichen und regulatorischen Anforderungen entsprechen.[550] Die Norm folgt einem prozessorientierten Ansatz und basiert auf den Grundsätzen des Qualitätsmanagements, darunter Kundenorientierung, Führung, Engagement von Personen, prozessorientierter Ansatz, Verbesserung, faktengestützte Entscheidungsfindung sowie Beziehungsmanagement.[551]

Die Norm richtet sich nicht an spezifische Branchen oder Produkttypen, sondern ist branchenübergreifend anwendbar und flexibel ausgestaltbar. Ihre Hauptstärke liegt in der Standardisierung betrieblicher Abläufe und in der systematischen Verankerung von Qualitätssicherung über alle Prozesse hinweg.

b) Relevanz für die Qualitätsanforderungen aus Art. 17 KI-VO

Obwohl die ISO 9001 keinen spezifischen Bezug zu KI-Systemen oder algorithmischen Risiken enthält, bietet sie ein solides Grundgerüst für das Qualitätsmanagement, das auch für die Umsetzung von Art. 17 KI-VO genutzt werden kann. Besonders relevant sind dabei die folgenden Aspekte:

- die Definition des Anwendungsbereichs des Managementsystems (ISO 9001:2015, Abschnitt 4),
- die Verpflichtung zur Führung und zur Festlegung von Rollen, Verantwortlichkeiten und Befugnissen (Abschnitt 5),
- das Risikobasierte Denken im Rahmen der Planung (Abschnitt 6),
- die operative Steuerung und die Anforderung an dokumentierte Informationen (Abschnitt 8),
- sowie das Monitoring, die Bewertung und die kontinuierliche Verbesserung (Abschnitte 9 und 10).

[550] ISO 9001:2015, Introduction.
[551] ISO 9001:2015, Anhang B.

Diese Elemente entsprechen in ihrer Zielrichtung weitgehend den strukturellen Anforderungen, wie sie Art. 17 KI-VO für das Qualitätsmanagement bei hochriskanten KI-Systemen fordert, auch wenn sie KI-spezifische Problemstellungen wie Bias Detection oder Transparenz nicht ausdrücklich adressieren.[552]

Besondere Bedeutung hat das in ISO 9001 verankerte Prinzip des risikobasierten Denkens, das verlangt, dass Organisationen Risiken und Chancen, die die Zielerreichung des Qualitätsmanagementsystems beeinflussen können, identifizieren und angemessene Maßnahmen festlegen.[553] Diese Verpflichtung lässt sich als methodische Grundlage nutzen, um auch KI-spezifische Risiken in das Qualitätsmanagementsystem einzubetten.

c) Stärken und Grenzen der ISO 9001 im Kontext KI

Die wesentliche Stärke der ISO 9001 liegt in ihrer universellen Anwendbarkeit und in der etablierten Methodik zur Prozessgestaltung und -verbesserung. Dies erleichtert es, Prozesse zur Risikobewertung und -minderung sowie zur Dokumentation und Überwachung in ein bestehendes Managementsystem zu integrieren.

Jedoch zeigt sich zugleich, dass die ISO 9001 den spezifischen Anforderungen der KI-VO, insbesondere hinsichtlich algorithmischer Risiken, datenethischer Fragestellungen und Bias Management, nicht vollumfänglich gerecht wird. Auch Aspekte wie Human Oversight, Nachvollziehbarkeit algorithmischer Entscheidungen oder Maßnahmen zur Sicherstellung der Trainingsdatenqualität sind in der Norm nicht explizit geregelt.[554]

Daher ist es für Anbieter hochriskanter KI-Systeme erforderlich, die ISO 9001 entweder um entsprechende KI-spezifische Leitlinien zu ergänzen oder diese mit Normen wie der ISO 42001 zu kombinieren, um die regulatorischen Anforderungen aus Art. 17 KI-VO umfassend abzudecken.

[552] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 7.
[553] ISO 9001:2015, Abschnitt 6.1.
[554] ISO 9001:2015, Abschnitt 6.1; BeckOK KI-Recht/Korge, KI-VO Art. 17 Rn. 7.

Die ISO 9001 kann dabei insbesondere die übergreifenden Managementstrukturen und das Qualitätsbewusstsein innerhalb der Organisation stärken und so ein Fundament für die Umsetzung der spezialisierten KI-bezogenen Anforderungen bilden. Sie ist somit ein wichtiges, aber nicht hinreichendes Element im Rahmen eines Compliance-konformen Qualitätsmanagementsystems nach KI-VO.

6. ISO 27001:2022 – Informationssicherheitsmanagement

a) Schutz von Informationssicherheit als Compliance-Faktor

Die ISO 27001:2022 bildet den internationalen Standard für Informationssicherheitsmanagementsysteme (ISMS) und stellt ein strukturiertes Rahmenwerk zur Verfügung, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen.[555] Sie adressiert damit zentrale Compliance-Anforderungen, die auch für hochriskante KI-Systeme von großer Bedeutung sind, insbesondere wenn diese auf sensible Daten angewiesen sind, etwa bei der Verarbeitung personenbezogener Daten, Gesundheitsinformationen oder bei sicherheitskritischen Anwendungen.

Das Managementsystem nach ISO 27001 basiert ebenfalls auf dem prozessorientierten Ansatz und folgt dem PDCA-Zyklus. Es enthält Anforderungen an die Risikobewertung und -behandlung, an die Etablierung von Sicherheitsrichtlinien, an das Asset Management sowie an den Schutz vor Bedrohungen durch interne und externe Akteure.[556] Die Norm fordert, dass Organisationen die relevanten Informationswerte identifizieren, Risiken bewerten und geeignete Maßnahmen zur Risikobehandlung umsetzen.

[555] ISO 27001:2022, Introduction.
[556] ISO 27001:2022, Abschnitt 6 ff.

b) Bezug zu Art. 17 KI-VO im Hinblick auf Risikomanagement und Dokumentation

Der Bezug der ISO 27001 zu Art. 17 KI-VO ergibt sich vor allem aus zwei zentralen Schnittstellen: dem Risikomanagement und der Dokumentationspflicht. Beide Elemente sind für die Erfüllung der Anforderungen des Art. 17 KI-VO von erheblicher Relevanz. Insbesondere die Forderung der KI-VO, ein Managementsystem einzuführen, das Risiken identifiziert, bewertet und angemessen adressiert, korrespondiert mit dem risikobasierten Ansatz der ISO 27001.

Die Norm verlangt detaillierte Verfahren zur Identifikation von Informationssicherheitsrisiken, zur Bestimmung der Eintrittswahrscheinlichkeit und Auswirkung dieser Risiken sowie zur Auswahl geeigneter Risikominderungsmaßnahmen.[557] Diese Methodik lässt sich problemlos auch auf KI-spezifische Risiken übertragen, etwa im Hinblick auf Manipulationen von Trainingsdaten (Data Poisoning), Angriffe auf Modelle (Model Inversion, Adversarial Attacks) oder unautorisierte Zugriffe auf kritische Systemkomponenten.

Zudem stellt die ISO 27001 strenge Anforderungen an die Dokumentation sämtlicher sicherheitsrelevanter Prozesse. Diese Anforderung deckt sich mit der Pflicht zur vollständigen Prozessdokumentation, wie sie Art. 17 KI-VO für das Qualitäts- und Risikomanagement vorschreibt.[558] Gerade im Hinblick auf die Nachvollziehbarkeit von Entscheidungen und die Auditierbarkeit der Compliance kann dies ein entscheidender Beitrag zur Umsetzung der regulatorischen Anforderungen sein.

c) Ergänzungspotential zur ISO 42001 und ISO 9001

Die besondere Stärke der ISO 27001 im Vergleich zu den anderen beiden hier betrachteten Normen liegt in ihrem dezidierten Fokus auf Informationssicherheit. Während die ISO 9001 primär auf die Produkt- und Prozessqualität und die ISO 42001 auf KI-spezifische Managementprozesse zielen, ergänzt die ISO 27001 diese Perspektive um den Aspekt der Sicherheitsarchitektur.

[557] ISO 27001:2022, Abschnitt 6 ff.
[558] Art. 17 II Buchst. b KI-VO.

Im Zusammenspiel mit ISO 42001 und ISO 9001 kann die ISO 27001 insbesondere dazu beitragen, die Anforderungen der KI-VO hinsichtlich Datenqualität und Datenintegrität umfassend abzusichern. Dies betrifft nicht nur den Schutz der Trainings- und Validierungsdaten, sondern auch die Sicherstellung der Verfügbarkeit und Unverfälschtheit der Modelle und Outputs während des Betriebs.[559]

Darüber hinaus bietet die ISO 27001 einen Katalog an organisatorischen und technischen Kontrollen (Annex A), die je nach Risikobewertung ausgewählt und implementiert werden können. Hierzu zählen unter anderem Zugangskontrollen, Verschlüsselung, Protokollierung, Incident Management und Maßnahmen zur Sicherstellung der Betriebskontinuität.[560] Diese Instrumente können im Rahmen eines integrierten Managementsystems auch zur Erfüllung der Anforderungen aus Art. 17 KI-VO herangezogen werden, insbesondere dort, wo der Schutz vor Manipulationen und Missbrauch von KI-Systemen gewährleistet sein muss.

Gleichwohl ist die ISO 27001, ebenso wie die anderen betrachteten Normen, kein vollständiger Ersatz für eine gezielte Umsetzung der KI-VO. Sie bildet jedoch ein tragfähiges Fundament für die Absicherung des Informationsflusses innerhalb von KI-gestützten Prozessen und leistet einen wichtigen Beitrag zur Erfüllung der regulatorischen Anforderungen.

7. Bewertung der Normenkombination für die Erfüllung von Art. 17 KI-VO

a) Synergien zwischen ISO 42001, ISO 9001 und ISO 27001

Die Kombination der ISO 42001, ISO 9001 und ISO 27001 bietet eine umfassende Grundlage zur Umsetzung der Anforderungen aus Art. 17 KI-VO. Während die ISO 9001 die allgemeine Prozessqualität sicherstellt und die ISO 27001 die Informationssicherheitsaspekte adressiert, ergänzt die ISO 42001 diese Perspektiven um KI-spezifische Fragestellungen wie Bias Management, Impact Assessments und human oversight.[561] Durch diese komplementären Schwerpunkte ergibt sich ein integratives Managementsystem, das sowohl die regulatorischen Vorgaben als auch ethische und technische Anforderungen systematisch abbilden kann.

[559] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 8.
[560] ISO 27001:2022, Annex A.
[561] ISO 42001:2023, Abschnitt 6 ff.

Besonders hervorzuheben ist die Möglichkeit, die Risikomanagementmethodik der ISO 9001 und 27001 mit den speziellen Anforderungen der ISO 42001 zu verknüpfen. Dies ermöglicht es, klassische betriebliche Risiken, Informationssicherheitsrisiken und KI-spezifische Risiken im Rahmen eines einheitlichen Risikomanagementsystems zu erfassen und zu steuern.[562]

Darüber hinaus profitieren Organisationen von der gemeinsamen HLS-Struktur der drei Normen, die eine einfachere Integration der verschiedenen Managementsysteme erlaubt. Synergieeffekte können etwa durch gemeinsame interne Audits, konsolidierte Management-Reviews oder integrierte Dokumentationssysteme erzielt werden.[563]

b) Lücken und spezifische Anforderungen der KI-VO

Trotz der genannten Synergien verbleiben relevante Lücken zwischen den ISO-Normen und den spezifischen Anforderungen der KI-VO. Insbesondere adressieren weder ISO 9001 noch ISO 27001 explizit die Anforderungen an Bias Detection, Erklärbarkeit („explainability") algorithmischer Entscheidungen oder menschliche Aufsichtspflichten („human oversight") in der Tiefe, wie sie Art. 17 iVm Art. 9 und Art. 14 KI-VO verlangt.[564]

Auch die Anforderung an eine systematische Überprüfung der eingesetzten Datensätze auf Repräsentativität und Eignung (Art. 10 KI-VO) sowie die Verpflichtung zur Gewährleistung der Transparenz gegenüber den Nutzern (Art. 13 KI-VO) sind in den betrachteten Normen nur unzureichend abgebildet. Hier besteht Anpassungsbedarf innerhalb des Qualitäts- und Risikomanagementsystems, um die regulatorischen Anforderungen vollumfänglich umzusetzen.[565]

Zusätzlich bleibt zu beachten, dass die KI-VO selbst keine Zertifizierungspflicht nach ISO-Normen vorsieht, sondern ausschließlich die tatsächliche Wirksamkeit der getroffenen Maßnahmen verlangt. Eine formale Zertifizierung kann daher nur

[562] ISO 9001:2015, Abschnitt 6; ISO 27001:2022, Abschnitt 6.
[563] Vgl. ISO 9001:2015, Annex SL.
[564] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 9.
[565] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 9; vgl. auch Art. 10 und Art. 13 KI-VO.

Indizwirkung haben und ersetzt nicht die eigenständige Prüfung der Compliance durch die zuständigen Behörden, vgl. § 17 Abs. 2 KI-VO.

c) Rechtliche Bewertung: Reicht Zertifizierung zur Erfüllung der Verordnungspflichten aus?

Aus juristischer Perspektive stellt sich die Frage, ob die Einführung und Zertifizierung eines Managementsystems nach ISO 42001, 9001 und 27001 allein geeignet ist, den Anforderungen des Art. 17 KI-VO zu genügen. Dabei ist zu berücksichtigen, dass die Verordnung eine substanzielle Compliance-Pflicht fordert, deren Erfüllung an der tatsächlichen Wirksamkeit der Prozesse gemessen wird.[566]Eine Zertifizierung kann im Rahmen der Compliance-Verteidigung („compliance defense") eine erhebliche Indizwirkung entfalten, vermag aber nicht automatisch die Haftung auszuschließen.

Die Rechtsprechung zur Produktsicherheit und zur Compliance in anderen Rechtsbereichen legt nahe, dass Zertifizierungen als ein Element ordnungsgemäßer Organisation angesehen werden können, sofern sie durch wirksame interne Prozesse flankiert werden.[567] Auch die KI-VO knüpft an diesen Maßstab an, indem sie neben der formalen Etablierung eines Qualitätsmanagementsystems die konkrete Risikominimierung sowie deren Überprüfung fordert.

Die alleinige Implementierung eines zertifizierten Managementsystems ohne tatsächliche Risikoanalyse und wirksame Maßnahmen zur Risikobeherrschung genügt daher nicht, um die Anforderungen der KI-VO zu erfüllen. Entscheidend ist vielmehr die inhaltliche Ausgestaltung der Prozesse, deren Wirksamkeit und die Fähigkeit der Organisation, auf neue Risiken oder Veränderungen des Systems angemessen zu reagieren.[568]

Damit ergibt sich, dass eine Zertifizierung nach ISO 42001, ISO 9001 und ISO 27001 ein wichtiger Bestandteil einer Compliance-Strategie im Bereich KI sein kann, jedoch keine vollständige Entlastung von der Verantwortung für die Umsetzung der Verordnungspflichten bewirkt. Eine kritische Auseinandersetzung mit den spezifischen Anforderungen der KI-VO und deren praktische Umsetzung bleibt unerlässlich.

---

[566] Art. 17 II KI-VO.
[567] Vgl. BGH NJW 2008, 3770.
[568] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 10.

8. CEN/CENELEC JTC21

Eine Konkretisierung der technischen und prozessualen Anforderungen an das QMS erfolgt jedoch nicht im Normtext selbst, sondern über die Rückbindung an harmonisierte Normen iSv Art. 40 KI-VO sowie über sogenannte gemeinsame Spezifikationen iSv Art. 41 KI-VO.

a) Erstellung harmonisierter Normen gem. Art. 40 KI-VO

Die Erstellung harmonisierter Normen ge. Art. 40 KI-VO obliegt den beiden europäischen Normungsorganisationen CEN (Comité Européen de Normalisation) und CENELEC (Comité Européen de Normalisation Électrotechnique), denen nationale Normungsinstitute wie DIN (Deutschland), AFNOR (Frankreich) oder BSI (UK, bis Brexit) als Mitglieder angehören.[569] Die Zuweisung der Zuständigkeit für die Ausarbeitung harmonisierter Normen im Sinne des Art. 40 KI-VO an die europäischen Normungsorganisationen CEN und CENELEC ergibt sich streng juristisch aus einem mehrstufigen Zusammenspiel von Primärrecht, sektorspezifischem Sekundärrecht sowie einschlägigen Durchführungsrechtsakten der Europäischen Kommission. Die Grundlage für die europäische Normung bildet Verordnung (EU) Nr. 1025/2012 über die europäische Normung, dabei definiert Art. 2 Nr. 1 definiert: „Europäische Norm" ist eine von einer der anerkannten europäischen Normungsorganisationen angenommene Norm: CEN, CENELEC oder ETSI.[570]

„Europäische Norm" ist eine von einer der anerkannten europäischen Normungsorganisationen angenommene Norm: CEN, CENELEC oder ETSI. Gem. Art. 10 I der Verordnung (EU) 1025/2012 kann die Kommission diesen Organisationen sog. Normungsaufträge (Standardisation Requests) erteilen, um „harmonisierte Normen" für die Zwecke der Unionsharmonisierungsvorschriften zu entwickeln.[571]

[569] BeckOK KI-Recht/Kilian, 1. Ed. 1.1. 2025, KI-VO Art. 40 Rn. 12-15.

[570] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 über die europäische Normung, ABl. L 316 vom 14.11.2012, S. 12-33, insbesondere Art. 2 Nr. 1 und Nr. 6 iVm Anhang I.

[571] BeckOK KI-Recht/Kilian, 1. Ed. 1.1. 2025, KI-VO Art. 40 Rn. 12-15.

Ein zentrales Gremium für die Entwicklung entsprechender Normen im Bereich künstlicher Intelligenz ist das Joint Technical Committee CEN/CLC JTC 21 mit dem formalen Titel: [572]

„*Artificial Intelligence – Horizontal aspects*"

Dieses Komitee wurde 2021 gegründet und ist ausdrücklich zuständig für die Entwicklung horizontaler Normen im KI-Bereich – also solcher, die branchenübergreifend anwendbar sind. Die Zielsetzung besteht darin, aufbauend auf den Arbeiten des internationalen ISO/IEC-Komitees JTC 1/SC 42 europäisch konsistente, an der KI-VO ausgerichtete Normen zu entwickeln. Besonders relevant sind hier unter anderem:

- EN ISO/IEC 42001 (KI-Managementsysteme)
- EN ISO/IEC 23894 (Risikomanagement für KI-Systeme)
- EN ISO/IEC 5338 (AI lifecycle management)

Diese Normen dienen als Referenz für die Umsetzung der Anforderungen aus Art. 17 KI-VO, etwa hinsichtlich Dokumentationspflichten, Auditverfahren, Rollenverantwortlichkeit und Prozessen des Lebenszyklusmanagements.[573]

Die nationale Beteiligung an Normungsprozessen erfolgt dabei über Spiegelgremien, in denen Vertreter aus Wirtschaft, Wissenschaft und Verwaltung mitwirken (im Falle des JTC 21 über das DIN/DKE Gremium NA 043-04-41 AA). Durch diese Struktur wird die Beteiligung maßgeblicher Interessenträger institutionalisiert und zugleich sichergestellt, dass nationale Belange und spezifische technische Rahmenbedingungen aus deutscher Sicht wirksam in den europäischen Normungsprozess eingespeist werden.

[572] CEN/CLC JTC 21, Artificial Intelligence – Horizontal aspects, Mandat und Arbeitsprogramme, Stand: Mai 2025, abrufbar unter: https://standards.cencenelec.eu.

[573] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 20.

b) Die Umsetzung der Anforderungen aus Art. 17 KI-VO durch ISO/IEC 42001, 23894 und 5338

Aktuell sind die Normen ISO/IEC 42001, ISO/IEC 23894 und ISO/IEC 5338 (noch) nicht als harmonisierte Normen im Sinne des Art. 40 KI-VO anerkannt.[574] Sie können daher de lege lata keine Konformitätsvermutung im Sinne von Art. 40 II KI-VO auslösen.[575] Dennoch stellt sich die Frage, ob ihre Anwendung gleichwohl inhaltlich geeignet ist, die Anforderungen aus Art. 17 KI-VO zu erfüllen.

c) EN ISO/IEC 42001 – Managementsysteme für Künstliche Intelligenz

Siehe hierzu die Ausführungen in Abschnitt IV.4.

aa) EN ISO/IEC 23894 – Risikomanagement für KI-Systeme

Diese Norm ergänzt ISO 42001um ein spezifisches Rahmenwerk für Risikomanagement in KI-Systemen und ist als „vertical extension" der allgemeinen Risikomanagementnorm ISO 31000 zu verstehen.576 Die ISO/IEC 23894 fordert u. a.:

- eine strukturierte Risikoidentifikation für KI-spezifische Risiken,
- Berücksichtigung von Bias, Erklärbarkeit und Transparenz,
- Dokumentation und Nachvollziehbarkeit von Risikoentscheidungen.

Damit erfüllt sie grundsätzlich die Anforderungen aus Art. 17 II Buchst. a, b und g KI-VO (Risikomanagementverfahren, Datenverarbeitung und Kontrolle, sowie Korrekturmaßnahmen) und konkretisiert das von Art. 9 KI-VO ebenfalls geforderte Risikomanagement.

bb) EN ISO/IEC 5338 – AI-Lifecycle Management

Die jüngere ISO/IEC 5338[577] widmet sich dem vollständigen Lebenszyklusmanagement von KI-Systemen – von der Idee über Entwicklung und Einsatz bis zur Stilllegung. Sie legt systematisch fest:

- Phasenstruktur (Planung – Entwicklung – Bereitstellung – Betrieb – Einstellung),

[574] KI-VO ErwGr. 77-78 zur Rolle von Normung und QM-Systemen.
[575] BeckOK KI-Recht/Kilian, 1. Ed. 1.1.2025, KI-VO Art. 40 Rn. 12-15.
[576] Vgl. ISO TC 262 / JTC 1/SC 42 (AI) – Risikomanagement für KI.
[577] aktueller Status: Draft international standard (DIS, seit 2024).

- Rollen und Verantwortlichkeiten,
- Anforderungen an Schnittstellenmanagement, Überwachung und Validierung.

Die Norm bietet damit eine strukturierte operationalisierbare Auslegung von Art. 17 II Buchst. a, e und f KI-VO, indem sie organisatorische Prozesse und Zuständigkeiten über den gesamten Lebenszyklus definiert. [578]

Auch wenn diese Norm (noch) nicht als harmonisierte Norm gilt, ist sie zur Erfüllung der Dokumentations- und Nachweispflichten aus Art. 17 iVm Art. 11 KI-VO einer technischen Dokumentation geeignet.

9. Resümee

Die Analyse der Anforderungen des Art. 17 KI-VO und deren mögliche Umsetzung über die Normen ISO 42001, ISO 9001 und ISO 27001 zeigt deutlich, dass ein integriertes Managementsystem einen wesentlichen Beitrag zur Einhaltung der regulatorischen Pflichten leisten kann. Dabei fungieren die genannten ISO-Standards als strukturgebende Instrumente, die es ermöglichen, Risikomanagement, Qualitätsmanagement und Informationssicherheit systematisch zu organisieren und zu dokumentieren.

Besonders die ISO 42001 bietet mit ihrem KI-spezifischen Fokus ein praxisnahes Rahmenwerk, um die besonderen Anforderungen der KI-VO – etwa hinsichtlich Bias Management, Transparenz und human oversight – zu operationalisieren. In Kombination mit den prozessorientierten Strukturen der ISO 9001 sowie den Sicherheitsarchitekturen der ISO 27001 ergibt sich ein robustes Fundament für ein Compliancegerechtes Management hochriskanter KI-Systeme.

Gleichwohl verbleiben Regelungslücken, die durch die Normen allein nicht geschlossen werden können. Die KI-VO setzt über die strukturellen Anforderungen hinaus auch inhaltliche Maßstäbe, etwa hinsichtlich der Qualität und Eignung von Trainingsdaten, der Gewährleistung menschlicher Kontrolle oder der Vermeidung systematischer Diskriminierung. Diese Aspekte erfordern eine vertiefte Auseinandersetzung, die über das hinausgeht, was die betrachteten ISO-Normen unmittelbar leisten können. Die bloße Existenz eines zertifizierten Managementsystems genügt nicht, um die

[578] BeckOK KI-Recht/Henke, KI-VO Art. 17 Rn. 15 ff.

Compliance sicherzustellen. Vielmehr ist die tatsächliche Wirksamkeit der getroffenen Maßnahmen und deren kontinuierliche Überprüfung ausschlaggebend.

Vor diesem Hintergrund erscheint es sinnvoll, ergänzend zu den bestehenden ISO-Normen branchenspezifische Leitlinien und sektorspezifische Standards zu entwickeln, die die regulatorischen Vorgaben der KI-VO konkretisieren und in die betriebliche Praxis im Sinne AI-Governance überführen. Auch eine Weiterentwicklung der ISO 42001 in Richtung einer engeren Anlehnung an die Anforderungen der KI-VO könnte zur weiteren Harmonisierung beitragen.

Zukünftig wird sich zudem die Frage stellen, ob europäische oder nationale Behörden die Zertifizierung nach ISO 42001, ISO 9001 oder ISO 27001 als Teil der Konformitätsbewertung im Sinne der KI-VO offiziell anerkennen werden. Eine solche Entwicklung könnte sowohl die Rechtssicherheit für Anbieter erhöhen als auch die behördliche Kontrolle erleichtern.

Art. 17 KI-VO entfaltet seine praktische Wirksamkeit auch im Zusammenspiel mit den Art. 40 und 41 KI-VO und der darauf aufbauenden europäischen Normungsstruktur. Die technischen Detailanforderungen an das QMS von Anbietern Hochrisiko-KI-Systemen werden dabei im Wesentlichen vom CEN/CLC JTC 21 formuliert und durch das DIN in deutsches Normenrecht überführt. Die hieraus resultierenden Normen (z. B. DIN EN ISO/IEC 42001) stellen faktisch den maßgeblichen Prüfungsmaßstab für regulatorische Konformität dar. Unternehmen, die sich an diesen Normen orientieren, können sich auf eine rechtlich anerkannte Konformitätsvermutung stützen.

Dies verdeutlicht die Untrennbarkeit rechtlicher und technischer Regulierung im Bereich der KI-Governance: Der Gesetzgeber gibt mit Art. 17 KI-VO die Leitplanken vor – die technische Ausgestaltung erfolgt durch europäische und nationale Normungsgremien, deren Arbeit für Rechtsanwender faktisch bindend ist.

Abschließend lässt sich festhalten, dass die Verknüpfung von Qualitätsmanagement, Risikomanagement und Informationssicherheit im Lichte der KI-VO ein zentraler Bestandteil einer effektiven Compliance-Strategie sein muss. Die Nutzung der

bestehenden ISO-Standards bietet hierfür ein bewährtes Instrumentarium, das jedoch einer kritischen Prüfung und Anpassung an die spezifischen Anforderungen der KI-VO bedarf. Nur so kann gewährleistet werden, dass KI-Systeme nicht nur formal, sondern auch materiell den Anforderungen an Sicherheit, Vertrauenswürdigkeit und Rechtskonformität genügen.

V. KI-Governance

Die KI-Governance im Kontext der KI-Verordnung (KI-VO) umfasst eine Vielzahl von rechtlichen Aspekten, die die Einführung und Anwendung von KI-Systemen regeln. Die KI-VO sieht spezifische Anforderungen vor, die auf Transparenz, Risikomanagement und Verantwortlichkeit abzielen. Im Folgenden werden die wesentlichen rechtlichen Aspekte der KI-Governance dargestellt, gefolgt von einer Diskussion zur praktischen Umsetzung in einem Governance-Tool.

1. Verantwortlichkeit und Rechenschaftspflicht

Ein zentrales Element der KI-Governance nach der KI-VO ist die klare Zuweisung von Verantwortlichkeiten. Gemäß Art. 28 KI-VO sind Anbieter von Hochrisiko-KI-Systemen verpflichtet, sicherzustellen, dass ihre Systeme mit den Vorschriften der Verordnung übereinstimmen. Dabei wird von den Verantwortlichen erwartet, dass sie die Implementierung und Einhaltung der Vorschriften überwachen und Maßnahmen ergreifen, um etwaige Verstöße zu verhindern oder zu korrigieren. Dieser Grundsatz der Rechenschaftspflicht verlangt, dass die Verantwortlichen über die Entwicklung, den Betrieb und die Überwachung der KI-Systeme berichten können (Art. 18 KI-VO).

Die Governance eines KI-Systems muss also ein umfassendes Compliance-System beinhalten, das in der Lage ist, die Einhaltung der Verordnung über den gesamten Lebenszyklus der KI sicherzustellen. Governance-Mechanismen sollten somit auch Verantwortlichkeiten und Rollen klar definieren, insbesondere bei sensiblen Entscheidungen wie der Risikobewertung und der Behebung von Verstößen.

2. Transparenz- und Dokumentationspflichten

Die KI-VO stellt hohe Anforderungen an die Transparenz von KI-Systemen. Art. 13 Abs. 1 der KI-VO schreibt vor, dass Hochrisiko-KI-Systeme so gestaltet sein müssen, dass ihre Benutzer über deren Funktionsweise und mögliche Risiken informiert werden. Hierzu gehört auch die Pflicht, technische Dokumentationen zu erstellen, die detaillierte Informationen über die Funktionsweise und den Aufbau des KI-Systems enthalten (Art. 18 KI-VO). Diese Dokumentationspflicht ermöglicht eine bessere Überprüfbarkeit der Systeme und gewährleistet, dass relevante Informationen bei Bedarf auch den Aufsichtsbehörden zur Verfügung gestellt werden können.
In der Governance eines KI-Systems muss daher ein strukturiertes Dokumentationssystem etabliert sein, das sicherstellt, dass alle wesentlichen Aspekte des Systems nachvollziehbar und überprüfbar sind.

3. Risiko- und Sicherheitsmanagement

Eine weitere zentrale Anforderung der KI-VO betrifft das Risiko- und Sicherheitsmanagement. Art. 9 Abs. 1 und 2 KI-VO fordern, dass Anbieter Hochrisiko-KI-Systeme kontinuierlich überwachen und auf mögliche neue Risiken prüfen. Es müssen geeignete Maßnahmen zur Risikominimierung ergriffen werden, um sicherzustellen, dass das System keine potenziellen Schäden verursacht. Dabei muss auch ein Eskalationsprozess definiert werden, um auf neu identifizierte Risiken schnell reagieren zu können.

Im Rahmen der KI-Governance ist daher ein System zu implementieren, das die Risikoüberwachung und Sicherheitsbewertung regelmäßig und systematisch durchführt. Dies umfasst die Überprüfung von Algorithmen, Daten und Modellen, um mögliche neue Risiken frühzeitig zu identifizieren.

4. Etablierung von Ethik- und Integritätsstandards

Zusätzlich zu den technischen und regulatorischen Anforderungen müssen Anbieter von KI-Systemen auch ethische und integritätsbezogene Standards etablieren, die sich aus den Grundwerten der EU und der KI-VO ableiten lassen. Die Verordnung hebt hervor, dass KI-Systeme im Einklang mit den Grundrechten und ethischen Grundsätzen stehen müssen, um eine verantwortungsvolle und faire Nutzung der Technologie sicherzustellen (Erwägungsgrund 40 KI-VO). Dies erfordert die Einrichtung eines Governance-Systems, das die Einhaltung ethischer Standards überwacht und sicherstellt, dass die KI-Systeme diskriminierungsfrei und im Einklang mit den europäischen Werten betrieben werden.

5. Umsetzung im Governance-Tool

Ein Governance-Tool zur Einhaltung der KI-VO sollte spezifische Funktionalitäten bieten, um die Einhaltung der beschriebenen Anforderungen zu gewährleisten:

- **Verantwortungsmanagement**: Das Tool sollte Rollen und Verantwortlichkeiten klar dokumentieren und zuweisen. Es muss nachvollziehbar machen, wer für welche Aspekte des KI-Systems verantwortlich ist und welche Maßnahmen im Falle eines Verstoßes oder eines Risikos ergriffen werden. Ein integriertes Eskalationsmanagement kann hier hilfreich sein, um eine schnelle Reaktion zu ermöglichen.

- **Dokumentations- und Transparenzmodul**: Um die Anforderungen an Transparenz und Dokumentation zu erfüllen, muss das Governance-Tool in der Lage sein, technische und rechtliche Dokumentationen bereitzustellen und revisionssicher zu speichern. Benutzer sollten zudem in die Lage versetzt werden, auf Dokumentationen zuzugreifen, die die Funktionsweise und möglichen Risiken des KI-Systems erläutern.

- **Risikomanagement-Funktionalitäten**: Ein Governance-Tool sollte ein Modul für das Risiko- und Sicherheitsmanagement enthalten, welches regelmäßige Bewertungen und Audits des Systems ermöglicht. Es sollte potenzielle Risiken frühzeitig erkennen, bewerten und dokumentieren sowie die Möglichkeit bieten, Sicherheitsmaßnahmen zu implementieren und ihre Wirksamkeit zu überwachen.

- **Ethik- und Integritätsüberwachung**: Ein umfassendes Governance-Tool muss auch Mechanismen zur Überwachung ethischer Standards bieten. Hierzu können Checklisten für Ethikprüfungen und Richtlinien zur Gewährleistung der Grundrechtekonformität integriert sein. Automatische Benachrichtigungen könnten etwa ausgelöst werden, wenn bestimmte Ethik- oder Diskriminierungsindikatoren überschritten werden.

Ein gutes KI-Governance-Tool nach der KI-VO gewährleistet nicht nur die Einhaltung der regulatorischen Anforderungen, sondern fördert auch die verantwortungsvolle und ethische Nutzung von KI-Systemen, indem es Transparenz, Rechenschaft und Risikomanagement integriert.

VI. Kritik[579]

1. Komplexität und Rechtsunsicherheit

Die KI-VO führt eine Klassifizierung von KI-Systemen nach Risikostufen ein, die zwar eine differenzierte Regulierung ermöglicht, jedoch auch eine erhebliche Komplexität und damit verbundene Rechtsunsicherheit mit sich bringt. Juristische Akteure haben Bedenken hinsichtlich der Abgrenzungskriterien zwischen den einzelnen Risikokategorien geäußert. Es besteht die Befürchtung, dass die vage Definition von Schlüsselbegriffen und die breite Auslegung dessen, was unter ein "KI-System" fällt, zu Interpretationsspielräumen führt, die die Rechtssicherheit untergraben könnten. Diese Unklarheiten könnten für Entwickler und Anbieter von KI-Systemen zu erheblichen Compliance-Herausforderungen führen, ins. bei KMU und kleineren Startups.

2. Administrative Lasten und Kosten

Ein weiterer kritischer Punkt betrifft die administrativen Lasten und die damit verbundenen Kosten, ebenfalls insb. für KMU. Die Einhaltung der umfangreichen Dokumentations-, Berichterstattungs- und Risikomanagementanforderungen, die vor allem für KI-Systeme mit hohem Risiko gelten, könnte für KMU eine erhebliche Belastung darstellen. Die Anforderungen könnten sie nicht nur unmittelbar finanziell

[579] *Verabschiedung der europäischen KI-Verordnung – Darstellung wesentlicher Punkte der KI-VO und Kritik* Söbbing, ITRB 2024, 108-111.

belasten, sondern auch indirekt die Ressourcenallokation beeinflussen, indem sie Unternehmen dazu zwingen, erhebliche Mittel für Compliance-Maßnahmen aufzuwenden, anstatt in Innovation und Entwicklung zu investieren.

3. Auswirkungen auf die Innovationsfähigkeit

Die Kritik erstreckt sich ferner auf die potenziellen Auswirkungen der KI-VO auf die Innovationsfähigkeit innerhalb der Europäischen Union. Während das Ziel der Verordnung, ein hohes Schutzniveau für Bürger und Gesellschaft zu gewährleisten, breite Zustimmung findet, warnen Kritiker vor einem möglichen Innovationshemmnis durch übermäßige Regulierung. Die Sorge besteht, dass die strikten Anforderungen, insb. für KI-Systeme mit hohem Risiko, die Entwicklung und Einführung neuer Technologien verlangsamen könnten. Dies könnte die Wettbewerbsfähigkeit europäischer Unternehmen auf dem globalen Markt beeinträchtigen, besonders im Vergleich mit Akteuren in weniger regulierten Jurisdiktionen.

4. Bürokratische Hürden und Durchsetzungsproblematik

Schließlich wird die praktische Durchsetzbarkeit der Verordnung kritisch hinterfragt. Die effektive Überwachung und Durchsetzung der vielfältigen und komplexen Anforderungen der KI-VO stellt eine erhebliche Herausforderung dar. Die Notwendigkeit einer starken und koordinierten Aufsichtsstruktur auf EU-Ebene, die in der Lage ist, die Einhaltung der Vorschriften effektiv zu überwachen und Verstöße zu ahnden, wirft Fragen hinsichtlich der erforderlichen Ressourcen und der bürokratischen Belastung auf. Zudem besteht die Gefahr, dass die Vielzahl der Anforderungen und die Komplexität der Materie zu einer Fragmentierung der Durchsetzungspraxis führen könnten, was wiederum die Rechtssicherheit und die Gleichbehandlung der Marktteilnehmer gefährdet.

5. Fazit

Die KI-Verordnung der Europäischen Union stellt einen ambitionierten Versuch dar, den Herausforderungen und Risiken der KI-Technologie auf umfassende Weise zu begegnen. Während die Intention, ein hohes Schutzniveau für die Gesellschaft zu gewährleisten und gleichzeitig Innovation zu fördern, zu begrüßen ist, werfen die dargelegten Kritikpunkte fundamentale Fragen hinsichtlich der praktischen Umsetzbarkeit, der übermäßigen Bürokratie, der Effizienz des Rechtsrahmens und der langfristigen Auswirkungen auf die Innovationsfähigkeit in der EU auf, was sich zu Lasten

der Wirtschaft und der Arbeitnehmer auswirken würde. Eine fortlaufende Evaluation und ggf. Anpassung der Verordnung erscheinen daher unerlässlich, um die Balance zwischen Schutz und Innovation in einem sich rasant entwickelnden technologischen Umfeld zu gewährleisten.

G. Autonomes Fahren[580]

Als ein autonomes Fahrzeug bezeichnet man dabei ein Fahrzeug, das frei (also ohne menschliche Unterstützung) navigiert.[581] Hierbei entscheidet das Auto (als KI/Roboter) autonom, wie es sein Fahrverhalten (Lenkung, Geschwindigkeit, etc.) an die Umgebung anpasst.[582] Roboter nehmen dabei sensorisch ihre Umwelt war und reagieren entsprechend ihrer Programmierung. Eine gewisse Lernfähigkeit, die zu einer Erweiterung der Möglichkeiten führt, ist sicherlich dabei nicht ausgeschlossen, sondern wünschenswert. Die Robotik beschäftigt sich dabei mit einer sog. manipulativen Intelligenz: Mit Hilfe von Robotern können gefährliche Tätigkeiten oder auch immer gleiche Manipulationen, wie das Entschärfen von Bomben auf Roboter verlagert werden. Der Grundgedanke ist es, Systeme (Roboter) zu schaffen, die intelligente Verhaltensweisen von Lebewesen nachvollziehen können.

I. Automatisierungsgrade

Die Bundesanstalt für Straßenwesen (BASt), welche als praxisorientierte, technisch-wissenschaftliche Forschungseinrichtung dem Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) in fachlichen und verkehrspolitischen Fragen Entscheidungshilfen gibt[583], hat eine Projektgruppe zur Identifizierung und begrifflichen Definition der unterschiedlichen Automatisierungsgrade ins Leben gerufen.[584] Das Ergebnis dieser Projektgruppe ist die Darstellung unterschiedlicher Level für das Autonome Fahren:

1. Level 0 – Driver only

Die Klassifizierung der Automatisierungsgrade gemäß BASt beginnt bei „Level 0 – Driver Only“ und damit mit einer Eingruppierung, die an und für sich dem Wortlaut nach überhaupt keine Automatisierung darstellt. Bei Level 0 führt der Fahrer dauerhaft, also während der gesamten Fahrt, die Längs- und Querführung des Fahrzeugs selbstständig aus.[585] Bei der Längsführung handelt es sich konkret um das Beschleunigen und Verzögern des Fahrzeugs. Wohingegen es sich bei der Querführung einzig um den Lenkvorgang an sich dreht. Aus praktischer Sicht ist daher unter Level 0-Systemausprägungen ein konventionelles

[580] Rechtliche Grenzen für KI-Entscheidungen im Rahmen des autonomen Fahrens Söbbing, RDi 2023, 239
[581] *Hägele/Schäfer*, in: Gevatter/Grünhaupt (Hrsg.), Handbuch der Mess- und Automatisierungstechnik in der Produktion, 2006.
[582] *Kirsch,* CT Magazin für Computertechnik Nr. 22, 2011, 43.
[583] https://www.bast.de/DE/BASt/BASt_node.html;jsessionid=905ABC3FD1F06FA5F8CD8E1F99925695.live2051 (zuletzt abgerufen am 24.01.2016).
[584] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 8.
[585] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.

Fahren ohne jegliche Unterstützung bei der Längs- und/oder Querführung zu verstehen, so dass der Fahrzeugführer hierbei alleine („driver only") für die Bewältigung der Fahraufgabe zuständig ist. [586]

2. Level 1 – Assistiert

Automatisierungsgrad „Level 1 – Assistiert" wird dadurch definiert, dass der Fahrer dauerhaft entweder die Quer- oder die Längsführung ausführt. Die jeweils andere Fahraufgabe wird dabei in gewissen Grenzen vom Fahrzeugsystem ausgeführt.[587] Entscheidend bei dieser Automatisierungsstufe ist, dass der Fahrzeugführer das Fahrzeugsystem dauerhaft überwachen und jederzeit unmittelbar zur vollständigen Übernahme der Fahrzeugführung bereit sein muss.[588] Damit ist der Fahrzeugführer neben Level 0 auch bei Level 1 jederzeit voll- und eigenständig für die Bewältigung der Fahraufgabe zuständig. Level 1-Systeme sind bereits seit langem auf dem Markt erhältlich und erfreuen sich insbesondere ab Mittelklassefahrzeugen zunehmender Beliebtheit. Beispiele für Fahrzeugsysteme des Level 1 sind unter anderem Adaptive Cruise Control oder ein Parkassistent. Das System Adaptive Cruise Control (ACC) ist ein Beispiel für die systemseitige Unterstützung bei der Längsführung des Fahrzeugs. Bei ACC handelt es sich um eine automatische Abstandsregelung, die die Geschwindigkeit und den Abstand zum vorausfahrenden Fahrzeug durch selbstständiges Beschleunigen und Verzögern weitestgehend konstant hält. Demgegenüber übernimmt das System bei einem Parkassistenten das automatische Lenken in Parklücken (Querführung), wobei die Verantwortung für das Beschleunigen und Verzögern durch Gas geben und Bremsen (Längsführung) dabei vollumfänglich beim Fahrzeugführer verbleibt. Zusammenfassend kann man für Systeme der Automatisierungsstufe 1 sagen, dass diese den ersten Schritt in eine automatisierte Zukunft darstellten. Gleichwohl unterstützen und entlasten derartige Systeme den Fahrzeugführer lediglich bei einer der beiden notwendigen Führungsaufgaben. Eine komplette und eigenständige Übernahme einer der beiden Führungsaufgaben durch das System ist auch auf dieser Stufe der Automatisierung aufgrund der dauerhaften Überwachung- und Eingriffsbereitschaft des Fahrzeugführers nicht gegeben.

[586] *Buchberger*, ITRB 2014, 116, 117.
[587] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.
[588] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.

3. Level 2 – Teilautomatisiert

Die Pflicht zur dauerhaften Überwachung und jederzeitigen sowie vollständigen Bereitschaft zur Übernahme der Fahrzeugführung trifft den Fahrzeugführer beim Automatisierungsgrad „Level 2 – Teilautomatisiert" ebenso wie bei Level 1. Der wesentliche Unterschied zwischen Level 1- und Level 2-Systemen ist jedoch darin zu sehen, dass beim teilautomatisierten Fahren das System sowohl die Quer- als auch die Längsführung für einen gewissen Zeitraum und/oder in spezifischen Situationen übernimmt.[589] Die Hauptaufgabe des Fahrzeugführers bei derartigen Systemen liegt vor allem in der Überwachung und gegebenenfalls Übersteuerung des teilautomatisierten Systems. Hierzu ist er nämlich vor allem beim Erreichen der Systemgrenzen, im Fehlerfall sowie beim Verlassen des konkreten Anwendungsbereiches unmittelbar verpflichtet.[590] Vor diesem Hintergrund ist es für den sicheren Gebrauch von teilautomatisierten Systemen unerlässlich, dass der Fahrzeugführer das System ständig überwacht und in Kenntnis aller Systemgrenzen sowie seiner persönlichen Fähigkeiten selbst erkennt, wann eine Korrektur des Systems angezeigt ist.[591] Ein, wenn auch nur temporäres, Entlassen des Fahrzeugführers aus der Fahraufgabe und der damit im Zusammenhang stehenden Verantwortung ist bei Level 2-Funktionen aus den vorgenannten Gründen unter keinen Umständen möglich. Das teilautomatisierte System befreit den Fahrzeugführer daher bis zur erforderlichen Rückübernahme der Fahrzeugsteuerung lediglich von der aktiven Handlungsführung.[592] Diese Funktion unterstützt im Geschwindigkeitsbereich zwischen 0 und ca. 65 km/h zusätzlich zur automatischen Abstandsregelung ACC (siehe „Level-1 – assistiert") bei der Lenkarbeit. Dabei führt es das Auto durch sanfte Lenkeingriffe und folgt der vorausfahrenden Kolonne innerhalb der jeweiligen Systemgrenzen. Somit unterstützen und entlasten teilautomatisierte Systeme den Fahrer bei der Bewältigung der Fahraufgaben in beiden Regelungsbereichen (Längs- und Querführung) und stellen damit einen höheren Funktionsumfang und Automatisierungsgrad als Level 1-Funktionen dar.

4. Level 3 – Hochautomatisiert

Beim hochautomatisierten Fahren des Levels 3 übernimmt das System ebenso wie beim

[589] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.
[590] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 11.
[591] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 11.
[592] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 12.

teilautomatisierten Fahren des Levels 2 die Längs- und Querführung für einen gewissen Zeitraum in spezifischen Situationen (wie z. B. einer Staufahrt auf der Autobahn). Von grundlegender und im weiteren Verlauf dieser Ausarbeitung entscheidender Bedeutung ist bei Level 3-Systemen die Tatsache, dass der Fahrzeugführer das System nicht mehr dauerhaft überwachen muss und er bei Bedarf mit ausreichender Zeitreserve vom System zur Übernahme der Fahraufgabe aufgefordert wird.[593] Aufgrund dieser vorgehaltenen Zeitreserve muss das hochautomatisierte System alle Systemgrenzen selbst erkennen und bei Erreichen von Systemgrenzen den Fahrer entsprechend informieren. Diese vom System vorgehaltene Zeitreserve hat darüber hinaus zur Konsequenz, dass der Fahrer während der automatisierten Fahrt nicht mehr mit der Fahraufgabe beschäftigt ist und daher die Beförderung eine neue Qualität der Entlastung aufweist. Hochautomatisierte Systeme sind bislang nicht im Markt erhältlich, befinden sich aber unter anderem bei dem deutschen Premiumhersteller Audi in Form des „Staupiloten" in einer seriennahen Entwicklung.[594] Der Fahrer soll dabei wie beim teilautomatisierten Fahren in monotonen und langweiligen Fahrsituationen entlastet werden, so dass dadurch Unfälle verhindert oder zumindest deren Folgen gemindert werden.[595] Da das hochautomatisierte System zwar alle Systemgrenzen rechtzeitig erkennt, aus diesen Situationen aber nicht immer selbständig in der Lage ist, den risikominimalen Zustand herzustellen, ist das Vorhandensein eines übernahmefähigen Fahrers ständig notwendig.[596]

[593] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.
[594] http://blog.audi.de/2015/05/26/per-autopilot-durch-die-megacity-shanghai/ (zuletzt abgerufen am 24.01.2016).
[595] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 38.
[596] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.

5. Level 4 – Vollautomatisiert

Durch eine Steigerung der Systemleistung beim vollautomatisierten Fahren (Level 4) ist bei derartigen Systemen im Gegensatz zu Systemen des Levels 3 auch gewährleistet, dass bei einer nicht erfolgten Übernahme der Fahraufgabe durch den Fahrer das System selbsttätig in einen sicheren Zustand zurückkehren kann.[597] Die Überführung in den risikominimalen Zustand erfolgt bei einem stehenden Fahrzeug dadurch, dass ein automatisiertes Wiederanfahren unterbunden wird. Bei einem sich bewegenden Fahrzeug wird der risikominimale Zustand durch ein moderates Verzögern bis in den Stillstand samt Aktivierung des Warnblinkers und der elektrischen Parkbremse hergestellt.[598] Anders als beim hochautomatisierten Fahren kann ein vollautomatisiertes System, sofern die Verkehrslage und der Systemzustand es zulassen, das Fahrzeug durch ein oder mehrere Fahrstreifenwechsel auf den Seitenstreifen gelenkt und dort zum Stillstand gebracht werden.[599] Im Übrigen entsprechen sich die technischen Ausprägungen der Automatisierungsstufen 3 und 4 aber weitestgehend.

II. Verhaltensrechtliche Vorschriften

Um die verhaltensrechtlichen Vorschriften des automatisierten Fahrens drehen sich derzeit die meisten Rechtsfragen. Zum einem stellt sich in diesem Zusammenhang die Frage, ob die zunehmend technische Entlastung und Reduzierung der Verhaltensanforderungen des Fahrzeugführers bei steigender Automatisierung auch mit geltendem Recht in Einklang zu bringen ist oder ob es gesetzgeberischen Handlungsbedarf gibt.[600]

1. Wiener Übereinkommen über den Straßenverkehr

Die allgemeine Grundlage für nationalstaatliche Regelungen für den Straßenverkehr bildet das Wiener Übereinkommen über den Straßenverkehr aus dem Jahre 1968[601] (im Folgenden „WÜ“). Bei dem Übereinkommen handelt es sich um einen völkerrechtlichen Vertrag, der aufgrund des stark zunehmenden grenzüberschreitenden Verkehrs notwendig gewesen ist. Durch die Unterzeichnung und Ratifizierung des WÜ wurde eine internationale Vereinheitlichung des Straßenverkehrsrechts, insbesondere der Verhaltensvorschriften und der

[597] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, 12.
[598] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 39.
[599] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 39.
[600] *Buchberger*, ITRB 2014, 116, 117.
[601] Abgedruckt in BGBl. II, 1977, S. 811 ff.

Verkehrszeichen geschaffen.[602] Das WÜ wurde am 8. November 1968 in Wien geschlossen und umfasst derzeit 73 beteiligte Nationen.[603]

Durch das WÜ verpflichten sich die Vertragsstaaten, die im Vertrag enthaltenen Bestimmungen auf die nationalen straßenverkehrsrechtlichen Vorschriften zu übertragen. Ferner sind diese Bestimmungen die Voraussetzung für die Zulassung im internationalen Verkehr, vgl. Art. 3 Abs. 3 WÜ. In Art. 8 und Art. 13 WÜ wird geregelt, dass das Fahrzeug ständig vom Fahrer kontrolliert und „dauernd" von ihm „beherrscht" wird. Problematisch werden diese Vorschriften bei Fahrerassistenzsystemen (KI-Systemen), die den Fahrer technisch von der Fahrzeugkontrolle befreien.[604] Handelt es sich beispielsweise um eine vom Fahrerassistenzsystem selbstständig ausgelöste Bremsung, die der Fahrer nicht übersteuern kann, erfüllt dies die Voraussetzung des WÜ nicht, da dem Fahrer keine Handlungsalternative gelassen wird.[605] Diese Beherrschungs- und Überwachungspflicht des Fahrers wurde im März 2014 auf der 68. Sitzung der Working Party on Road Traffic Safety (WP.1) in Genf diskutiert und weiter entwickelt bzw. angepasst. Die Anpassung sieht vor, dass die entsprechende Verpflichtung auch dann erfüllt wird, solange die Fahrerassistenzsysteme für den Fahrer beeinflussbar („übersteuerbar oder abschaltbar gestaltet") sind.[606] Mittlerweile wird die Änderung von den Vertragsstaaten ohne Gegenstimmen akzeptiert.[607]

a) Europäisches Zulassungsrecht – ECE-Regelungen

Neben dem WÜ steht das ECE- Abkommen von 1958, auf dessen Basis auch verbindliche Regeln (sog. ECE-Regelungen) hinsichtlich der technischen Zulassung von Fahrzeugen festgelegt wurden. In Deutschland erfolgt die Zulassung von Fahrzeugen heute nach europäischem Recht (RL 2007/46/EG). Diese Richtlinie verweist im Anhang IV auf die ECE-Regelungen. Auch diese Regelungen werden regelmäßig durch die UN-ECE[608] an den technischen Fortschritt angepasst, allerdings wesentlich schneller als beim WÜ. Diese

[602] *Frenz/van den Broek*, NZV 2009, 530; BT-Drs. 8/178, S. 308 ff.

[603] Eine umfassende Liste der beteiligten Vertragsstaaten ist unter http://www.unece.org/trans/conventn/legalinst_08_RTRSS_RT1968.html abrufbar (zuletzt abgerufen am 24.01.2016).

[604] *Albrecht*, VD 06/2006, 143, 144.

[605] *Gasser*, VKU 2009, 224.

[606] *Buchberger*, ITRB 2014, 116, 117.

[607] https://treaties.un.org/doc/Publication/CN/2015/CN.529.2015.Reissued.06102015-Eng.pdf (Stand: 05.02.2016).

[608] Unterorganisation der UN mit der Aufgabe technische Anforderungen an Fahrzeugen zu erarbeiten, welche dann auf völkerrechtlicher Basis angenommen werden. Diese sollen der Vereinheitlichung der Anforderungen zwischen den einzelnen Staaten dienen. Weitere Informationen zur UN-ECE finden sich unter: https://www.unece.org/leginstr/cover.html (zuletzt abgerufen am 29.12.2015).

Ungleichbehandlung in der Anpassung führt zu erhöhtem Aufwand bei den Mitgliedstaaten und damit zu einer unnötigen Behinderung des technischen Fortschritts. Deshalb wurde auch zu diesem Punkt im Rahmen der Änderungen der WP.1 eine Lösung gefunden, in dem Art. 39 Abs. 1 S. 3 WÜ neu hinzugekommen ist und die Einhaltung der technischen Anforderungen entsprechend den ECE-Regeln unterstellt wird.[609]

b) StVO

Mit der Reform der Straßenverkehrsordnung (StVO) wurde eine Erhöhung der Verkehrssicherheit angestrebt. Dazu gehörten auch Regelungen zu Verhaltenspflichten zur Unfallvermeidung.[610] Ermächtigungsgrundlage und Schutzzweck der StVO ergeben sich aus dem Straßenverkehrsgesetz (§§ 6 Abs. 1 Nr. 3, 4a, 5a 13 ff. StVG). Erhaltung der Ordnung und Sicherheit im öffentlichen Raum, also die Erhaltung der allgemeinen Verkehrssicherheit und der einzelnen Person (hier i. S. d. § 823 Abs. 2 BGB) werden hiermit angestrebt.[611] Das WÜ ist das höherrangige Recht und dient in Deutschland als Grundlage für die geltende Straßenverkehrsordnung (StVO). Dadurch enthält auch die aktuelle Fassung der StVO den Passus der „ständigen Beherrschbarkeit" des Fahrzeugs durch den Fahrer.[612]

Bei KI- Technologien in Fahrzeugen, die dem Levels 2 entsprechen, handelt es sich um sog. teilautomatisierte Funktionen, welche im aktivierten Modus die Längs- und Querführung für den Fahrzeugführer übernehmen. Eine Abwendung von der Fahraufgabe ist dem Fahrzeugführer bei teilautomatisierten Systemen nicht gestattet.[613] Der Fahrer kann durch das KI-System des Fahrzeuges jederzeit zur Übernahme der Fahrzeugführung aufgefordert werden. Vor diesem Hintergrund hat der Fahrzeugführer als Verhaltensanforderung beim teilautomatisierten Fahren das System dauerhaft zu überwachen und jederzeit zur vollständigen Übernahme der Fahrzeugführung bereit zu sein. Damit ist bei dem aktiven Betrieb eines teilautomatisierten Systems immer noch der Fahrzeugführer als Mensch derjenige, der das Fahrzeug mittelbar dauerhaft in Bewegung hält. Eine Substitution des Fahrers durch das teilautomatisierte System ist gerade nicht der Fall, so dass dem Fahrzeugführer weiterhin die Gesamtverantwortung für das In-Bewegung-Setzen und die Fortbewegung des

[609] *Lutz*, DAR 8/2014, 446, 448.
[610] VkBl 1970, 797, 798 f. Begründung des Bundesverkehrsministers zur Straßenverkehrsordnung.
[611] *Gasser*, VKU 2009, 224.
[612] *Buchberger*, ITRB 2014, 116, 117.
[613] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.

Fahrzeugs obliegt.[614] Folglich hat der Fahrzeugführer dauerhaft zu überwachen, dass er gem. § 3 Abs. 1 S. 1 StVO nur so schnell fährt, dass das Fahrzeug ständig beherrscht wird. Eine vergleichbare Regelung gilt für den Abstand zu einem anderen Fahrzeug. Der Fahrzeugführer hat gem. § 4 Abs. 1 StVO den Abstand zu einem vorausfahrenden Fahrzeug so groß zu halten, dass hinter diesem auch gehalten werden kann, wenn es plötzlich bremst. Somit liegt auch dem Gebot des ausreichenden Abstands die Verhaltensanforderung des Beherrschens des Fahrzeugs zugrunde. Im Allgemeinen hat sich der Fahrzeugführer nach § 1 Abs. 2 StVO grundsätzlich so zu verhalten, dass kein anderer geschädigt, gefährdet oder mehr, als nach den Umständen vermeidbar, behindert oder belästigt wird. Dies gilt aufgrund der dauerhaften Überwachungsverpflichtung des Fahrzeugführers bei teilautomatisierten Systemen unverändert fort, so dass er unter Umständen übersteuernd eingreifen müsste.

Bei KI-Systemen in Fahrzeug auf dem Niveau des Levels 3 übernimmt das hochautomatisierte Systeme nicht nur die Längs- und Querführung des Fahrzeugs,[615] sondern gewährt dem Fahrzeugführer im automatisierten Betrieb auch Freiraume dahingehend, dass er das System nicht mehr dauerhaft überwachen muss und bei Bedarf vom System mit ausreichender Zeitreserve zur Übernahme der Fahraufgabe aufgefordert wird. Durch den vorgenannten Freiraum und der fehlenden Notwendigkeit der Überwachung des Fahrgeschehens durch den Fahrzeugführer ist grundsätzlich zweifelhaft, ob der Fahrzeugführer überhaupt als solcher im Sinne der verhaltensrechtlichen Anforderungen der StVO noch bezeichnet werden kann. Ein Fahrzeug führt, wer es „unter bestimmungsgemäßer Anwendung seiner Antriebskräfte unter eigener Allein- oder Mitverantwortung in Bewegung setzt und es unter Handhabung seiner technischen Vorrichtungen während der Fahrbewegung durch den öffentlichen Verkehrsraum ganz oder wenigstens zum Teil leitet“. Bei der hochautomatisierten Fahrt mangelt es dem „Fahrer“ aber gerade dauerhaft an der Eigenschaft das Fahrzeug wenigstens zum Teil zu leiten. Bei der aktivierten hochautomatisierten Fahrt wird der „Fahrer“ von den wesentlichen Verhaltensanforderung der StVO entbunden, da diese gerade

[614] *Buchberger*, ITRB 2014, 116, 117.
[615] BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, Tab. 2-1, S. 9.

durch das Fahrzeug und nicht mehr durch den menschlichen Fahrer eigenständig ausgeführt und erfüllt werden.[616]

2. Anforderungen nach StVG

Abweichend von der „normalen" zivilrechtlichen Haftung in Kapitel L. „Haftung" können durch das Autonome Fahren weitere Haftungstatbestände erfüllt werden.

a) Fahrerhaftung nach § 18 StVG

Als Verhaltensstörer steht zunächst der Fahrer des Fahrzeugs im Haftungsfokus. Für den Fahrer, ob ohne oder mit Assistenzsystem, richtet sich die Fahrerhaftung nach § 18 StVG. Der Fahrzeugführer haftet nach § 18 StVG im Falle eines persönlich vorwerfbaren Sorgfaltsverstoßes, wobei gem. § 18 Abs. 1 S. 2 StVG sein Verschulden grundsätzlich vermutet wird und er insoweit die Beweislast hinsichtlich eines möglichen Entlastungsbeweises zu tragen hat.[617] Einen solchen Entlastungsbeweis kann der Fahrzeugführer vor allem erbringen, wenn er nachweisen kann, dass der Unfall auf einen technischen Fehler des Fahrzeugs zurückzuführen ist (z. B. Versagen der Bremsen) oder aber wenn sich der Fahrer in der jeweiligen Verkehrssituation regelkonform verhalten hat.[618]

Im Falle eines Mangels haftet der Hersteller. Hat sich der Unfallgegner verkehrswidrig verhalten, haftet natürlich dieser. Weil beim teilautomatisierten Fahren zwar die Quer- und Längsführung vom Fahrzeug ausgeführt wird, die permanente Überwachung und die damit einhergehende unmittelbare Eingriffsaufgabe aber dem Fahrzeugführer obliegt, ist ein Verschulden des Fahrzeugführers im Schadensfall grundsätzlich vorhanden. Entscheidend ist hierbei, dass der Fahrzeugführer von seinen Sorgfaltspflichten bei der teilautomatisierten Fahrt nicht entbunden ist. Dies bedeutet aber nicht, dass ihm im Einzelfall der Entlastungsnachweis des § 18 Abs. 1 S. 2 StVG verwehrt ist. Vielmehr bleibt diese Möglichkeit bestehen, so dass grundsätzlich keinerlei qualitativer Unterschied zwischen einer manuellen bzw. assistierten Fahrt und einem teilautomatisierten Betrieb festgestellt werden kann.

---

616 *Buchberger*, ITRB 2014, 116, 117.
617 *Berz/Dedy/Granich*, DAR 2002, 545.
618 *Buchberger*, ITRB 2014, 116, 117.

b) Haftung des Halters nach § 7 StVG

Nach § 7 StVG ist der Halter einem Geschädigten zum Schadensersatz verpflichtet, wenn beim „Betrieb eines Kraftfahrzeugs oder eines Anhängers, ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt wird". Dabei trifft den Halter bei einem Unfall die Gefährdungshaftung, d. h. der Halter haftet ohne jegliches Verschulden für das Halten seines Fahrzeuges.[619] Grundsätzlich dient die Gefährdungshaftung dem Ziel, auf die Auswirkungen von Gefahren zu reagieren bzw. diese auszugleichen.[620] Damit begründet die Halterhaftung nicht den Ausgleich für begangenes Verhaltensunrecht, sondern für Schäden, die durch den Betrieb eines Fahrzeugs entstehen.[621] Der Halter haftet daher für die Gefahr, die sich aus der Eröffnung einer Gefahrenquelle realisiert.[622] Ein Halter eines Fahrzeuges ist, wer das eigene Kraftfahrzeug auf eigene Rechnung in Gebrauch hat und die Verfügungsgewalt darüber besitzt. Halter bedeutet demnach nicht zugleich auch Eigentümer (siehe Leasing). Bei der Verfügungsgewalt ist das tatsächliche Herrschaftsverhältnis maßgeblich, also z. B. fallen bei Leasingverträgen der Halter und der Eigentümer regelmäßig auseinander und trotz Leasingvertrag haftet der Halter auch wenn er nicht Eigentümer des Fahrzeugs ist, wie es dem Wesen der Veranlasserhaftung entspricht.[623] In § 1 Abs. 2 StVG werden alle Fahrzeuge erfasst, die durch Maschinenkraft bewegt werden. Zu beachten ist dabei, dass § 7 Abs. 1 StVG nicht zur Anwendung kommt, wenn § 8 Nr. 1 StVG eintritt, also ein Unfall durch ein Kraftfahrzeug verursacht wird, das nicht schneller als 20 km/h fahren kann. Weitere Ausnahmetatbestände sind in § 8 Nr. 2 und 3 StVG geregelt.

Nach § 7 StVG muss der Schaden beim Betrieb des Fahrzeugs entstanden sein. Dies ist immer dann anzunehmen, wenn das Fahrzeug im öffentlichen Verkehrsbereich in Bewegung gesetzt wurde.[624] Dabei wird der öffentliche Verkehrsbereich sehr weit ausgelegt und findet nach § 7 Abs. 1 StVG Anwendung, wenn das Fahrzeug in verkehrsbeeinflussender

[619] *Berz/Dedy/Granich*, DAR 2002, 545.
[620] *Deutsch/Ahrens*, Deliktsrecht, 6. Aufl. 2014, Rn. 7
[621] *Kuhnert,* in: Haus/Krumm/Quarch, Gesamtes Verkehrsrecht, 2. Aufl. 2017, § 7 StVG Rn. 4.
[622] *Berz/Dedy/Granich*, DAR 2002, 545.
[623] *Berz/Dedy/Granich*, DAR 2002, 545.
[624] *Kuhnert,* in: Haus/Krumm/Quarch, Gesamtes Verkehrsrecht, 2. Aufl. 2017, § 7 StVG Rn. 4.

Weise ruht, beispielsweise parkt.[625] Zusätzlich muss sich die typische Betriebsgefahr realisiert haben. Das bedeutet, dass örtlich und zeitlich ein Zurechnungszusammenhang zwischen dem Betrieb des Fahrzeugs und dem Eintritt des Schadens[626] bestehen und sich gerade die durch das Fahrzeug verursachte spezifische Gefahr verwirklicht haben muss. Wird ein Fahrerassistenzsystem verwendet und entsteht bei einem Verkehrsunfall ein Schaden, so ist der Schaden nicht aufgrund unwahrscheinlicher Umstände eingetreten, sondern es konnte vernünftigerweise davon ausgegangen werden, dass ein Assistenzsystem bei fehlerhafter Arbeitsweise oder falscher Bedienung Schaden anrichten kann.[627] Die Halterhaftung inkludiert schuldhaftes Fehlverhalten des Fahrers als auch Fehlfunktionen von Assistenzsystemen. Dazu gehören auch aktiv eingreifende Systeme, selbst wenn diese nicht übersteuerbar sind. Begründet wird diese Haftung darin, dass der Fahrzeughalter für die jeweilige Betriebsgefahr des von ihm in den Verkehr gebrachten Fahrzeuges Verantwortung übernehmen muss.[628] Gehaftet wird für alle Schäden aufgrund von Fehlern in der Beschaffenheit des Fahrzeuges. Bei Fahrerassistenzsystemen besteht die Schadensersatzpflicht des Halters demnach grundsätzlich, wenn diese fehlerhaft arbeiten oder Fehler im Umgang mit ordnungsgemäß arbeitenden Fahrerassistenzsystemen zu Tage treten.[629] Fraglich ist, inwieweit dann eine Haftung des Hersteller vorliegt und der Fahrer von diesem Ersatz verlangen kann.

c) Haftungsgrenzen

Grundsätzlich ist die gesetzliche Haftungsbegrenzung der StVO auch bei der Verwendung on KI-Systemen in Fahrzeugen zu berücksichtigen. Nach § 12 StVG haftet der Fahrer wie Halter bei Personenschäden bis zu fünf Million Euro und bei Sachbeschädigung bis zu einer Millionen Euro. Die weitere Ersatzpflicht ist in §§ 10, 11 und 13 StVG geregelt.

Zu berücksichtigen ist auch ein Haftungsausschluss, der sich aus höherer Gewalt ergeben könnte. Bei höherer Gewalt kommen lediglich elementare Naturkräfte oder Handlungen Dritter in Frage zum Haftungsausschluss. Diese müssen nach der menschlichen Einsicht

[625] *Gasser*, VKU 2009, 224, 228.
[626] BGH, NJW 1975, 1886.
[627] *Berz/Dedy/Granich*, DAR 2002, 545.
[628] *Gasser*, VKU 2009, 224, 228.
[629] *Walter*, SVR 2006, 41, 69.

und Erfahrung unvorhersehbar und unabwendbar sein. Fahrfehler anderer oder plötzlich auf die Straße laufende Fußgänger oder Kinder fallen nicht unter höhere Gewalt.[630]

Bei einem Betrieb und Nutzung von teilautomatisierten Systemen wird eine anderweitige rechtliche Bewertung nicht überzeugen. So schafft der Fahrzeughalter bei Systemen des Levels 0 oder 1 ebenso wie bei Level 2-Funktionen durch das Kraftfahrzeug eine Gefahrenquelle, die sich im Falle eines konkreten Unfalls gerade realisiert. Des Weiteren ist als Argument anzuführen, dass sich Fahrzeuge mit derartigen Systemen auch nicht permanent im aktivierten Level 2-Betrieb, sondern zum weitaus größten Teil der Nutzung im manuellen oder assistierten Betrieb befinden.[631] Vor diesem Hintergrund ist festzuhalten, dass die Zuordnung der Betriebsgefahr zum Fahrzeughalter und die damit im Zusammenhang stehende Haftung nach § 7 StVG auch im teilautomatisierten Betrieb folgerichtig und konsequent ist.[632]

d) Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion, § 1a StVG

In Jahre 2017[633] hat die Politik mit den neugeschaffenen § 1a und § 1b StVG auf die Anforderungen der Wirtschaft reagiert und gesetzliche Regelungen zu hoch- und vollautomatisierten Fahrfunktionen geschaffen. Der Fahrer darf die Steuerung des Fahrzeugs in bestimmten Situationen und je nach System dem Computer überlassen.

Nach § 1a Abs. 1 StVG ist der Betrieb eines Kraftfahrzeugs mittels hoch- oder vollautomatisierter Fahrfunktion dann zulässig, wenn die Funktion bestimmungsgemäß verwendet wird. Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion im Sinne der StVG sind solche, die über eine gem. § 1a Abs. 2 StVG technische Ausrüstung verfügen,

- die zur Bewältigung der Fahraufgabe – einschließlich Längs- und Querführung – das jeweilige Kraftfahrzeug nach Aktivierung steuern (Fahrzeugsteuerung) kann,

- die in der Lage ist, während der hoch- oder vollautomatisierten Fahrzeugsteuerung den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen,

630 *Walter*, SVR 2006, 41, 69.
631 *Buchberger*, ITRB 2014, 116, 117.
632 BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012, S. 18 f.
633 Drucksache 69/17 vom 27.01.17.

- die jederzeit durch den Fahrzeugführer manuell übersteuerbar oder deaktivierbar ist,

- die die Erforderlichkeit der eigenhändigen Fahrzeugsteuerung durch den Fahrzeugführer erkennen kann,

- die dem Fahrzeugführer das Erfordernis der eigenhändigen Fahrzeugsteuerung mit ausreichender Zeitreserve vor der Abgabe der Fahrzeugsteuerung an den Fahrzeugführer optisch, akustisch, taktil oder sonst wahrnehmbar anzeigen kann und

- die auf eine der Systembeschreibung zuwiderlaufende Verwendung hinweist.

Der Betrieb eines Kfz mittels hoch- oder teilautomatisierter Fahrfunktion ist nach § 1a Abs. 1 StVG nur zulässig, wenn die Funktion bestimmungsgemäß verwendet wird. Die Bedingungen wie das System genutzt werden darf, müssen vom Hersteller vorgegeben werden.[634] Hält sich der Fahrzeugführer nicht an diese Bedingungen, muss das System des Fahrzeuges den Fahrzeugführer darauf hinweisen, vgl. § 1a II 1 Nr. 6 StVG und es trifft den Fahrer das Verschulden an einem dadurch verursachten Unfall. Dies gilt nicht nur, wenn er sich über einen Hinweis des Systems hinweggesetzt hat, sondern nach § 1b II Nr. 2 StVG auch dann, wenn er von sich aus erkennen musste, dass die Voraussetzungen für eine bestimmungsgemäße Verwendung offensichtlich nicht mehr vorliegen. Mit den Bestimmungen des Herstellers muss sich der Fahrzeugführer vertraut machen.[635] Kommt es zu einem Schadensfall (Verkehrsunfall) dadurch, dass der Fahrzeugführer in die Funktion der automatischen Steuerung eingegriffen hat, so muss der Fahrzeugführer darlegen und beweisen, dass dies der im Verkehr erforderlichen Sorgfalt entsprach oder dass es auch ohne den Eingriff zu dem Unfall gekommen wäre. Dies ist in der Praxis sicherlich nur durch ein Gutachten möglich und stellt diese vor neue Herausforderungen. Hat der Fahrzeugführer auf eigenes Veranlassen oder durch eine Aufforderung des Systems folgend die Steuerung wieder übernommen, muss er beweisen, dass er verkehrsgerecht agiert hat. Hierbei kommt es auf die Gefahrenlage im Zeitpunkt der Übernahme der Steuerfunktion an. Er haftet daher z. B. nicht

[634] *Greger*, NZV 2018, 1 ff.
[635] *Grünvogel*, MDR 2017, 973, 974.

für das Anfahren eines Fußgängers, welches nachweisbar bei fortwährender Beobachtung des Verkehrsgeschehens, aber nicht mehr bei Übernahme der Steuerung vermeidbar gewesen wäre.[636] Hätte der Fahrzeugführer gem. § 1b Abs. 2 Nr. 1 i. V. m. § 1a Abs. 2 1 Nr. 5 StVG nicht unverzüglich eingegriffen, obwohl er vom System dazu aufgefordert worden war, muss er beweisen, dass der Unfall auch durch sein Eingreifen nicht verhindert worden wäre. Dabei ergibt sich aus § 1b Abs. 1 StVG, dass der Fahrzeugführer zu dem unverzüglichen Eingreifen auch „jederzeit" bereit sein muss. Das an sich zulässige Abwenden von der Fahrzeugsteuerung darf also nicht so weit gehen, dass der Fahrer gehindert ist, auf das entsprechende Warnsignal hin die der Verkehrslage entsprechende Führung des Kfz unverzüglich zu übernehmen. „Unverzüglich" bedeutet nach allgemeinem Verständnis (s. § 121 Abs. 1 Nr. 1 BGB) ein nach den Umständen des Falles zu bemessendes beschleunigtes, nicht vorwerfbar verzögertes Handeln.[637] Der Fahrer muss so schnell auf die Aufforderung durch das System reagieren, wie ihm dies in der konkreten Situation auf zumutbare Weise möglich ist. Anders als bei Willenserklärungen kann ihm hier keine Prüf- und Bedenkzeit eingeräumt werden.[638] Da er „jederzeit" zur Übernahme der Steuerung bereit sein muss, ist eine Reaktion innerhalb weniger Sekunden zu erwarten,[639] denn nur dann kann die Warnung durch das System, die trotz der in § 1a Abs. 2 Nr. 5 StVG vorgeschriebenen Vorlaufzeit eine akute Gefahrenlage signalisiert, ihren Zweck erfüllen. Hat sich der Fahrer außer Stande gesetzt, derart schnell zu reagieren, trifft ihn die Schuld an einem Unfall, der ohne die Zeitverzögerung vermeidbar gewesen wäre. Dies ist insbesondere der Fall, wenn der Fahrer den Fahrersitz verlassen oder in Liegestellung gebracht hat oder wenn er einer Beschäftigung nachgeht, die er nicht sofort beenden kann.[640] Der große Streit der Zukunft des autonomen Fahrens wird sein, ab welchem Zeitpunkt der Fahrzeugführer die Steuerung vom System hätte übernehmen müssen. Grundsätzlich müsste der Fahrzeugführer nachdem er erkannt hat oder auf Grund offensichtlicher Umstände erkennen musste, dass die Voraussetzungen für eine bestimmungsgemäße Verwendung der automatisierten Fahrfunktionen nicht mehr vorliegen (§ 1b Abs. 2 Nr. 2 StVG), die Steuerung des Fahrzeuges

[636] *Greger*, NZV 2018, 1 ff.
[637] BVerwG, NJW 1989, 52, 53. So auch die Bundesregierung in BT-Drs. 18/11534, 15; *König,* NZV 2017, 123, 125.
[638] BGH, NJW 2008, 985, 986.
[639] Der Bundesrat hat sich für eine Reaktionszeit von 1,5 bis 2 Sekunden zuzüglich eines Sicherheitszuschlages ausgesprochen; BT-Drs. 18/11534, S. 4.
[640] *Greger*, NZV 2018, 1 ff.

übernehmen. Denn der Fahrzeugführer darf sich nur so weit vom Verkehrsgeschehen und der Fahrzeugsteuerung abwenden, dass er dieser Pflicht jederzeit nachkommen kann (§ 1b Abs. 1 StVG). Wie dies im Einzelfall zu beurteilen ist, kann nur von Gutachter beurteilt werden, aus dem Gesetz ist dazu lediglich zu entnehmen, dass ein „Erkennenmüssen" ein fahrlässiges Nichterkennen (§ 122 Abs. 2 BGB) bedeutet. Lediglich durch das Merkmal „auf Grund offensichtlicher Umstände" wird der allgemeine Fahrlässigkeitsbegriff modifiziert: Schuldhaft handelt der Fahrer, wenn er trotz offensichtlicher Umstände nicht erkannt hat, dass eine bestimmungsgemäße Verwendung der automatischen Fahrfunktion nicht mehr gegeben ist.[641]

In § 1a Abs. 3 StVG wird klargestellt, dass auch Fahrzeuge, die mit hoch- oder vollautomatisierte Fahrfunktionen ausgestattet sind, wie alle anderen Fahrzeuge auch eine Betriebserlaubnis, Einzelgenehmigung oder Typgenehmigung benötigen. Diese Genehmigungen werden nur erteilt, wenn die notwendigen technischen Voraussetzungen erfüllt sind. Des Weiteren wird klargestellt, dass auch Kraftfahrzeuge, die eine EG-Typgenehmigung gem. Art. 20 der RL 2007/46/EG haben, trotzdem am Verkehr teilnehmen dürfen, obwohl noch keine UN-ECE-Regelung (Internationale Vorschrift) zu einer automatisierten Fahrfunktion vorliegt.

Nach § 1a Abs. 4 StVG ist Fahrzeugführer auch derjenige, der eine automatisierte Fahrfunktion aktiviert und zur Fahrzeugsteuerung verwendet, auch wenn er im Rahmen der bestimmungsgemäßen Verwendung dieser Funktion das Fahrzeug nicht eigenhändig steuert. Auch das vollständige Abwenden vom Verkehrsgeschehen, selbst das Verlassen des Fahrersitzes würde ihn nicht der Führereigenschaft entheben. Er haftet gegenüber einem Unfallgeschädigten daher nach § 18 StVG, ohne dass dieser ihm ein Verschulden nachweisen muss. Um sich von dieser Haftung zu befreien, muss er beweisen, dass ihn kein unfallursächliches Verschulden trifft (§ 18 Abs. 1 Nr. 2 StVG), etwa weil er das System in verkehrswidriger Weise manuell übersteuert oder entgegen § 1b Abs. 2 StVG die Fahrzeugsteuerung nicht wieder übernommen habe. In welchem Zustand sich das System zum Unfallzeitpunkt befand, ist anhand der Datenspeicherung nach § 63a StVG feststellbar. Um den Entlastungsbeweis führen zu können, kann der Fahrzeugführer verlangen, dass der Halter die Übermittlung der zur Abwehr der Haftung erforderlichen Daten an ihn

[641] *Greger*, NZV 2018, 1 ff.

veranlasst (§ 63a Abs. 3 StVG). Dieselbe Befugnis wird auf Grund seiner Regulierungsvollmacht dem Haftpflichtversicherer zuzuerkennen sein und zur Abwehr des Mitverschuldenseinwands auch den Geschädigten. Einzelheiten der Datenspeicherung sind in der Verordnung nach § 63b StVG zu regeln.[642]

e) Rechte & Pflichten bei Nutzung hoch-/vollautomatisierter Fahrfunktionen, § 1b StVG

Im Regierungsentwurf[643] wurden neben den Vorgaben für die Kfzs mit hoch- und vollautomatisierter Fahrfunktion insbesondere die Pflichten des Fahrzeugführers gem. § 1b Abs. 2 StVG herausgestellt. Mit dem neu eingefügten § 1b Abs. 1 StVG wird das Recht des Fahrzeugführers klargestellt, dass sich dieser vom Verkehrsgeschehen und der Fahrzeugsteuerung abwenden darf, während die hoch- und vollautomatisierte Fahrfunktion aktiv ist. Der Fahrzeugführer darf dabei im Rahmen der Systembeschreibung die Hände vom Lenkrad nehmen, den Blick von der Straße abwenden und anderen Tätigkeiten nachgehen. Die Gesetzesbegründung nennt hier beispielsweise die Bearbeitung von E-Mails im Infotainment-System.[644] Gleichzeitig treffen den Fahrzeugführer aber auch Pflichten während der Nutzung des hoch- und vollautomatisierten Systems. Hierzu gehört, die Fahrzeugsteuerung unverzüglich wieder zu übernehmen, wenn die Technik ihn dazu auffordert, vgl. § 1b Abs. 2 Nr. 1 StVG.[645] Damit soll sichergestellt werden, dass der Fahrzeugführer bspw. nicht erst noch eine E-Mail zu Ende liest, bevor er die Steuerung wieder übernimmt. Außerdem ist der Fahrzeugführer verpflichtet, die Steuerung wieder zu übernehmen, wenn er erkennt oder aufgrund offensichtlicher Umstände erkennen musste, dass die Voraussetzung für die Nutzung des hoch- und vollautomatisierten Systems nicht mehr vorliegen (§ 1b Abs. 2 Nr. 2 StVG). Ziel der Regelung ist es, bspw. bei offensichtlichen Störungen, wie einem Reifenplatzer, eine Handlungspflicht des Fahrzeugführers sicherzustellen.[646]

Zusammenfassend bleibt festzustellen, dass der Fahrzeugführer im hoch- und vollautomatisierten Fahren so wahrnehmungsbereit sein muss, dass er seine Pflichten nach § 1b Abs.

[642] *Greger*, NZV 2018, 1 ff.
[643] Drucksache 69/17 vom 27.01.17.
[644] BT-Drs. 18/11776, S. 10.
[645] BT-Drs. 18/11300, S. 22.
[646] *Lange*, NZV 2017, 345.

2 StVG erfüllen kann. Die Umstände, bei denen der Fahrer während der hoch- und vollautomatisierten Phase reagieren muss, müssen so offensichtlich sein, dass diese auch beim Abwenden von der Fahrzeugsteuerung und dem Verkehrsgeschehen erkennbar sind. Davon ist beispielsweise auszugehen, wenn der Fahrer durch das Hupen eines anderen Fahrzeugs auf Fahrfehler und damit auf eine technische Störung des Systems aufmerksam gemacht wird oder das System ohne äußeren Anlass eine Vollbremsung durchführt.[647] Ein weiteres denkbares praktisches Anwendungsszenario könnte in diesem Zusammenhang das Martinshorn eines von hinten sich nähernden Rettungsfahrzeuges sein. Hier weiterhin die Wahrnehmungsbereitschaft vom Fahrzeugführer zu fordern, ist insofern systemgerecht, als das auch die reguläre Aufforderung zur Rückübernahme der Fahrzeugsteuerung u. a. akustisch angezeigt werden kann, vgl. § 1a Abs. 2 Nr. 5 StVG.[648]

f) Datenverarbeitung mit hoch- oder vollautomatisierter Fahrfunktion, § 63a StVG

Bei Kraftfahrzeugen i. S. v. § 1a Abs. 1 S. 1 StVG müssen die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben gem. § 63a Abs. 1 S. 1 StVG gespeichert werden, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt. Eine derartige Speicherung erfolgt gem. § 63a Abs. 1 S. 2 StVG auch, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt. Ziel des Datenspeichers ist es, nachvollziehbar festzuhalten, ob die Fahrzeugsteuerung durch das System oder den Fahrzeugführer erfolgte und damit ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System stattgefunden hat.[649]

Zudem wurde in § 63a Abs. 5 StVG die Möglichkeit aufgenommen, Daten zur Unfallforschung in anonymisierter Form an Dritte zu übermitteln. Dabei ist jedoch zu beachten, dass die grundlegenden Anforderungen an den Datenspeicher Bestandteil der EU-Vorgaben sein werden. Vor diesem Hintergrund wurden in § 63b StVG eine Reihe an Verordnungsermächtigungen zugunsten des Bundesministeriums für Verkehr und digitale Infrastruktur vorgesehen. Hierdurch sollen die zur Durchführung der internationalen

[647] BT-Drs. 18/11776, S. 10f
[648] *Lange*, NZV 2017, 345.
[649] BT-Drs. 18/11776, S. 11.

Vorgaben notwendigen Regelungen eingeführt werden können. Diese umfassen die technische Ausgestaltung und den Ort des Speichermediums sowie die Art und Weise der Speicherung, den Adressaten der Speicherpflicht nach § 63a Abs. 3 StVG und die Maßnahmen, die zur Sicherung der gespeicherten Daten gegen unbefugten Zugriff bei Verkauf des Kraftfahrzeuges ergriffen werden müssen.[650]

g) Fahrerloses Parken, § 6 Abs. 1 Nr. 14a StVG

Bereits heute sind Fahrzeuge in der Lage fahrerlos und damit selbstständig zu parken. Der Gesetzgeber will diesem Umstand mit der Regelung in § 6 Abs. 1 Nr. 14a StVG gerecht werden. Denn gem. § 6 Abs. 1 Nr. 14 a StVG wird das Bundesministerium für Verkehr und digitale Infrastruktur ermächtigt, Regelungen für die Einrichtung und Nutzung von fahrerlosen Parksystemen zu schaffen. Diese sollen im niedrigen Geschwindigkeitsbereich auf Parkflächen, die durch bauliche oder sonstige Einrichtungen vom übrigen öffentlichen Straßenraum getrennt sind und nur über besondere Zu- und Abfahrten erreicht und verlassen werden können, eingerichtet werden können.

Die Firma Google Inc. ist bekannt für viele KI- Technologien, insbesondere durch den selbstlernenden Algorithmus ihrer Suchmaschine. Google beschäftigt sich seit Jahren auch mit selbstfahrenden Autos. Seit Mai 2014 hat Google begonnen, 100 hauseigene Elektro-Testfahrzeuge zu bauen, wobei erste Prototypen des Google Autos ohne Lenkrad, Bremse und Gaspedal auskommen sollen.[651] Langfristig soll der Fokus auf der Bereitstellung einer Serviceleistung – zum Beispiel mit führerlosen Taxis – liegen und nicht unbedingt auf dem Eigentum des Fahrers am Fahrzeug.

Als ein autonomes Fahrzeug bezeichnet man dabei ein Fahrzeug, das frei (also ohne menschliche Unterstützung) navigiert.[652] Hierbei entscheidet das Auto (als KI/Roboter) autonom, wie es sein Fahrverhalten (Lenkung, Geschwindigkeit, etc.) an die Umgebung anpasst.[653] Roboter nehmen dabei sensorisch ihre Umwelt war und reagieren entsprechend ihrer Programmierung. Eine gewisse Lernfähigkeit, die zu einer Erweiterung der

[650] BT-Drs. 18/11776, S. 11.
[651] Selbstfahrende Autos: Google baut ein eigenes Auto, in: Web-Nachrichtenticker: Heise online. Abgerufen am 29.05.2014.
[652] *Hägele/Schäfer*, in: Gevatter/Grünhaupt (Hrsg.), Handbuch der Mess- und Automatisierungstechnik in der Produktion, 2006.
[653] *Kirsch,* CT Magazin für Computertechnik Nr. 22, 2011, 43.

Möglichkeiten führt, ist sicherlich dabei nicht ausgeschlossen, sondern wünschenswert. Die Robotik beschäftigt sich dabei mit einer sog. manipulativen Intelligenz: Mit Hilfe von Robotern können gefährliche Tätigkeiten oder auch immer gleiche Manipulationen, wie das Entschärfen von Bomben auf Roboter verlagert werden. Der Grundgedanke ist es, Systeme (Roboter) zu schaffen, die intelligente Verhaltensweisen von Lebewesen nachvollziehen können.

III. Wertungsmöglichkeiten der Künstlichen Intelligenz

Beim autonomen Fahren tritt anstelle des Menschen die Künstliche Intelligenz oder ein Algorithmus i. V. m. Machine Learning (nachfolgend nur Künstliche Intelligenz), um das Fahrzeug zu führen. Der Künstlichen Intelligenz müssen somit gewisse Wertungsmöglichkeiten zu gestanden werden, denn auch gem. § 1 e Abs. 2 Nr. 1, Nr. 2 Alt. 1 StVG müssen Kraftfahrzeuge mit autonomer Fahrfunktion über eine technische Ausrüstung verfügen, die in der Lage ist,

die Fahraufgabe innerhalb des jeweils festgelegten Betriebsbereichs selbstständig zu bewältigen, ohne dass eine fahrzeugführende Person in die Steuerung eingreift oder die Fahrt des Kraftfahrzeugs permanent von der Technischen Aufsicht überwacht wird, selbstständig den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen und die über ein System der Unfallvermeidung verfügt, das auf Schadensvermeidung und Schadensreduzierung ausgelegt ist.

Fraglich ist indes, ob darüber hinausgehende Einschränkungen berücksichtigt werden müssen.[654] Zu denken ist etwa an Ad-hoc-Verkehrszeichen oder Weisungen von Verkehrspolizisten, welche von autonomen Fahrfunktionen (noch) nicht erfasst werden können.[655] Nach § 1 e Abs. 2 Nr. 3 StVG müssen Kraftfahrzeuge mit autonomer Fahrfunktion technisch so ausgerüstet sein, dass sie sich unter bestimmten Umständen (siehe § 1 e Abs. 2 Nr. 3, 5, 7, 8, 10 StVG) in einen risikominimalen Zustand versetzen können. Notwendig ist dies, wenn die Fortsetzung der Fahrt nur unter Verletzung des Straßenverkehrsrechts möglich ist – etwa weil eine Ampel aufgrund eines technischen Defekts nicht auf grün umspringt.[656] Dabei wird der Begriff des risikominimalen Zustands in § 1 d Abs. 4 StVG

[654] *von Bodungen/Gatzke*, RDi 2022, S. 354.
[655] *Hilgendorf*, JZ 2021, S. 444 (447).
[656] *von Bodungen/Gatzke*, RDi 2022, S. 354.

legaldefiniert und ist danach ein solcher Zustand, in dem das Fahrzeug mit aktivierter Warnblinkanlage an geeigneter Stelle zum Stillstand kommt, um größtmögliche Sicherheit für die Fahrzeuginsassen, andere Verkehrsteilnehmende und Dritte zu gewährleisten.

Bereits die Ethikkommission Automatisiertes und Vernetztes Fahren ist in ihrem Bericht von Juni 2017 unter Ziff. 5 zu der Erkenntnis gekommen, dass automatisierte und vernetzte Technik Unfälle so gut wie praktisch möglich vermeiden sollte. Die Technik muss nach ihrem jeweiligen Stand so ausgelegt sein, dass kritische Situationen gar nicht erst entstehen; dazu gehören auch Dilemma-Situationen, also eine Lage, in der ein automatisiertes Fahrzeug vor der „Entscheidung" steht, eines von zwei nicht abwägungsfähigen Übeln notwendig verwirklichen zu müssen. Mit der Einführung des § 1e Abs. 2 Nr. 2 lit. c) StVG zum 28.07.2021 wurde dazu die Neuerung ins Gesetz aufgenommen, dass Kraftfahrzeuge mit autonomer Fahrfunktion für den Fall einer unvermeidbaren alternativen Gefährdung von Menschenleben keine weitere Gewichtung anhand persönlicher Merkmale vornehmen dürfen.[657]

Bereits im Oktober 2016 auf den 30. Münchner Medientagen hat die damalige Bundeskanzlerin Angela Merkel gefordert, dass Algorithmen, die Internetdienste für das Filtern von Informationen nutzen, transparent bleiben müssten. Die Mediennutzung werde immer stärker durch Algorithmen, Bots und intelligente Empfehlungssysteme beeinflusst. Algorithmen führten dazu, dass etwa Leser verstärkt im Netz nur noch die Themen angeboten bekämen, die ihrem Suchverhalten entsprechen. Das könne ihre Fähigkeit verringern, sich mit anderen Meinungen auseinanderzusetzen.[658] Dabei gibt es schon Regelungen, die zur Neutralität von Algorithmen führen sollen. Bereits im Erwägungsgrund 71 DSGVO findet sich eine Verpflichtung zur „Neutralität von Algorithmen". Ähnlich wie für das Scoring in § 28b Nr. 1 BDSG werden für das Profiling ein „geeignetes mathematisches oder statistisches Verfahren" und der Ausschluss diskriminierender Rechenverfahren verlangt.[659] Im Falle von § 1e Abs. 2 Nr. 2 lit. c) StVG geht man sogar einen Schritt weiter und untersagt – zu Recht – einer Künstlichen Intelligenz, eine Wertung über die Qualität von

[657] BT-Drucks. 19/27439 vom 09.03.2021, S. 1-2.

[658] https://www.heise.de/newsticker/meldung/Algorithmen-und-Scoring-Maas-fordert-digitales-Anti-Diskriminierungsgesetz-3761722.html?seite=2 (abgerufen 07.03.2023).

[659] *Härting*, ITRB 2016, S. 209-211.

Menschenleben auszuüben.

Wirklich erfreulich ist, dass sich damit auch die vermeintlich philosophische Frage von Gesellschaftsforschern erledigt hat, ob ein Algorithmus darüber werten darf, ob ein kleines Mädchen einen höherrangigen Wert für die Gesellschaft darstellt, als ein Al-Qaida-Führer. Auch wurde die philosophische Frage zur Anwendung der Robotergesetze (englisch: Three Laws of Robotics) von Isaac Asimov damit einfach ausgeschlossen. Es gibt für die Künstlichen Intelligenz keine Grundlagen für eine moralische Entscheidung über Menschenleben, weil sie über die Wertigkeit von Menschenleben nicht entscheiden darf. Sollte ein Hersteller dennoch eine solche Technologie verwenden, wird er sich erheblichen Schadenersatzforderungen der jeweils unterlegenen Person oder deren Angehörigen stellen müssen, z. B. nach § 823 Abs. 2 i. V. m. § 1e Abs. 2 Nr. 2 lit. c) StVG.

Neben dem Verbot einer qualitativen Wertung von Menschenleben bleibt aber die Frage der quantitativen Wertung offen: Es wäre nach dem Gesetzeswortlaut durchaus erlaubt, bei Kraftfahrzeugen mit autonomer Fahrfunktion z. B. einen Algorithmus zu implementieren, der unterscheidet, ob in einem unausweichlichen Unfall der Algorithmus eine Wahl trifft, ob eine Gruppe mit einer geringeren oder einer höheren Anzahl von Menschen gefährdet werden muss. An dieser Stelle sollte noch nachgebessert werden und auch hier sollte der Algorithmus ebenfalls keine Wertung vornehmen dürfen, sondern alle technischen Möglichkeiten ergreifen, damit es gar nicht erst zu einer solchen Entscheidung kommen muss.

Wenn man es positiv formuliert, könnte der neu geschaffene § 1e Abs. 2 Nr. 2 lit. c) StVG Modellcharakter haben und somit (hoffentlich) einen erheblichen Einfluss auf andere Bereiche des Rechts der Künstlichen Intelligenz haben. Dennoch muss der § 1e Abs. 2 Nr. 2 lit. c) StVG im Bereich der quantitativen Wertung von Menschen noch (dringend) nachgebessert werden.

Wirklich erfreulich ist, dass mit der Schaffung des § 1e Abs. 2 Nr. 2 lit. c) StVG die leidige Diskussion, ob der Algorithmus des Fahrzeuges besser den Genozid verübenden Taliban oder das unschuldige kleine Mädchen töten sollte, endgültig beendet wurde.

H. Haftung

Die EU-Kommission hat am 28. September 2022 einen **Entwurf für eine Richtlinie über KI-Haftung**[660] veröffentlicht. Ziel ist es, das bestehende europäische Haftungsrecht an die Herausforderungen durch künstliche Intelligenz (KI) anzupassen. Der Entwurf ergänzt die geplante KI-Verordnung (KI-VO) und die überarbeitete Produkthaftungsrichtlinie.

Hinter diesem speziellen Gesetz, welches als zunächst als Lex specials angesehen werden kann, steht die rechtlichen Haftungsbewertung von Herstellern, Eigentümern/Nutzern dar.[661] Entscheidend kommt es darauf an, wer eine kausale und zurechenbare Ursache für den Schadenseintritt gesetzt hat.[662] Die Feststellung von Verursachungsbeiträgen wird bei Schädigungen durch KI eine wesentliche Herausforderung sein. Handelt die KI-Technologie/der Roboter autonom und schädigt dabei einen Menschen oder Sachwerte, müssten zunächst die Verursachungsbeiträge technisch nachvollzogen werden, was im Regelfall sachverständige Hilfe erfordern dürfte.[663] Die Fähigkeit zum autonomen Handeln und künstliche Intelligenz führen dazu, dass nicht mehr jede Aktion einer Maschine unmittelbar von einem Menschen beeinflusst wird. Der Mensch gibt das System aus der Hand und dadurch wird eine Kausalitäts- und Zurechnungsbestimmung erschwert.[664] Bereits bei der Herstellung greifen die Beiträge der Beteiligten eng ineinander und abhängig vom Nutzerverhalten ist eine Weiterentwicklung der KI-Technologie möglich, unabhängig von Konstruktion und Programmierung durch den Hersteller.[665]

I. Richtlinie über KI-Haftung

Die Richtlinie verfolgt das Ziel, effektiven Rechtsschutz für geschädigte Parteien zu gewährleisten, die durch KI-Systeme Schäden erleiden, und die Innovationsfähigkeit der europäischen KI-Wirtschaft zu fördern.[666]

[660] Entwurf der EU-Richtlinie über KI-Haftung (COM/2022/496 final)
[661] Vgl. auch *Riehm*, ITR B 2014, 113.
[662] *Günther/Böglmüller*, BB 2017, 53 bis 58.
[663] *Groß/Gressel*, NZA 2016, 990, 996.
[664] *Günther/Böglmüller*, BB 2017, 53 bis 58.
[665] *Beck*, in: Japanisch-Deutsches Zentrum, Mensch-Roboter-Interaktionen aus interkultureller Perspektive, 2011, S. 124, 126
[666] Entwurf der EU-Richtlinie über KI-Haftung (COM/2022/496 final)

1. Anwendungsbereich

Die Richtlinie betrifft außervertragliche Haftungsansprüche und richtet sich an zwei zentrale Gruppen:

- Betreiber und Entwickler von KI-Systemen,
- Dritte, die KI-Systeme verwenden oder einsetzen.

Sie deckt dabei Schäden ab, die durch Handlungen oder Unterlassungen von Akteuren entstehen, die KI-Systeme in Verkehr bringen oder betreiben.

2. Beweislast und Haftungserleichterungen

Die Richtlinie sieht spezielle Regelungen zur Erleichterung der Beweislast für Geschädigte vor. Diese berücksichtigen die technische Komplexität und Intransparenz von KI-Systemen (sogenannte „Black-Box-Problematik“).

a) Offenlegungspflichten

- Geschädigte können von Betreibern oder Entwicklern die Offenlegung relevanter Informationen über das KI-System verlangen, wenn diese zur Beweisführung erforderlich sind.
- Unternehmen müssen die Offenlegung nur leisten, wenn ein Gericht die Notwendigkeit dieser Informationen anerkennt.

b) Vermutungen zur Kausalität

- Bei Verstößen gegen Sorgfaltspflichten, die für die Nutzung oder Entwicklung des KI-Systems gelten, wird eine widerlegbare Kausalitätsvermutung eingeführt. Es wird vermutet, dass der Schaden durch das fehlerhafte Verhalten des Betreibers oder Entwicklers verursacht wurde.
- Diese Vermutungsregel gilt insbesondere bei Verstößen gegen Bestimmungen der KI-VO (z. B. bei nicht ausreichendem Risikomanagement).

3. Verhältnis zur Produkthaftung

Die Richtlinie ergänzt die Produkthaftungsrichtlinie, die auf verschuldensunabhängige Haftung für fehlerhafte Produkte abstellt. Die KI-Haftungsrichtlinie ist verschuldensbasiert und regelt insbesondere:

- Fälle, in denen ein KI-System durch den Einsatz oder die Anwendung zu Schäden

führt, ohne dass ein Produktfehler im Sinne der Produkthaftungsrichtlinie vorliegt.

- Die Haftung für autonome Entscheidungen von KI-Systemen, die zu Schäden führen.

4. Ziele der Richtlinie

- Rechtsklarheit: Geschädigte erhalten ein effektives Mittel, ihre Ansprüche durchzusetzen, auch bei komplexen und undurchsichtigen KI-Systemen.
- Innovationsschutz: Unternehmen profitieren von Rechtssicherheit und einem innovationsfreundlichen Haftungsrahmen.
- Angleichung der Haftungsregime: Die Richtlinie harmonisiert die Haftungsregelungen innerhalb der EU, um Fragmentierung zwischen den Mitgliedstaaten zu vermeiden.

5. Kritik und Herausforderungen

- Schutzlücken: Die Richtlinie lässt wichtige Fragen zur Haftung autonomer KI-Systeme im Grenzbereich zwischen Produkthaftung und außervertraglicher Haftung offen.
- Verwaltungsaufwand: Die Anforderungen an Dokumentation und Offenlegung könnten insbesondere für KMUs belastend sein.
- Balance zwischen Opferschutz und Innovation: Die Richtlinie versucht, Opferrechte und Innovationsschutz auszubalancieren, was jedoch nicht in allen Punkten als gelungen gilt.

6. KI-Verordnung (KI-VO) RL KI-Haftung

Die KI-Verordnung (KI-VO)[667] und die EU-Richtlinie über KI-Haftung[668] ergänzen sich und bilden gemeinsam einen kohärenten Rechtsrahmen, der die Entwicklung, Nutzung und Haftung für Künstliche Intelligenz (KI) in der Europäischen Union regelt. Ihr Zusammenspiel basiert auf einer klaren Aufgabenteilung und dem Ziel, sowohl rechtliche als auch technische Anforderungen an KI-Systeme abzudecken.

[667] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828

[668] COM/2022/496 final

Die KI-VO und die EU-Richtlinie über KI-Haftung haben unterschiedliche Schwerpunkte. So legt die KI-VO technische Anforderungen an KI-Systeme fest, insbesondere zur Risikominimierung und zum Schutz von Grundrechten. Sie adressiert die Pflichten der Entwickler, Anbieter und Nutzer von KI-Systemen in verschiedenen Risikokategorien (z. B. Hochrisiko-KI). Zentrale Punkte sind die Transparenzpflichten, Risikoanalysen und die Schaffung eines Zertifizierungs- und Überwachungsmechanismus. Ziel der KI-VO ist die Ex-ante-Regulierung zur Verhinderung von Schäden durch die Einhaltung technischer Standards. Geschädigten effektive Möglichkeiten zur Geltendmachung von Schadensersatzansprüchen zu geben, indem spezifische Beweiserleichterungen und Kausalitätsvermutungen eingeführt werden. Insbesondere wird vermutet, dass ein Schaden auf die Nutzung einer KI zurückzuführen ist, wenn Sorgfaltspflichten verletzt wurden. Die Richtlinie knüpft somit an die Vorgaben der KI-VO an, indem Verstöße gegen deren technische und organisatorische Anforderungen als Grundlage für die Haftung herangezogen werden können. Dadurch entstehen klare Haftungsmaßstäbe, die sowohl den Opferschutz als auch die Rechtssicherheit für Betreiber und Entwickler stärken.

Das Zusammenspiel beider Regelwerke zeigt sich insbesondere darin, dass die KI-VO die Standards für die Sorgfaltspflichten vorgibt, deren Missachtung eine Haftung nach der Richtlinie auslösen kann. Die KI-VO schafft somit präventive Vorgaben, während die Haftungsrichtlinie für den Schadensfall rechtliche Absicherung bietet. Beide Instrumente fördern zudem die Harmonisierung des Rechtsrahmens innerhalb der EU, indem sie Fragmentierungen zwischen den Mitgliedstaaten vermeiden und einheitliche Regeln für den Umgang mit KI schaffen. Gleichzeitig wird durch diese Verzahnung eine Balance zwischen Innovationsförderung und Verbraucherschutz erreicht.

Ein konkretes Beispiel für die Zusammenarbeit der Regelwerke wäre ein Schaden, der durch eine Hochrisiko-KI verursacht wurde, etwa im Bereich der medizinischen Diagnostik. Verstößt der Betreiber gegen die Vorgaben der KI-VO, indem er mangelhafte Datenqualität verwendet, könnte dieser Verstoß nicht nur zu Sanktionen nach der Verordnung führen, sondern auch die Grundlage für Schadensersatzforderungen nach der Haftungsrichtlinie bilden. Für Geschädigte greifen hier Beweiserleichterungen und eine Kausalitätsvermutung, die eine effektive Rechtsdurchsetzung ermöglichen.

Das Zusammenspiel von KI-VO und Haftungsrichtlinie stärkt sowohl die Prävention von Schäden als auch die Kompensation im Schadensfall. Während die KI-VO durch klare technische Standards Vertrauen in den sicheren Einsatz von KI-Systemen schafft, gewährleistet die Haftungsrichtlinie, dass Opfer von KI-bedingten Schäden einen wirksamen Rechtsschutz erhalten. Diese duale Herangehensweise bildet die Grundlage für ein innovationsfreundliches und zugleich verbraucherorientiertes Regelwerk in der Europäischen Union. Der Entwurf der KI-Haftungsrichtlinie ist ein bedeutender Schritt zur Anpassung des Haftungsrechts an die Besonderheiten von KI-Systemen. Insbesondere die Einführung von Beweiserleichterungen und Kausalitätsvermutungen adressiert die Schwierigkeiten, die sich aus der Intransparenz von KI ergeben. Dennoch bleibt die Richtlinie in einigen Punkten unklar und wird in der Rechtspraxis auf ihre Wirksamkeit geprüft werden müssen. Die Harmonisierung mit der Produkthaftungsrichtlinie und der KI-VO wird entscheidend sein, um ein kohärentes Haftungsregime in der EU zu schaffen.[669]

II. Herstellerhaftung

Die Erstellung von KI-Systemen wirft grundsätzlich keine besonderen Rechtsfragen gegenüber der allgemeinen Produkthaftung und der für sie entwickelten Pflichten auf.[670] Folglich lassen sich alle Herstellerpflichten bzw. darauf bezogene Fehlerkategorien wie Konstruktionsfehler oder Fertigungsfehler auf die Herstellung von KI-System anwenden. So ist der Hersteller von KI-Systemen verpflichtet, alle allgemein oder ihm speziell zugänglichen Erkenntnisquellen auszuschöpfen, um Gefahren von den von ihm in Verkehr gebrachten Produkten abzuwehren.[671] Maßgeblich ist, ob dem Hersteller bereits bei der Inverkehrgabe die Fehler bekannt sein mussten.[672] Produktrisiken, die erst später bekannt werden, führen nicht dazu, dass dem Hersteller ein Konstruktionsfehler anzulasten wäre.[673] Hierbei handelt es sich vielmehr um einen Entwicklungsfehler, so dass allein nachträgliche Pflichten im

669 *Osborne Clarke*: Analyse der neuen EU-Haftungsrichtlinien

670 So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

671 BGH, 12.11.1991 – VI ZR 7/91, BGHZ 116, 60, 70 f. = VersR 1992, 96, 99; 17.10.1989 – VI ZR 258/88, NJW 1990, 906, 907 f.; 23.5.1952 – III ZR 168/51, NJW 1952, 1091; *Kullmann*, NJW 2002, 30, 32; *Kullmann,* in: Kullmann/Pfister, Produzentenhaftung, Stand 1/2012, Knz. 1520, S. 7; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 378; *Spindler,* in: Beck OGK/BGB, § 823 Rn. 607, 610

672 So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

673 *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 71, 103 ff.; vgl. *Jänisch/Schrader/Reck*, NZV 2015, 313, 317 „zum Zeitpunkt des Inverkehrbringens"; *Vogt*, NZV 2003, 153, 159.

Rahmen der Produktbeobachtung eingreifen können.[674] In dem der KI so verwandten IT-Umfeld, wird z. B. vertreten, dass auch wenn IT-Systeme zuweilen sehr komplex sind, nichts daran vorbei führt, dass bekannte Sicherheitsprobleme unverzüglich beseitigt werden müssen, bevor das Produkt auf den Markt gebracht wird.[675]

1. Herstellerpflichten

Auch der Hersteller eines KI-Systems muss den Käufer eines solchen Systems über den richtigen Gebrauch und die Inbetriebnahme instruieren. Besteht das KI-System lediglich aus einem Algorithmus, so muss auch der Hersteller bspw. eines Kreditscores den Verwender des Scores (Betreiber) auf die Risiken der Verwendung des Scores hinweisen. Insbesondere auch um Haftungsfälle nach § 824 BGB „Kreditgefährdung" zu vermeiden (siehe 4.). Bei der Verwendung von Robotern und vergleichbaren technischen KI-Systemen, wird es sich ggf. um Nutzer und Betreiber handeln, die selbst in einer Weise professionell tätig sind, so dass sich hier die Instruktionspflichten entsprechend erheblich reduzieren können.[676] Dabei ist natürlich zu berücksichtigen, dass Kreditreferenten oder Ärzte[677] häufig zwar über das fachliche Know-how verfügen, aber zuweilen nicht über das technische Fachwissen, um ein KI-System zu verstehen und ohne Einweisung zu verwenden. Bei Fahrzeugen, die mit KI-Systemen für autonomes Fahren ausgestattet sind, ist natürlich zu berücksichtigen, dass es sich bei den Käufern und Fahrern der Fahrzeuge i. d. R. nicht um KI-Experten handelt. [678]

2. Produktbeobachtungspflichten

Auch dem Hersteller eines KI-Systems obliegen Produktbeobachtungspflichten, denn nach der Inverkehrgabe wird der Hersteller nicht vollständig von seiner Verantwortung für das Produkt frei. Der Begriff der Produktbeobachtungspflicht steht quer zu den Konstruktions-, Fabrikations- und Instruktionspflichten des Herstellers, weil sich die Verletzung der Produktbeobachtungspflicht nicht ohne Weiteres in einer negativ bewerteten Produkteigenschaft – einem „Fehler" – niederschlägt.[679] Die Anerkennung von

---

[674] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[675] *Meier*/*Wehlau*, CR 1990, 95, 97; s. auch *Schneider*/*Günther*, CR 1997, 389 ff.; *Bartsch*, CR 2000, 721, 722 ff.

[676] BGH, 14.05.1996 – VI ZR 158/95 = NJW 1996, 2224, 2226 m. w. N. – Grimm'sches Leitrad; näher *Spindler,* in: BeckOGK/BGB, § 823 Rn. 607.

[677] Wobei hier spezielle Pflichten nach dem Medizinproduktegesetz (MPG) bestehen, siehe Kapitel E. „Cyborg" u. a. § 14 MPG i. V. m. Medizinprodukte-Betreiberverordnung. S. dazu *Lippert,* in: Deutsch/Lippert/Ratzel/Tag, MPG, 2. Aufl. 2010, § 2 MPBetreibV Rn. 1 ff.

[678] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[679] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 836 bis 837.

Produktbeobachtungspflichten verdankt sich dem Umstand, dass die Sorgfaltspflichten des Warenherstellers zeitpunktbezogen sind und damit auf historischen Risikoeinschätzungen und Gefahrsteuerungsmöglichkeiten beruhen.[680] Die Intensität der Produktbeobachtungspflicht richtet sich nach den allgemeinen Regeln, d. h. sie ist abhängig einerseits vom Umfang des drohenden Schadens und dem Grad der Gefahr, andererseits von der Möglichkeit und wirtschaftlichen Zumutbarkeit von Beobachtungsmaßnahmen.[681] Sie ist generell schwächer ausgeprägt bei bewährten Produkten, die schon seit langer Zeit und in großer Stückzahl am Markt sind, und besonders intensiv bei komplexen Neuentwicklungen mit großem Schädigungspotential.[682] Bei KI-Systemen wie z. B. Robotern, ist ein Vergleich zu komplexen IT-Systemen möglich;[683] denn gerade aus dem Wissen um die objektive Unvermeidbarkeit von Programmierungsfehlern („Bugs") erwächst eine Pflicht des Herstellers zur besonders sorgfältigen Produktbeobachtung.[684] Die Verpflichtung zur aktiven Produktbeobachtung betrifft die Generierung von Informationen über mögliche Schadensrisiken des eigenen Produkts.[685] Als Quellen für solche Informationen kommen Erfahrungen mit Konkurrenzprodukten gleicher oder ähnlicher Beschaffenheit in Betracht, sofern derartige Daten dem Hersteller zugänglich sind.[686] Bei drohenden Gefahren für Leib und Leben ist sogar bereits ein ernstzunehmender Verdacht hinreichend, um Warnpflichten auszulösen[687]; gerade bei autonom fahrenden Fahrzeugen[688] werden daher hier die Pflichten zur Beobachtung besonders intensiviert. Bei Sachschäden und nicht akuter Bedrohung kann sich der Produzent im Falle eines Verdachts zunächst auf eigene Ermittlungen und aktive Beobachtung des Produktes beschränken, ohne vor dem Produkt oder dessen spezifische

[680] Grdl. BGHZ 80, 199, 202 ff. = NJW 1981, 1606, 1607 f. – Benomyl; genauso BGHZ 80, 186, 191 = NJW 1981, 1603, 1604 – Apfelschorf.

[681] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 838.

[682] BGHZ 99, 167, 170 f. = NJW 1987, 1009, 1010 – Lenkerverkleidung; BGH, NJW 1994, 517, 519 – Gewindeschneidemittel I; NJW-RR 1995, 342, 343 – Gewindeschneidemittel II.

[683] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[684] *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 174 f.; *Spindler*, in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich, erscheint demnächst, S. 45; a. A. LG Köln, 21.07.1999 – 20 S 5/99, CR 2000, 362 = NJW 1999, 3206: Keine Pflicht zur Warnung bei nachträglichen Erkenntnissen über Virenbefall einer Diskette.

[685] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 839.

[686] *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 375.

[687] BGH, 17.03.1981 – VI ZR 191/79, BGHZ 80, 186, 192 = NJW 1981, 1603; OLG Frankfurt, 11.11.1993 – 1 U 254/88, NJW-RR 1995, 406, 408; 29.09.1999 – 23 U 128/98, NJW-RR 2000, 1268, 1270; OLG Karlsruhe, 27.3.1996 – 7 U 61/94, VersR 1998, 63, 64 f.; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 314.

[688] Allgemein *Jänich/Schrader/Reck*, NZV 2015, 313, 318 m. w. N.

Verwendung warnen zu müssen.[689] Im Einzelnen ist zwischen aktiver und passiver Produktbeobachtung zu unterscheiden: Die passive Produktbeobachtungspflicht beschränkt sich darauf, Beschwerden von Kunden über Schadensfälle und Sicherheitsdefizite entgegen zu nehmen, zu sammeln und systematisch auszuwerten.[690] Derartige Maßnahmen sind mit geringem wirtschaftlichen Aufwand möglich und generieren einen hohen Nutzen, weil sie auf reale Erfahrungen gestützt und deshalb besonders verlässlich sind, wirtschaftlich aufwändige Untersuchungs- und Testverfahren erübrigen und dem Hersteller kostenlos, ohne jeden Suchaufwand, zur Verfügung gestellt werden.[691] Auch eine Beobachtungspflicht im Hinblick auf das Zusammenwirken der eigenen mit fremden Produkten ist von der Rechtsprechung für fremd produziertes Zubehör entwickelt worden.[692] Ob diese – bislang vereinzelt gebliebene – Rechtsprechung tatsächlich auf eine Beobachtung der Interaktion von KI-Systemen (z. B. Robotern) mit allen möglichen anderen, sich in der Umgebung befindlichen Produkten erweitert werden kann, erscheint allerdings angesichts der Uferlosigkeit der daraus resultierenden Pflichten mehr als zweifelhaft.[693] Die Rechtsprechung schießt hier über ihr Ziel hinaus: Eine generelle Ausdehnung der Beobachtungspflichten auf Zubehörteile oder Kombinationsgefahren kann nicht allein damit begründet werden, dass der Hersteller ohnehin zur Beobachtung der Produkte verpflichtet ist. Grundsätzlich ist der Hersteller nur für die Gefahren verantwortlich, die er selbst geschaffen hat, nicht aber für Gefahrenerhöhungen, die durch Dritte verursacht werden,[694] erst recht, wenn die Zubehörprodukte wesentlich später nach Entwicklung, Konstruktion und Fabrikation auf den Markt gebracht werden.[695] Jedenfalls muss es als ausreichend angesehen werden, wenn der Hersteller den Produktbenutzer allgemein dahingehend instruiert, dass nur von ihm selbst freigegebene bzw. als unbedenklich eingestufte Zubehörteile gefahrlos benutzt werden können und dass die Benutzung nicht autorisierten Zubehörs auf Gefahr des Benutzers

---

689 BGH, 17.03.1981 – VI ZR 191/79, BGHZ 80, 186 (192) = NJW 1981, 1603; *Kullmann*, NJW 1996, 18 (23).

690 BGHZ 99, 167, 170 f. = NJW 1987, 1009, 1010 – Lenkerverkleidung; BGH, NJW 1994, 517, 519 – Gewindeschneidemittel I; NJW-RR 1995, 342, 343 – Gewindeschneidemittel II.

691 MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 839.

692 Grundlegend dazu BGH, 09.12.1986 – VI ZR 65/86 , BGHZ 99, 167 = NJW 1987, 1009 – Honda = CR 1987, 230; dazu *Ulmer*, ZHR 152, 564, 570 ff.; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 25 Rn. 178 ff.; *Kullmann,* in: Kullmann/Pfister, Produzentenhaftung, 1/2012, Knz. 1520, S. 52.

693 So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

694 Ähnlich *Ulmer*, ZHR 152, 564, 579; *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 25 Rn. 222; zust. *v. Bar,* in: v. Bar, Produktverantwortung und Risikoakzeptanz, 1998, S. 29, 36.

695 So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

erfolgt.[696] Die Verpflichtung zur aktiven Produktbeobachtung betrifft die Generierung von Informationen über mögliche Schadensrisiken des eigenen Produkts.[697] Als Quellen für solche Informationen kommen Erfahrungen mit Konkurrenzprodukten gleicher oder ähnlicher Beschaffenheit in Betracht, sofern derartige Daten dem Hersteller zugänglich sind.[698] Im Übrigen ist das wissenschaftlich-technische Fachschrifttum auszuwerten, soweit es für das eigene Angebot relevant ist.[699] Die Reichweite dieser Verpflichtung im Einzelnen hängt wiederum vom Schädigungspotential des Produkts, von seinem Preis und den darauf gestützten berechtigten Sicherheitserwartungen seiner Nutzer und schließlich von dem Aufwand ab, mit dem sich entsprechende Informationen beschaffen lassen.[700]

3. Reaktionspflichten

Die Verletzung der Produktbeobachtungspflicht allein verursacht keine Schäden, sondern diese entstehen erst dadurch, dass es der Hersteller unterlassen hat, aus den im Wege der Beobachtung gewonnenen Informationen die gebotenen Konsequenzen zu ziehen oder es versäumt hat, tatsächlich verfügbare Informationen zu erheben oder auszuwerten, und sich dadurch von vornherein jeder Reaktionsmöglichkeit begeben hat. Insofern ist die Produktbeobachtungspflicht nur Mittel zum Zweck der Reaktion. Die Frage, wie diese Reaktion im Einzelnen beschaffen sein muss, markiert einen der Brennpunkte des aktuellen Produkthaftungsrechts.[701] Die Reaktionspflichten gelten auch für KI-Systeme und wenn es sich nur um die Verwendung eines Algorithmus handelt. Sie sind daher entsprechend von Hersteller von KI-Systemen zu berücksichtigen und anzuwenden.

---

[696] *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 25 Rn. 187 ff. In der Tendenz auch BGH, 09.12.1986 – VI ZR 65/86 , BGHZ 99, 167, 174 = NJW 1987, 1009 = CR 1987, 230.

[697] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 839.

[698] *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 375.

[699] BGHZ 80, 199, 202 f. = NJW 1981, 1606, 1607 f. – Benomyl; BGH, NJW 1990, 906, 907 f. – Pferdeboxen.

[700] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 809.

[701] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 823 Rn. 840.

4. Rückrufpflichten

Eine Folge der Beobachtungspflicht ist natürlich die Rücknahme des entsprechenden fehlerhaften KI-Systems, um damit dafür zu sorgen, dass durch das fehlerhafte KI-System kein weiterer Schaden entsteht. Umstritten ist, ob und ggf. unter welchen Voraussetzungen der Hersteller darüber hinaus gehalten sein kann, die bereits vermarkteten Produkte zurückzurufen, um sie auszutauschen oder zu reparieren, und wer die Kosten für derartige Maßnahmen zu tragen hat. Nach einer Ansicht sind Rückrufpflichten des Herstellers abzulehnen,[702] weil der Hersteller seinen Gefahrsteuerungspflichten bereits mit der Herausgabe einer Warnung vor den Produktgefahren genüge[703] und bei Anerkennung weitergehender Rückruf- und Reparaturpflichten die Wertungen des Gewährleistungsrechts beiseitegeschoben würden.[704] Grundsätzlich neigt die Rechtsprechung dazu,[705] den Schaden auf die Kosten des Ausbaus der fehlerhaften Teile zu beschränken, nicht jedoch die Kosten für den Einbau neuer, fehlerloser Teile zu erstatten[706] – außer es handelt sich wiederum um Schäden an Leben und Gesundheit, etwa Herzschrittmacher (siehe „Cyborg"). Jedoch ist der Hersteller verpflichtet, Gefahren für von § 823 Abs. 1 BGB geschützte Rechtsgüter zu vermeiden, so dass zumindest ein Anspruch aus § 1004 BGB anzunehmen ist.[707] Daher hat der Hersteller die Kosten in vollem Umfang[708] jedenfalls für die Rücknahme des Produktes zu tragen, wenn von dem Produkt Gefahren für andere Rechtsgüter drohen.[709] Bei einem drohenden Schaden allein am Produkt selbst genügt eine Warnung des Produktbenutzers, da ansonsten das Äquivalenzinteresse und die Erwartung, das Produkt nutzen zu können, geschützt würde.[710] Daraus ist für KI-Systeme grundsätzlich erst einmal zu schließen, dass aus dem Produkthaftungsrecht prinzipiell keine Pflicht abgeleitet wird, dass KI-Systeme und

---

[702] LG Frankfurt a. M., VersR 2007, 1575 f. – Röntgengerät; *Brüggemeier*, ZHR 152, 1988, 511, 525 f.; ders., DeliktsR Rn. 565 ff.; ders., RabelsZ 66, 2002, 193 ff.; *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 340 ff., § 39 Rn. 2 ff. (wenn auch mit Differenzierungen).

[703] *Brüggemeier,* ZHR 152, 1988, 522, 525; *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 344 ff., 354 ff.

[704] LG Frankfurt a. M., VersR 2007, 1575 – Röntgengerät; *Brüggemeier*, ZHR 152, 1988, 511, 525 f.; *Foerste,* in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24 Rn. 349 ff., § 39 Rn. 6; *Foerste,* DB 1999, 2199, 2200.

[705] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[706] OLG Stuttgart, 29.07.1966 – 10 U 1/66, NJW 1967, 572; zust. OLG Düsseldorf, 31.05.1996 – 22 U 13/96, NJW-RR 1997, 1344, 1346.

[707] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[708] *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflichtig der Produzenten, 1994, S. 223 f.; abw. *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 367: ausnahmsweise Kostenteilung.

[709] OLG Düsseldorf, 31.05.1996 – 22 U 13/96, NJW-RR 1997, 1344, 1345; OLG Karlsruhe, 02.04.1993 – 15 U 293/91, NJW-RR 1995, 594, 597; *Wagner*, in: MünchKomm/BGB, 6. Aufl. 2013, § 823 Rn. 677; *Hager*, in: Staudinger, BGB, 2009, § 823 Rn. 26, je m. w. N.; *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, 1994, S. 236; nur bei Gefahren für Leib und Leben: Michalski, BB 1998, 961, 965.

[710] Zutr. *Foerste*, DB 1999, 2199, 2200; *Taschner/Frietsch*, ProdHaftG, 2. Aufl. 1990, Einführung Rn. 89; ähnlich *Pieper*, BB 1991, 985, 988 mit dem Hinweis, dass andernfalls eine „deliktische Gewährleistung" entstünde; anders *v. Westphalen*, DB 1999, 1369, 1370; *Koch*, AcP 203, 2003, 603, 624 ff., 631 f., will Ersatz der Aus- und Einbaukosten unter Ausschluss von Materialkosten gewähren.

insbesondere seine Software, die KI-Systeme wie Roboter oder Autos steuern, stets gepflegt und aktualisiert werden müssen, da es genügen würde, dass der Kunde das Produkt nicht mehr benutzt[711], um seine Integritätsinteressen zu wahren.[712] Hierbei ist aber zu berücksichtigen, dass sich aus geschlossen Wartungs- und Betreuungsverträgen (z. B. bei Cyborg und deren Implantate) etwas anders ergeben kann.

5. Beweislast

Bei komplexen KI-Systemen die ggf. fehlerhaft sind, ist die Frage der Beweisbarkeit des Mangels als erheblich in der Praxis anzusehen. Grundsätzlich ist davon auszugehen, dass die von der Rechtsprechung entwickelten Regeln zur Beweislastumkehr zugunsten des Geschädigten im Rahmen der Produkthaftung[713] naturgemäß auch bei der deliktischen Haftung für Roboter eingreifen. Die Gründe für diese Beweislastumkehr – die fehlenden Einsichtsmöglichkeiten des Geschädigten in die Vorgänge in der Sphäre des Schädigers[714] – sollten mutatis mutandis auch auf die Betreiber von KI-Systemen übertragen werden.[715] Zwar ist vereinzelt gefordert worden, von dieser Beweislastverteilung generell (also auch für den vertragsrechtlichen Bereich) für Roboter und damit auch für andere KI-Systeme abzukehren, da sich nicht immer klären lasse, worauf eine Fehlfunktion eines Roboters beruhe, etwa auf der falschen Auswertung von Informationen aus seiner Umgebung oder von der falschen Eingabe von Informationen.[716] Eine derartige Rückverlagerung der Beweislast auf den Geschädigten würde indes die eigentlichen Gründe für die Beweislastumkehr verkennen, namentlich die bessere Beherrschung der Gefahrenquelle „komplexes Maschinensystem"; nur dann, wenn tatsächlich die Fehlfunktionen auf einem Fehlgebrauch beruhen, kann die Darlegungs- und Beweislast nicht erleichtert werden.[717]

In der Praxis wird es schwierig sein, die notwendige Kausalität plausibel darzulegen. Haftet der Hersteller aus seiner Herstellerhaftung oder war eine Handlung des Betreibers kausal

[711] Siehe zur Nichtbenutzung auch *Molitoris*, NJW 2009, 1049, 1050 f.; *Klindt*, BB 2009, 792, 793; *Spindler,* in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich, erscheint demnächst, S. 50.

[712] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[713] Siehe *Spindler,* in: BeckOGK/BGB, § 823 Rn. 663 ff.; *Wagner,* in: MünchKomm/BGB, 6. Aufl. 2013, § 823 Rn. 684 ff. m. w. N.

[714] BGH, 26.11.1968 – VI ZR 212/66, BGHZ 51, 91, 104 f. = NJW 1969, 269, 275 – Hühnerpest; *Spindler*, in: BeckOGK/BGB, § 823 Rn. 663; *Wagner*, in: MünchKomm/BGB, 6. Aufl. 2013, § 823 Rn. 623.

[715] *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

[716] Dies erkennt im Ansatz auch *Lutz*, NJW 2015, 199, 120; wesentlich skeptischer dagegen generell *Hanisch*, in: Hilgendorf (Hrsg.), Robotik im Kontext zwischen Recht und Moral, 2014, S. 27, 38.

[717] So *Spindler* für Roboter und autonomes Fahren, CR 2015, 766 bis 776.

für den entstandenen Schaden. So wird z. B. im Bereich des autonomen Fahrens mit einer erheblichen Beweisschwierigkeit gerechnet, da nur mit Problemen aufklärbar sei, worauf ein Unfall beruhe, ob auf einem Fehler des Steuerungssystems oder einem Eingreifen des Fahrers.[718] Arbeiten KI-Systeme mit „Flugschreibern" vergleichbaren Geräten oder mit sog. Logfiles, so lässt sich daraus relativ einfach entnehmen, wer für den Schaden kausal verantwortlich ist.[719] Anders ist die Haftung natürlich bei der Verwendung von reinen Algorithmen zu betrachten. Hier kann nur mittels eines mathematischen Beweisverfahrens ermittelt werden, dass ein mangelhafter Algorithmus kausal für den entstandenen Schaden gewesen ist. Grundsätzlich obliegt auch bei einem KI-System dem Geschädigten die Pflicht, den Beweis für eine Rechtsverletzung zu erbringen, dazu gehört die Mangelhaftigkeit des KI-Systems sowie der Nachweis, dass der Produktfehler im Organisationsbereich des Herstellers entstanden ist und bereits zum Zeitpunkt des Inverkehrbringens vorlag.[720] Bezogen auf die objektive Verkehrspflichtverletzung als auch des Verschuldens greift zugunsten des Geschädigten eine Beweislastumkehr ein,[721] wonach sich der Hersteller in Bezug auf alle seine Hilfskräfte zu entlasten hat.[722] Hat dagegen der Hersteller des KI-Systems eine ordnungsgemäße Instruktion gegenüber dem Betreiber erbracht und wäre dieser Schaden bei einer ordnungsgemäßen Instruktion nicht eingetreten, so greift keine Beweiserleichterung.[723] Auch bei Verletzungen der Produktbeobachtungspflicht greift keine Beweislastumkehr zugunsten des Geschädigten hinsichtlich des objektiven Pflichtverstoßes ein, da hier nur allgemein zugängliche Informationen in Rede stehen, zu denen der Geschädigte notfalls durch Sachverständigengutachten ebenso Zugang wie der Hersteller hat.[724]

---

[718] So *Jänich/Schrader/Reck*, NZV 2015, 313, 315; *Lutz*, NJW 2015, 119, 120; Beispielszenario bei: *Schuhr,* in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 13, 17.

[719] Dies erkennt im Ansatz auch *Lutz*, NJW 2015, 199, 120; wesentlich skeptischer dagegen generell *Hanisch,* in: Hilgendorf (Hrsg.), Robotik im Kontext zwischen Recht und Moral, 2014, S. 27, 38.

[720] *Spindler,* in: BeckOGK/BGB, § 823 Rn. 666 f.

[721] BGH, 17.03.1981 – VI ZR 191/79, BGHZ 80, 186, 196 f. = WM 1981, 544; bestätigt wiederum in BGH, 11.06.1996 – VI ZR 202/95, NJW 1996, 2507, 2508; 02.02.1999 – VI ZR 392/97, VersR 1999, 456; *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 30 Rn. 62 ff.

[722] BGH, 17.10.1967 – VI ZR 70/66, NJW 1968, 247 ff.; *Wagner*, in: MünchKomm/BGB, 6. Aufl. 2013, § 823 Rn. 684 f

[723] Vgl. BGH, 02.03.1999 – VI ZR 175/98, DB 1999, 891, 891; OLG Frankfurt, 11.03.1998 – 23 U 55/97, NJW-RR 1999, 27, 30.

[724] Vgl. die in BGH, 17.03.1981 – VI ZR 191/79, BGHZ 80, 186, 195 ff. = WM 1981, 544 aufgestellten Grundsätze; s. auch BGH, 12.11.1991 – VI ZR 7/91, BGHZ 116, 69, 72 f. = ZIP 1992, 38, 40 ff.; krit. demgegenüber *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 30 Rn. 89; *Tiedtke*, in: FS Gernhuber, 1993, S. 471, 480 f.

6. Deliktische Haftung

Der Einsatz von KI als Gehilfen für den Menschen wirft neben vertragsrechtlichen Problemen[725] insbesondere Fragen der deliktischen Haftung, vor allem der Produkthaftung, auf.[726] Zentrale Bedeutung aufgrund des im Gegensatz zum ProdHaftG oder anderen Gefährdungshaftungstatbeständen nicht eingeschränkten Anwendungsbereichs hat die verschuldensabhängige deliktische Haftung, die grob in zwei Bereiche unterteilt werden kann, zum einen der Rechtsgutsverletzung nach § 823 Abs. 1 BGB, zum anderen der Schutzgesetzverletzung nach § 823 Abs. 2 BGB.[727]

Eine Verletzung der von § 823 Abs. 1 BGB geschützten Rechtsgüter durch KI, sind vor allem mittelbar infolge von Fehlfunktionen in Algorithmen oder Ausfällen bei autonomen/teilautonehmen Systemen denkbar.[728] Zunächst gilt es hier die Äquivalenz- von den Integritätsinteressen abzugrenzen: Das Allgemein- bzw. Verkehrsinteresse an sicheren Robotersystemen kann sich nicht auf das Interesse an einem funktionierenden Roboter beziehen, was allein das Äquivalenzinteresse betrifft. Systemstörungen können daher allein vertragsrechtlich bewältigt werden.[729] Vor allem Schäden bei autonomen/teilautonomen Systemen aufgrund von Fehlfunktionen der verwendenden KI (z. B. ein mangelhaft erstellter Algorithmus) dürften in aller Regel das Äquivalenzinteresse betreffen. Dies ist vor allem dann anzunehmen, wenn sich der Algorithmus nicht mehr von der Maschine, die durch den Algorithmus gesteuert wird, trennen lässt, wie z. B. beim Autonomen Fahren.[730] Dies hängt allerdings stark von den jeweiligen technischen Gegebenheiten ab: Lassen sich die Steuerungselemente vom Rest des Kfz trennen, insbesondere ohne dessen Funktionsfähigkeit zu beeinträchtigen, dürfte es sich um funktional abgrenzbare Teile handeln, so dass in

[725] Siehe dazu *Spindler,* in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 63, 66 f. m. w. N. wobei er es nur auf Roboter bezieht.

[726] Vgl. *Fleck/Thomas*, NJOZ 2015, 1393, 1398; *Lutz,* NJW 2015, 119 ff.; *Schuhr,* in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 13, 17; *Weisser/Färber,* MMR 2015, 506, 511.

[727] *Spindler*, CR 2015, 766 bis 776.

[728] Für den IT-Bereich: *Koch*, NJW 2004, 801, 802; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 259 f.; *Koch*, Versicherbarkeit von IT-Risiken, 2005, Rn. 185 ff., 355 ff., 632 ff.

[729] *Spindler,* Roboter, CR 2015, 766 bis 776.

[730] Dazu eingehend *Spindler,* in: Lorenz, Karlsruher Forum 2010: Haftung und Versicherung im IT-Bereich, 2011, S. 26 ff.; ders., in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich, erscheint demnächst, S. 36

diesen Fällen doch das Integritätsinteresse berührt wäre.[731]

Die Deliktische Haftung von § 823 Abs. 1 BGB setzt u. a. ein Verschulden vorausaus. Die §§ 276 bis 278 BGB bestimmen, was alles der Schuldner zu vertreten hat. Darunter fällt nicht nur eigenes Verschulden, sondern auch Verschulden seiner Hilfsperson sowie Beschaffungshindernisse, wenn der Schuldner ein Beschaffungsrisiko übernommen hat, und erst recht seine Zahlungsunfähigkeit. Dabei sind diese Normen keine Anspruchsgrundlagen, sondern nur Hilfsnormen, die das Haftungsmaß im Schuldverhältnis festlegen.[732] Ein Verschulden des Schuldners ist grundsätzlich nicht Anspruchsvoraussetzung, sondern wird lediglich vermutet.[733] Der Schuldner muss die Vermutung widerlegen und nach §§ 280 Abs. 1 S. 2, 286 Abs. 4 BGB beweisen, dass er die Pflichtverletzung nicht zu vertreten hat.[734] Gem. § 276 Abs. 1 BGB haftet der Schuldner für eigenes Verschulden, sprich er haftet für die beiden Schuldformen des Zivilrechts: Vorsatz und Fahrlässigkeit. Das BGB stellt sie gleichrangig nebeneinander, denn Fahrlässigkeit genügt. Der Vorsatz schlägt erst bei der Schadensabwägung nach § 254 BGB durch.[735] Schuldhaft muss der Schuldner nur die vertragliche oder gesetzliche Verpflichtung verletzen, nicht auch den Schaden verursachen. Neben der Haftung für eigenes Verschulden haften die Vertragsparteien gem. § 278 BGB darüber hinaus im gleichen Umfang für ein Verschulden ihres Erfüllungsgehilfen. Erfüllungsgehilfen sind die Personen, die die Vertragsparteien zur Erfüllung ihrer vertraglichen Pflicht einsetzen.[736]

a) Vorsatz

Das Gesetz enthält für den Vorsatz keine Legaldefinition, er ist aber mit allgemeiner Auffassung als Wissen (intellektuelles Element) und Wollen (voluntatives Element) der nach dem objektiven gesetzlichen Tatbeständen maßgeblichen Umständen zu verstehen.[737] Denkbar sind solche Fälle, wenn KI Technologien dazu verwendet werden, um andere

---

[731] Vgl. *Jänisch/Schrader/Reck*, NZV 2015, 313, 316; *Vogt*, NZV 2003, 153, 158. Zustimmend hinsichtlich Software und weiterfressendem Mangel: *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 21 Rn. 67; *Marly*, Praxishandbuch Softwarerecht, 6. Aufl. 2014, Rn. 1861; *Sodtalbers*, Softwarehaftung im Internet, 2006, Rn. 513, 518.

[732] Palandt/*Grüneberg*, BGB, 72. Aufl. 2013, § 276 Rn. 2.

[733] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1710.

[734] BGH, 06.05.1981 - IVa ZR 170/80 = BGHZ 80, 269; NJW 1981, 1729; MDR 1981, 735; BGH, 09.06.1982 - IVa ZR 9/81 = BGHZ 84, 244; NJW 1982, 2238; ZIP 1982, 1214; MDR 1982, 915; VersR 1982, 850; BGH, 13.12.1991 - LwZR 5/91 = BGHZ 116, 334; NJW 1992, 1036; MDR 1992, 371; ZMR 1992, 140; WM 1992, 831; BGH, 05.10.1989 - III ZR 126/88 = NJW 1990, 1230; MDR 1990, 416; VersR 1990, 207; WM 1990, 438.

[735] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1711.

[736] Insb. gesetzliche Vertreter wie Mitarbeiter, Erfüllungsgehilfen, aber auch Subunternehmer; Palandt/*Heinrichs*, 77. Aufl. 2018, § 278 Rn. 4.

[737] *Dauner-Lieb,* in: Dauner-Lieb/Langen, BGB Schuldrecht Band 2/1, 2. Aufl. 2012, § 276 Rn. 10.; *Grundmann,* in: Münchener Kommentar BGB Bd. 2: Schuldrecht Allgemeiner Teil (§§ 241 - 432), 7. Aufl. 2015, § 276 Rn. 150 bis 163.

Systeme zu schädigen wie z. B. im Hochfrequenzhandel oder wenn bewusst Verletzungen im Datenschutzrecht in Kauf genommen werden, um den eigenen Profit zu steigern. Der Schuldner handelt vorsätzlich, wenn er bewusst und gewollt die Leistung unmöglich macht, verzögert oder schlecht erfüllt.[738] Beim Vorsatz wird grundsätzlich zwischen der Absicht, dem direkten und dem bedingten Vorsatz unterschieden. Hierbei spielen für den Vorsatz als zivilrechtliche Haftungsvoraussetzung die hauptsächlich im Strafrecht erarbeiteten Unterscheidungen keine Rolle.[739] Im Zivilrecht genügt die letztgenannte, schwächste Form.[740] Im Zivilrecht gehört zum Vorsatz auch das Bewusstsein der Rechtswidrigkeit, so dass jeder Verbotsirrtum den Vorsatz ausschließt.[741] Einem Verbotsirrtum erliegt der Schuldner dann, wenn er sein vertragswidriges Verhalten irrig für vertragsgemäß hält.[742] Aber nur der unmittelbare Verbotsirrtum entlastet den Schuldner auch vom Vorwurf der Fahrlässigkeit.[743] Die Beweislast trägt der Schuldner.[744] Der Verbotsirrtum ist jedoch meistens vermeidbar und somit fahrlässig.[745] Die einschlägigen Rechtsvorschriften und Vertragsregeln muss der Schuldner kennen.[746] Nicht einmal der falsche Rat eines Rechtsanwalts entschuldigt stets.[747]

Zum Teil wird aus der angloamerikanischen Vertragspraxis heraus versucht, die Haftung für Vorsatz auch der Höhe nach zu begrenzen. Nach § 276 Abs. 3 BGB kann aber die Haftung wegen Vorsatzes dem Schuldner nicht im Voraus erlassen werden. Diese Regelung kann für Vorsatz weder abbedungen bzw. summenmäßig begrenzt werden.[748]

[738] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1711.

[739] *Dauner-Lieb,* in: Dauner-Lieb/Langen, BGB Schuldrecht Band 2/1, 2. Aufl. 2012.

[740] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 306.

[741] BGH, 12.05.1992 – VI ZR 257/91 = BGHZ 118, 201; NJW 1992, 2014; NJW-RR 1992, 1117 (Ls.); ZIP 1992, 847; MDR 1992, 751; VersR 1992, 1006; WM 1992, 1379; BB 1992, 1379; BB 1992, 379; DB 1992, 1775; Rpfleger 1992, 529; BGH, 10.07.1984 – VI ZR 222/82 = NJW 1985, 134; MDR 1985, 219; VersR 1984, 1071; WM 1984, 1433; BauR 1984, 658; ZfBR 1984, 276; ZfBR 1987, 196.

[742] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1713.

[743] *Dauner-Lieb,* in: Dauner-Lieb/Langen, BGB Schuldrecht Band 2/1, 2. Aufl. 2012, § 276 Rn. 10.

[744] Palandt/*Grüneberg*, BGB, 72. Aufl. 2013, § 276 Rn. 10.

[745] BGH, 30.05.1972 – VI ZR 6/71; 89, 303 = BGHZ 59, 30; NJW 1972, 1366; GRUR 1973, 90; VersR 1972, 938; BB 1972, 857; DB 1972, 1530; BGH, 18.04.1974 - KZR 6/73 = NJW 1974, 1903; BGH, 14.06.1994 - XI ZR 210/93 = NJW 1994, 2754; ZIP 1994, 1350; MDR 1994, 1204; VersR 1994, 1349; WM 1994, 1613; BB 1994, 1812; DB 1994, 1819; BGH, 04.07.2001 - VIII ZR 279/00 = NJW 2001, 3114; MDR 2001, 1293; WM 2001, 2012.

[746] BGH, 10.07.1984 – VI ZR 222/82 = NJW 1985, 134; MDR 1985, 219; VersR 1984, 1071; WM 1984, 1433; BauR 1984, 658; ZfBR 1984, 276; ZfBR 1987, 196; BGH, 14.06.1994 - XI ZR 210/93 = NJW 1994, 2754; ZIP 1994, 1350; MDR 1994, 1204; VersR 1994, 1349; WM 1994, 1613; BB 1994, 1812; DB 1994, 1819; BGH, 04.07.2001 - VIII ZR 279/00 = NJW 2001, 3114; MDR 2001, 1293; WM 2001, 2012.

[747] BGH, 15.05.1979 - VI ZR 230/76 = BGHZ 74, 281; NJW 1979, 1882; VersR 1979, 769.

[748] Palandt/*Heinrichs*, 77. Aufl. 2018, § 276 Rn. 35.

c) Fahrlässigkeit

Wie bereits mehrfach erwähnt, sind KI-Technologien zu vielen Dingen in der Lage, die gegen Verbotsnormen verstoßen und somit eine Haftung nach § 823 Abs. 2 BGB in Verbindung mit der entsprechenden Verbotsnorm auslösen. Denkbar sind diese Fälle vor allem, wenn die Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO verletzt werden, da KI-Technologien hierzu schnell in der Lage sind.

Gem. § 276 Abs. 2 BGB handelt derjenige fahrlässig, der die im Verkehr erforderliche Sorgfalt außer Acht lässt. Dabei bedeutet Fahrlässigkeit die „Vermeidbarkeit des rechtswidrigen Erfolgs", hier: der Leistungsstörung durch Verletzung einer schuldrechtlichen Pflicht. Grundsätzlich unterscheidet man zwischen der bewussten und der unbewussten Fahrlässigkeit. Bewusst fahrlässig handelt der Schuldner, der den rechtswidrigen Erfolg voraussieht, aus Nachlässigkeit aber hofft, den Erfolg zu vermeiden. Bei KI-Technologien ist dies wohl dann anzunehmen, wenn der Hersteller es unterlässt, bestimmte Schutzmechanismen in die KI-Technologien zu implementieren, um diese sicherer zu machen. Sieht er aus Nachlässigkeit nicht einmal die Gefahr, die von der KI-Systemausgeht, handelt er unbewusst fahrlässig.[749] Bei der Fahrlässigkeit muss man grundsätzlich zwischen den beweisbedürftigen Tatsachen, die den Vorwurf begründen, und dem Vorwurf selbst, der eine rechtliche Wertung ist, unterscheiden.[750]

Beim Grad der Fahrlässigkeit wird in Haftungsklauseln (nicht nur bei KI-Technologien) häufig differenziert zwischen grober und leichter Fahrlässigkeit. Grundsätzlich haftet der Schuldner, Hersteller der KI-Technologie, gesetzlich für beide Formen der Fahrlässigkeit; ggf. kann die schwere Form der Fahrlässigkeit zu einem größeren Mitverschulden nach § 254 BGB führen. Gesetzliche Ausnahmen, bei der eine Differenzierung zwischen grober und leichter Fahrlässigkeit eine Rolle spielt, sind:

- Der Schuldner während des Gläubigerverzugs (§ 300 Abs. 1 BGB),
- Der Schenker (§ 521 BGB)
- Der Verleiher (§ 599 BGB),
- Der Notgeschäftsführer ohne Auftrag (§ 680 BGB)
- und der Finder (§ 968 BGB).

---

[749] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1714.

[750] BGH, 11.05.1953 - IV ZR 170/52 = BGHZ 10, 14; NJW 1953, 1139, BGH, 05.10.1973 - V ZR 163/71 = NJW 1973, 2207; VersR 1974, 169.

- Nur grobe Fahrlässigkeit verhindert den gutgläubigen Erwerb von beweglichen Sachen, Wechseln und Schecks (§ 932 Abs. 2 BGB; Art. 16 Abs. 2 WG; Art. 21 ScheckG).
- Nur grobe Fahrlässigkeit des Versicherungsnehmers befreit den Versicherer (§ 61 VVG).

Noch wichtiger ist die Unterscheidung zwischen grober und leichter Fahrlässigkeit wegen § 309 Nr. 7. Für leichte Fahrlässigkeit kann die Haftung durch AGB regelmäßig abbedungen werden, für grobe Fahrlässigkeit gegenüber Nichtunternehmern nicht (inwieweit § 307 einen formularmäßigen Haftungsausschluss gegenüber Unternehmern beschränkt, ist zweifelhaft).[751] Grundlegend handelt derjenige grob fahrlässig, der die gebotene Sorgfalt ungewöhnlich schwer verletzt und sich über einfachste Bedenken hinwegsetzt, die jedem einleuchten müssen.[752] Hierbei ist neben der objektiven Komponente auch eine subjektive maßgeblich: Es muss gerade dem Täter ein besonders schwerer Vorwurf zu machen sein.[753] Aus diesem Grund kommt es hierbei auch auf das persönliche Leistungsvermögen an, das sonst bei der objektiven Fahrlässigkeit keine Rolle spielt.[754] Hier kann eine vom BSG geprägte Definition Verwendung finden: *Fahrlässigkeit ist danach eine besonders grobe und auch subjektiv schlechthin unentschuldbare Pflichtverletzung, die das gewöhnliche Maß an Fahrlässigkeit erheblich übersteigt.*[755]

In Haftungsklauseln finden sich häufig andere Haftungsrahmen für grobe und leichte Fahrlässigkeit. Liegt somit eine fahrlässige Handlung vor, welche aber nicht als grobe Fahrlässigkeit bezeichnet werden kann, haftet der Hersteller nur im Rahmen der Haftungsbegrenzung für die leichte Fahrlässigkeit. I. d. R. fallen die Haftungsklauseln für leichte Fahrlässigkeit der Höhe nach geringer aus, als für grobe Fahrlässigkeit, da der groben Fahrlässigkeit eine erhebliche Pflichtverletzung zugrunde liegt.

[751] BGH, 19.01.1984 – VII ZR 220/82 = BGHZ 89, 363; NJW 1984, 1350; ZIP 1984, 457; MDR 1984, 482; BB 1984, 746; BGH, 23.02.1984 – VII ZR 274/82 = NJW 1985, 3016; ZIP 1984, 971; MDR 1984, 1018; WM 1984, 1224; BB 1984, 939; ZfBR 1990, 134; ZfBR 1991, 20.

[752] BGH, 08.10.1991 - XI ZR 238/90 = NJW 1992, 316; ZIP 1991, 1477; MDR 1992, 369; WM 1991, 1946; DB 1991, 2478; BGH, 29.09.1992 - XI ZR 265/91 = NJW 1992, 3235; ZIP 1992, 1534; MDR 1993, 41; VersR 1993, 105; WM 1992, 1849; DB 1992, 2543.

[753] BGH, 06.05.1985 – II ZR 162/84 = VersR 1985, 730, 731.

[754] BGH, 12.01.1988 – VI ZR 158/87 = NJW 1988, 1265; NJW-RR 1988, 657 (Ls.); MDR 1988, 488; NZV 1988, 19; VersR 1988, 474; ZfBR 1989, 68.

[755] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 311.

Eine Abgrenzung zwischen Vorsatz und Fahrlässigkeit ist theoretisch leicht zu beantworten: Der Vorsatztäter will die Verwirklichung des Tatbestandes, der Fahrlässigkeitstäter will sie nicht.[756] Dies macht die Beweislage für die Praxis aber nicht gerade einfach, es sei denn der Schuldner gibt zu, vorsätzlich gehandelt zu haben.

d) Produkthaftung / Produkthaftungsrichtlinie

Grundsätzlich könnte der Hersteller von KI-Technologien nach dem Produkthaftungsgesetz (ProdHaftG)[757] haften. Bei der so verwandten Software wurde die Anwendung des Produkthaftungsgesetzes oft mit Berufung darauf abgelehnt, dass Software kein beweglicher Gegenstand und damit auch kein Produkt i. S. d. ProdHaftG sei.[758] Diese Argumentation könnte ebenfalls für Algorithmen gelten. Für Standardsoftware wird aber die Anwendbarkeit des Produkthaftungsgesetzes grundsätzlich bejaht, da diese eine bewegliche Sache i. S. d. § 90 BGB ist.[759] Dieser Standpunkt entspricht sowohl der nationalen „opinio communis"[760] als auch dem Stand der internationalen Produkthaftungsdiskussion.[761] Obwohl die Diskussion, in der Literatur und der Rechtsprechung nicht geführt worden ist, ist dennoch davon auszugehen, dass von einer reinen physikalischen Betrachtung her ein Algorithmus keine Sache ist. Dennoch spricht für die Anwendung des ProdHaftG, dass das ProdHaftG auch handwerkliche Produkte umfasst.[762] Auch zu berücksichtigen ist aber vor allem, dass das ProdHaftG nach seinem Sinn und Zweck das Problem der Haftung für den Fall eines mehrstufigen Absatzes von Massenprodukten regelt, seien sie nun maschinell oder handwerklich gefertigt.[763] Das ProdHaftG spricht in seiner Gesetzesbegründung immer wieder davon, dass „ein Produkt in Verkehr gebracht und verwendet" wird,[764] und bezieht sich immer wieder auf „Warenhersteller" und „Verbraucher".[765] Ein

[756] *Brox/Walker,* Schuldrecht AT, 36. Aufl. Rn. 315.

[757] ProdHaftG vom 15.12.1989, BGBl. I, S. 2198.

[758] Vgl. auch *Redeker*, IT-Recht, 5. Aufl. 2012, Rn. 830; *Hoeren*, IT-Recht, Stand Okt. 2018, S. 183.

[759] *Hoeren,* IT-Recht Skript, Stand Okt. 2018, S. 184.

[760] Vgl. *Bartl*, Produkthaftung nach dem neuen EG-Recht ProdHaftG, Landsberg 1989, 142; *Taschner*, Produkthaftung, 1986, 84; *Junker* Computerrecht, 3. Aufl. 2003, Rn. 478 ff.; *Hoeren*, RdV 1988, 115, 119; *Hoeren*, Softwarehaftung innerhalb der Europäischen Gemeinschaft, in: Handbuch der modernen Datenverarbeitung, Heft 146/1989, 22, 30 f.; *Junker*, WM 1988, 1217 ff., 1249 ff.

[761] So etwa *Stuurman*, Product liability for software in Europe. A discussion of the EC-directive of 25 July 1985, in: Vandenberghe (Hrsg.), Advanced Topics of Law and Information Technology, Deventer 1989, 110, 112 ff.; *Whittaker*, European Product Liability and Intellectual Products, in: LQR 105 (1989), 125, 138 ff.; *Bown*, Liability for Defective Software in the United Kingdom, in: Software Protection 1/1986, 1, 12; *Reed*, Product Liability for Software, in: Computer Law & Practice 4 (1988), 149 ff.; ähnlich für den Bereich des UCC Aubrey´s R.V. Ctr., Inc. v. Tandy Corp., 46 Wn. App. 595, 600, 731 P.2d 1124 (1987) (accepting agreement of parties that U.C.C. Article 2 applied to transaction involving defective software); mAdvent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 675–76 (3d Cir. 1991) (holding that computer software falls within definition of a 'good' under U.C.C. Article 2).

[762] So die Argumentation von *Junker*, Computerrecht, 3. Aufl. 2003 Rn. 480.; *Hoeren*, IT-Recht Stand Okt. 2018, S. 184.

[763] *Hoeren,* IT-Recht Stand Okt. 2018, S. 184.

[764] Begründung zum Gesetz über die Haftung für fehlerhafte Produkte, zit. n. PHI Sonderdruck/87, 106.

[765] Vgl. Entwurfsbegründung, PHI Sonderdruck/87, 94, 101 u. a.

„Inverkehrbringen" liegt nach der Begründung nur dann vor, wenn ein Produkt „in die Verteilungskette gegeben wurde".[766] Eine der zentralen Neuerungen ist die explizite Einordnung von Software als Produkt gemäß Art. 4 Abs. 1 Nr. 1 S. 2 ProdHaftRL.[767] Damit wird klargestellt, dass auch KI-Modelle und KI-Systeme als Software grundsätzlich unter die Produkthaftung fallen. Die damit einhergehenden Diskussionen nach geltendem Recht (s.o.) wären hiermit erledigt. Hersteller von KI-Systemen haften dann auch nach dem ProdHaftG.

Voraussetzung der Produkthaftung ist gem. § 1 Abs. 1 S. 1 ProdHaftG u. a., dass ein Fehler der schadensursächlichen Sache vorlag (sprich: im KI-System). Ein solcher Fehler könnte ggf. vorliegen, wenn der Hersteller keine geeigneten Sicherheitsmaßnahmen bei der Programmierung der KI vorgenommen hat. Der Hersteller haftet jedenfalls nicht, wenn das KI-System den schadensursächlichen Fehler noch nicht aufwies[768] und wenn der Fehler nach dem Stand der Wissenschaft und Technik zu dem Zeitpunkt, zu dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte, vgl. § 1 Abs. 2 Nr. 5 ProdHaftG. Dennoch muss der Hersteller von KI-Sicherungsmaßnahmen in ein KI-System einbauen, so dass selbst nach einem KI-Lernprozess keine Schäden auftreten können.

Die Erstellung von KI wird nach den gleichen Maßstäben bewertet wie die Herstellung anderer Hard- oder Software. Der Hersteller haftet nach der allgemeinen Produkthaftung und den dazu einschlägigen Pflichten bzw. entsprechend der Pflichtverletzungen. Die Haftung für KI-Systeme kann sich dabei aus Konstruktionsfehlern oder Fertigungsfehlern ergeben.[769] Darüber hinaus hat der Hersteller des KI-Systems eine Produktbeobachtungspflicht, alle allgemeinen oder ihm speziell zugänglichen Erkenntnisquellen auszuschöpfen.[770] Maßgeblich ist, ob dem Hersteller bereits beim Inverkehrbringen die

[766] Entwurfsbegründung, PHI Sonderdruck/87, 102 mit Verweis auf Art. 2d des Europäischen Übereinkom- mens v. 27.01.1977 über die Produkthaftung und Tötung.

[767] Seit dem 24. Januar 2024 liegt der Entwurf der Produkthaftungsrichtlinie (ProdHaftRL) beim Europäischen Rat. In seiner Sitzung am 10. Oktober 2024 hat der Rat der Europäischen Union die Produkthaftungsrichtlinie formell verabschiedet. Die Mitgliedstaaten haben ab der Veröffentlichung im Amtsblatt 24 Monate Zeit, um sie in nationales Recht (ProdHaftG) umzusetzen https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/

[768] *Sprau*, in: Palandt – Kommentar zum BGB, 77. Aufl. 2017, § 1 ProdHaftG Rn. 17.

[769] *Spindler*, CR 2015, 766.

[770] BGH, 12.11.1991 – VI ZR 7/91, BGHZ 116, S. 60,70 f. = VersR 1992, S. 96, 99; 17.10.1989 – VI ZR 258/88, NJW 1990, S. 906, 907 f.; 23.05.1952 – III ZR 168/51, NJW 1952, S. 1091; *Kullmann*, NJW 2002, 30, 32; *Kullmann,* in: *Kullmann*/*Pfister*, Produzentenhaftung, 1/2012, 1520, S. 7; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 378; *Spindler,* in: BeckOK/BGB, § 823 Rn. 607, 610.

Fehler bekannt sein mussten.[771] Bei selbstlernender KI wäre die Frage des Inverkehrbringens differenzierter zu betrachten. Im Grunde wäre dann ein Inverkehrbringen anzunehmen, wenn die KI im Netz oder auf der Straße anfängt zu lernen. Produktrisiken die nach dem Inverkehrbringen bekannt werden, führen nicht dazu, dass dem Hersteller ein Konstruktionsfehler anzulasten ist;[772] hier handelt es sich vielmehr um einen Entwicklungsfehler, so dass allein nachträgliche Pflichten im Rahmen der Produktbeobachtung greifen können.[773] Auch wenn ein KI-System ein äußerst komplexes Produkt darstellt, bei dem eine Fehlerbehebung erheblichen Aufwand bedeutet, führt dies nicht daran vorbei, dass bekannte Sicherheitsprobleme unverzüglich beseitigt werden müssen, bevor das Produkt auf den Markt gebracht wird.[774]

Ein Sonderthema im ProdHaftG ist, dass der Schadensersatzanspruch gem. § 1 Abs. 1 S. 2 ProdHaftG nur bei Gesundheitsschäden oder der Beschädigung anderer Sachen gewährt wird, sofern diese gewöhnlicherweise privat genutzt werden. Fraglich ist, wann dies bei der Nutzung eines reinen Algorithmus der Fall sein soll. Denkbar wäre dies bei einem KI gesteuerten Haushaltroboter, Implantaten (siehe Cyborg) oder einem Roboter im Pflegedienst. Weiterhin wäre dies denkbar bei dem Einsatz von selbstfahrenden Autos oder bei Drohnen. Für Schäden an gewerblich genutzten Gegenständen ist das Gesetz von vornherein nicht anwendbar. Hinzu kommt, dass das Gesetz für den Fall der Sachbeschädigung gem. § 11 ProdHaftG von einer Selbstbeteiligung in Höhe von 500 Euro ausgeht. Das Gesetz spielt nur deshalb eine (bescheidene) Rolle, da die Haftung nach dem ProdHaftG vertraglich nicht ausschließbar ist (§ 14 ProdHaftG). Dies führt dazu, dass in jeder Haftungsklausel der Verweis auf die unbeschränkte Haftung nach dem ProdHaftG aufgenommen werden muss. Im Übrigen bleibt die deliktische Haftung nach § 823 BGB neben dem ProdHaftG bestehen (§15 Abs. 2 ProdHaftG), was für Sachschäden unter 500 Euro und Schäden an gewerblich genutzten Sachen eine zentrale Bedeutung hat.[775]

Dementsprechend kann aus dem Produkthaftungsrecht prinzipiell keine Pflicht abgeleitet werden, dass KI-System und insbesondere ihre Software stets gepflegt und aktualisiert

---

[771] *Spindler,* CR 2015, 766 bis 776.
[772] *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 71, 103 ff.; vgl. *Jänisch/Schrader/Reck*, NZV 2015, 313, 317: „zum Zeitpunkt des Inverkehrbringens"; *Vogt*, NZV 2003, 153, 159.
[773] *Spindler,* CR 2015, 766.
[774] *Meier/Wehlau,* CR 1990, 95, 97; s. auch *Schneider/Günther,* CR 1997, 389 ff.; *Bartsch,* CR 2000, 721, 722 ff.
[775] *Hoeren*, IT-Recht, Stand Okt. 2018, S. 184.

werden, da es genügen würde, dass der Kunde das Produkt nicht mehr benutzt[776], um seine Integritätsinteressen zu wahren. Allerdings funktioniert dies nur, wenn keine begleitenden Pflege- oder Wartungsverträge geschlossen werden – gerade dies findet sich aber oftmals bei softwarebezogenen Produkten. Bedenkt man, dass etwa bei Autos regelmäßige Inspektionen durch den Hersteller vorgesehen werden, liegt es nahe, dass auch die entsprechende Steuerungshard- und -software einer kontinuierlichen Pflege unterzogen werden – indes handelt es sich auch hier dann um vertragsrechtliche Pflichten, nicht um deliktsrechtlich hergeleitete.[777]

Mit der neuen Produkthaftungsrichtlinie wird eine Beweislastumkehr etabliert, die in Art. 9 ProdHaftRL[778] geregelt ist. Üblicherweise muss der Kläger beweisen, dass ein Produkt fehlerhaft ist, dass er einen Schaden erlitten hat und dass dieser Schaden durch den Produktfehler verursacht wurde. Mit der neuen Richtlinie ist vorgesehen, dass das Produkt als fehlerhaft gilt, wenn der Hersteller wichtige Informationen nicht offenlegt, wenn das Produkt nicht den vorgeschriebenen Sicherheitsstandards entspricht oder wenn es offensichtlich während des normalen Gebrauchs versagt. [779] Die Produkthaftungsrichtlinie für KI-Systeme ist Teil der umfassenden EU-Strategie zur Regulierung Künstlicher Intelligenz (KI) und ergänzt die bestehenden Vorschriften der Produkthaftungsrichtlinie von 1985.[780] Der neue Vorschlag der Europäischen Kommission vom 28. September 2022 zielt darauf ab, die Haftungsregelungen an die Besonderheiten von KI anzupassen, insbesondere im Hinblick auf komplexe Kausalitätsfragen und die Besonderheiten digitaler Technologien. Hersteller haften nach Art. 7 ProdHaftRL für Fehler in der Konzeption, der Produktion oder der Bereitstellung von KI-Systemen. Betreiber können haftbar gemacht werden, wenn sie wesentliche Änderungen an der KI vornehmen (z. B. durch Software-Updates oder Anpassungen), die den ursprünglichen Zustand erheblich beeinflussen. Die Richtlinie deckt sowohl physische als auch immaterielle Schäden ab, sofern diese nach nationalem Recht als

[776] S. zur Nichtbenutzung auch *Molitoris*, NJW 2009, 1049, 1050 f.; *Klindt*, BB 2009, 792, 793; *Spindler,* in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich, erscheint demnächst, S. 50.

[777] *Spindler,* CR 2015, 766 bis 776.

[778] Zusammenfassung zur Produkthaftungsrichtlinie für KI-Systeme (Vorschlag der EU-Kommission, COM(2022) 495 final)

[779] Seit dem 24. Januar 2024 liegt der Entwurf der Produkthaftungsrichtlinie (ProdHaftRL) beim Europäischen Rat. In seiner Sitzung am 10. Oktober 2024 hat der Rat der Europäischen Union die Produkthaftungsrichtlinie formell verabschiedet. Die Mitgliedstaaten haben ab der Veröffentlichung im Amtsblatt 24 Monate Zeit, um sie in nationales Recht (ProdHaftG) umzusetzen https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/

[780] Richtlinie 85/374/EWG

ersatzfähig gelten. Sie legt ausdrücklich fest, dass Datenverluste oder Schäden durch fehlerhafte KI-Entscheidungen in den Anwendungsbereich fallen können.

Die Richtlinie baut auf dem bisherigen Fehlerbegriff der Produkthaftungsrichtlinie[781] auf, ergänzt diesen jedoch um Besonderheiten für KI. Ein Produkt gilt gem. Art 7 ProdHaftRL als fehlerhaft, wenn es nicht die Sicherheit bietet, die die breite Öffentlichkeit unter Berücksichtigung aller Umstände, insbesondere der nachfolgenden, erwarten darf:

- der Aufmachung des Produkts, einschließlich der Anweisungen für Installation,
- Verwendung und Wartung;
- der vernünftigerweise vorhersehbaren Nutzung und missbräuchlichen Nutzung
- des Produkts;
- der Auswirkungen einer etwaigen Fähigkeit, nach Einsatzbeginn weiter zu
- lernen, auf das Produkt;
- der Auswirkungen anderer Produkte auf das Produkt, bei denen nach
- vernünftigem Ermessen davon ausgegangen werden kann, dass sie zusammen
- mit dem Produkt verwendet werden;
- des Zeitpunktes, zu dem das Produkt in Verkehr gebracht oder in Betrieb
- genommen wurde, oder, wenn der Hersteller nach diesem Zeitpunkt die

Für KI-Systeme wird klargestellt, dass Sicherheitsanforderungen dynamisch zu bewerten sind, insbesondere bei Systemen mit lernfähigen Komponenten. Die Haftung ist nicht auf klassische „Produkte" beschränkt, sondern umfasst auch digitale Leistungen, die eng mit physischen Produkten verbunden sind (z. B. Cloud-basierte KI-Dienste für autonome Fahrzeuge).[782]

Die Produkthaftungsrichtlinie steht in engem Zusammenhang mit der geplanten KI-Verordnung (COM(2021) 206 final). Ein Verstoß gegen die in der KI-VO festgelegten Anforderungen kann als Indiz für einen Produktfehler dienen (Art. 4 Abs. 2 Produkthaftungsrichtlinie).

[781] Art. 6 RL 85/374/EWG
[782] https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/

e) KI als Erfüllungsgehilfe

Fraglich ist, ob die Haftung des KI-Systems nach § 280 Abs. 1 BGB dem Nutzer gem. § 278 BGB zugerechnet werden kann. Dies scheitert aber bereits daran, dass dem KI-System keine eigene Rechtspersönlichkeit zugeordnet werden kann (siehe 7.) Teilweise wird auch die analoge Anwendung von § 278 BGB in Betracht gezogen.[783] Hierbei ist zu berücksichtigen, dass der Vertreter i. S. v. § 278 BGB schuldhaft gehandelt haben muss, was faktisch mangels eigener Rechtspersönlichkeit des KI-Systems nicht möglich ist (siehe auch 4.).[784]

f) Wartungsverträge

Wird zwischen dem Hersteller und dem Betreiber ein Wartungsvertrag für die KI-Systemgeschlossen, so haftet der Hersteller neben der Produkthaftung auch aus dem Wartungsvertrag. Dabei ist auch jede Nichterfüllung vertraglicher Nebenpflichten eine Pflichtverletzung und führt zur Schadensersatzpflicht, soweit der Lieferant nicht nachweisen kann, dass er die Pflichtverletzung nicht zu vertreten hat (§ 280 Abs. 1 S. 2 BGB). Zusätzlich kann der Betreiber bei jeder nicht unerheblichen Pflichtverletzung nach erfolgloser Fristsetzung Schadensersatz statt der Leistung verlangen (§ 281 Abs. 1 BGB) oder vom Vertrag zurücktreten (§ 323 Abs. 1 BGB).[785]

Die Verantwortlichkeit bereits im Zeitpunkt der Vertragsanbahnung ist in § 311 Abs. 2 i. V. m. § 241 Abs. 2 BGB geregelt. So muss z. B. ein Hersteller eines KI-Systems bereits vor dem Vertragsschluss Rücksicht auf Rechte, Rechtsgüter und Interessen des potentiellen Kunden nehmen. Dazu zählen vor allem Aufklärungspflichten in Bezug auf das KI-System. Erfüllt der Verkäufer des KI-Systems gegenüber dem Besteller diese Pflichten schuldhaft nicht, so muss er für eintretende Schäden entsprechend haften. Wichtig ist in dem Zusammenhang zu wissen, dass der Verkäufer des KI-Systems gegenüber dem Besteller im sog. „Fachhandel" nur Aufklärungspflichten in Bezug auf die Eigenschaften hat, die er kennt oder kennen muss.[786] Auf völlig absurde oder weit entfernte Risiken muss auch ein Hersteller eines KI-Systems nicht hinweisen. Dieser Aspekt ist wichtig, da in vielen Bereichen heute noch nicht absehbar ist, welche Schadensfälle KI-Systeme verursachen können. Auch

[783] *Mayiner,* Die künstliche Person, 2017, S. 84 f.
[784] *Müller-Hengstenberg/Kirn,* NJW 2014, 307, 311.
[785] *Hoeren*, IT Rechtskript, Stand Okt. 2018, S. 181,
[786] *Hoeren*, IT Rechtskript, Stand Okt. 2018, S. 181.

ist hierbei zu berücksichtigen, dass der Ausschluss der Haftung in Formularverträgen (AGB) für leichte Fahrlässigkeit aufgrund feststehender Rechtsprechung und der Regelung in § 307 Abs. 2 Nr. 2 BGB nur insoweit möglich ist, soweit keine wesentlichen Vertragspflichten verletzt werden.[787] Grundsätzlich sind gem. § 442 Abs. 1 S. 1 BGB die Rechte des Käufers (auch eines KI-Systems) wegen eines Mangels ausgeschlossen, wenn er bei Vertragsschluss den Mangel kennt. Eine Pflicht zur Erkundigung beim Hersteller über die Eigenschaften des Kaufgegenstandes trifft einen Verkäufer nur, wenn er aufgrund konkreter Anhaltspunkte Zweifel an der Eignung der Ware für die vom Käufer beabsichtigte Verwendung hat oder haben muss.[788] Dies gilt auch, wenn gem. § 442 Abs. 1 S. 2 BGB dem Käufer ein Mangel infolge grober Fahrlässigkeit unbekannt geblieben ist. Dem Verkäufer eines KI-Systems trifft die Pflicht zur Ermittlung der Wünsche und Erwartungen des Kunden; jede Unklarheit geht zu Lasten des Lieferanten.[789] Den Verkäufer trifft auch die Pflicht zum Hinweis auf Restriktionen für die Anwendung (hier: ungeeignete Hardware des Anwenders).[790] Zudem sind Hinweise auf mögliche Kapazitätsprobleme geschuldet.[791]

Die wirtschaftlichen Folgen der Verwirklichung eines Risikos kann der Käufer im Regelfall auch nicht dadurch auf den Verkäufer abwälzen, dass er ihn um Beratung über den Kaufgegenstand bittet.[792] Grundsätzlich liegt das Verwendungsrisiko beim Käufer, es sei denn, es handelt sich um einen Fall der Mängelhaftung. Dies bedeutet in der Praxis, dass der Käufer selbst entscheiden muss, ob das von ihm erworbene KI-System für die vom Käufer geplanten Aktivitäten geeinigt ist. Etwas anderes ist anzunehmen, wenn im Pflichtenheft, Leistungsbeschreibung oder Produktbeschreibung die Verwendung des KI-Systems für die geplanten Einsatzmöglichkeiten genau beschrieben ist. Gelingt dem Käufer der Nachweis, dass ihn der Lieferant fahrlässig vor Abschluss des Vertrags nicht richtig über vertragswesentliche Umstände informiert hat, so bieten sich ihm mehrere Möglichkeiten. Er kann Rücktritt vom Vertrag erklären,[793] Anspruch auf Ersatz seiner nutzlosen Aufwendungen geltend machen oder das KI-System behalten und einen günstigeren Preis verlangen.[794]

---

[787] *Stoffels,* AGB-Recht, 5. Aufl. 2024, Rn. 982.
[788] BGH, 16.06.2004 VIII ZR 303/03, NJW 2004, 2301 = WM 2004, 1489.
[789] LG Arnsberg, DV-Rechtsprechung Bd. 2, 99.
[790] OLG Celle, 26.02.1986 – 6 U 154/84, CR 1988, 305.
[791] LG Köln, 19.02.1986 – 23 O 450/83, CR 1987, 508.
[792] *Hoeren,* IT Rechtskript, Stand Okt. 2018, S. 181.
[793] BGH, 16.01.1985 – VIII ZR 317/83, NJW 1985, 1771 = WM 1985, 463.
[794] BGH, 08.12.1989 – V ZR 259/87, NJW 1990, 1661; BGH, 17.12.1987 – 4 StR 440/87, NJW- RR 1990, 1335.

Dabei verjähren die Ansprüche aus § 280 Abs. 1 BGB in der allgemeinen Frist des § 199 BGB. Allerdings gilt eine kürzere (zweijährige) Verjährungsfrist gem. § 438 BGB analog, wenn die Schäden in unmittelbarem Zusammenhang mit Sachmängeln stehen.[795] Gem. § 249 S. 1 BGB hat der Schuldner, der zum Schadensersatz verpflichtet ist, den Zustand herzustellen, der bestehen würde, wenn der zum Ersatz verpflichtende Umstand nicht eingetreten wäre. Dabei soll der Schädiger allen Schaden ersetzen, der durch das zum Ersatz verpflichtende Ergebnis eingetreten ist (sog. *Totalreparation*).[796] Außer der Regel der Totalreparation wird in § 249 S. 1 BGB noch ein weiterer Grundsatz des Schadensrechts ausgedrückt, nämlich das Prinzip der Herstellung oder des Naturalersatzes. Hierbei soll der Schädiger den Zustand in Geld herstellen, der ohne das Schadensereignis bestünde.

g) Pflichten und technische Standards

Die Bestimmung von nicht ausdrücklich beschriebenen vertraglichen Pflichten gestaltet sich als äußerst schwierig bei KI-Technologien, insbesondere wenn es um das Zusammenwirken von komplexen technischen Systemen und Menschen geht (sog. Interface kollaborierender Roboter).[797] Die nicht vertraglich beschriebenen Pflichten werden dabei maßgeblich vom Erkenntnisstand von Wissenschaft und Technik mitbestimmt. Die Rechtsprechung nimmt in diesem Rahmen häufig Bezug auf die Kategorien der „anerkannten Regeln der Technik", den „Stand der Technik" sowie den „Stand von Wissenschaft und Technik",[798] ohne die Verwendung dieser Begriffe näher zu erläutern, was in der Praxis dazu führt, dass diese Begriffe ins Leere laufen. Für die Bestimmung der Pflichten ist das konkrete Gefährdungspotential eines Produktes ausschlaggebend.[799] Dies ist sicherlich bei KI-Technologien sehr unterschiedlich zu betrachten. So besteht durch einen Roboter sicherlich ein größeres Haftungspotenzial für Personenschäden als durch einen Algorithmus, wobei wiederum im medizinischen Umfeld andere Haftungspotenziale durch Algorithmen entstehen können. Die Untergrenze der Sorgfaltsanforderungen bilden die anerkannten

[795] BGH, 21.11.1989 - VI ZR 350/88 = NJW 1990, 908; MDR 1990, 531; VersR 1990, 204; WM 1990, 564; BB 1990, 445.

[796] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 585.

[797] *Spindler*, CR 2015, 766 bis 776.

[798] BGH, 20.04.1971 – VI ZR 232/69, NJW 1971, 1313 (anerkannte Regeln der Technik); 17.05.1972 – VIII ZR 98/71, DB 1972, 1335 (Stand der Technik); 17.03.1981 – VI ZR 191/79, BGHZ 80, 186 = NJW 1981, 1603 (Stand von Wissenschaft und Technik); ausführlich zur Abgrenzung der Begriffe BVerfG, 08.08.1978 – 2 BvL 8/77, BVerfGE 49, 89 = NJW 1979, 359, 362; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 17 ff. m. w. N.

[799] Dazu ausführlich *Finke*, Die Auswirkungen der europäischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, 2001, S. 9 ff.; *Foerste,* in: Foerste./v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 37

Regeln der Technik, d. h. die in den Kreisen der betreffenden Techniker bekannten und als richtig anerkannten Regeln, welche in der Praxis erprobt, dort verbreitet und bewährt sind.[800] In der Praxis wird dies häufig mittels eines Gutachters festgestellt, was natürlich mit einem Gutachterstreit enden kann und letztlich auf einen Vergleich herausläuft. Grundsätzlich werden die Sorgfaltsanforderungen begrenzt durch den Stand von Wissenschaft und Technik,[801] welcher das realisierbare Ergebnis neuester naturwissenschaftlicher Forschung und ingenieurwissenschaftlicher Erfahrungssätze, deren Akzeptanz durch die Mehrheit der Praktiker noch aussteht, widerspiegelt.[802] Während in der Produkthaftung der Hersteller für zum Zeitpunkt der Inverkehrgabe nicht voraussehbare Gefahren (Entwicklungsfehler) nicht haftet,[803] trifft den Betreiber dafür die Pflicht, die Sicherungsvorkehrungen stets an neue Erkenntnisse anzupassen.[804] Was insbesondere auch für KI Technologien gilt.

Für die Ausfüllung dieser unbestimmten Rechtsbegriffe und damit der Konkretisierung der Pflichten in der deliktischen Haftung für den Einsatz von Technologien, insbesondere auch im Bereich der Produkthaftung, sind technische Standards von herausragender Bedeutung. Sie sind in überbetrieblichen technischen Normen niedergelegt, wie DIN-, CEN- oder ISO-Normen, aber auch in anderen Regelwerken wie etwa in Gefahrverhütungsregeln im Rahmen des Arbeitsschutzes.[805] Darüber hinaus kann eine Konkretisierung der Pflichten aus dem ProdSG erfolgen.[806] Zudem wird in der Literatur dazu vertreten, dass die Regelwerke vonseiten der Rechtsprechung wie Rechtsnormen zugrunde gelegt würden.[807] Diese Standards begründen meist einen prima-facie-Beweis für die Einhaltung der Sicherungspflichten, auch wenn im Einzelfall bei besonderen Gefahrenlagen strengere Anforderungen

[800] *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 22; *Wilrich*, GPSG, 2004, § 2 GPSG Rn. 107; *Vieweg,* in: Schulte, Handbuch des Technikrechts, 2. Aufl. 2010, S. 353.

[801] *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 20 f.; *Spindler*, Unternehmensorganisationspflichten, 2. Aufl. 2011, S. 796; hierzu auch: *Weisser/Färber*, MMR 2015, 506, 511.

[802] BVerfG, 08.08.1978 – 2 BvL 8/77, BVerfGE 49, 89, NJW 1979, 359, 362; OLG Köln, 06.05.1991 – 12 U 130/88, NJW-RR 1991, 1077, 1079; *Marburger*, Die Regeln der Technik im Recht, 1974, S. 164 f.; *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 16.

[803] BGH, 16.06.2009 – VI ZR 107/08, BGHZ 181, 253, 265 Rn. 28 = BB 2009, 1884, 1888; *Spindler*, in: BeckOGK/BGB, § 823 Rn. 589; *Wagner*, in: MünchKomm/BGB, 6. Aufl. 2013, § 823 Rn. 654 ff.; *Foerste*, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 20, 103 ff.

[804] Für die Pflicht einer gesetzlichen Pflegekasse, Gefahren durch fehlerhafte Krankenbetten abzuwenden: BGH, 16.12.2008 – VI ZR 170/07, BGHZ 179, 157, 163 ff., Rn. 16 ff.; auf den Einzelfall abstellend: *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 27 Rn. 14 f.

[805] *Spindler*, CR 2015, 766 bis 776.

[806] *Wagner,* in: MünchKomm/BGB, 6. Aufl. 2013, § 823 Rn. 651.

[807] *Foerste,* in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 42 Fn. 120 unter Verweis auf OLG Celle, 10.10.2005 – 7 U 155/05, VersR 2007, 253.

gestellt werden können.[808] Der Hinweis auf Zertifizierungen oder TÜV-Abnahmen kann dabei in der Regel weder den Betreiber noch den Hersteller von seiner Haftung entlasten.[809] Die richtigen Standards für KI Technologien zu finden, erscheint zum einen sehr schwierig und zum anderen sind die Ansichten dazu sehr unterschiedlich. Echte Standards bei der Entwicklung von Algorithmen lassen sich nicht finden, dagegen gibt es durchaus Standards für die Entwicklung für andere KI-Systeme. So werden auf der Ebene der sog. kollaborierenden Roboter (an der Schnittstelle zum Menschen) ISO-Standards vorbereitet, die sich mit den spezifischen Sicherheitsregeln befassen.[810] Für das autonome Fahren bzw. selbststeuernde Autos sind vor allem die technischen Normen IEC 61508 und DIN ISO 26262 von Bedeutung.[811] Zwar mag man den Möglichkeiten durch technische Standards (und Schutzgesetze) Haftungsrisiken zu umreißen, skeptisch gegenüberstehen, da die Systeme komplex sind und stets Neuerungen unterliegen,[812] doch enthebt dies nicht der Notwendigkeit, Standards zu definieren, die als Benchmarks dienen können, nicht nur im Hinblick auf Pflichtenprogramme, sondern auch im Bereich der Gefährdungshaftung von KI Technologien, etwa wenn es um die Frage von Entwicklungsfehlern geht.[813]

h) Schadensarten

I. d. R. sind mit Personenschäden die in § 823 Abs. 1 S. 1 BGB genannten personenbezogenen Schadensarten Leben, Körper, die Gesundheit und die Freiheit gemeint. Die Begriffe Körper- oder Gesundheitsverletzung sind weit auszulegen. Darunter sind jegliche Beeinträchtigungen der körperlichen, geistigen oder seelischen Integrität zu verstehen.[814] Das Recht am eigenen Körper ist ein gesetzlich ausgeformter Tatbestand des allg.

[808] Ausführlich dazu *Spindler*, in: BeckOGK/BGB, § 823 Rn. 389, Rn. 584 ff.; *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2, Rn. 144 (zuletzt abgerufen am: 20.11.2015).; BGH, 14.05.1998 – VII ZR 184/97, NJW 1998, 2814, 2815; 27.09.1994 – VI ZR 150/93, NJW 1994, 3349, 3350; LG Berlin, MDR 1997, 246, 247.

[809] Eingehend *Spindler*, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären, 2007, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2, Rn. 145 ff. (zuletzt abgerufen am: 20.11.2015).; BGH, 09.01.1990 – VI ZR 103/89, CR 1990, 402 = NJW-RR 1990, 406 f.; s. auch OLG Celle, 28.05.2003 – 9 U 7/03, NJW 2003, 2544, 2545.

[810] ISO/TS 15066 „Robots and robotic devices – Safety requirements for industrial robots – Industrial collaborative workspace"; daneben ebenfalls in Vorbereitung: ISO/DIS 13482 „Robots and robotic devices – Safety requirements for non-industrial robots – Non-medical personal care robot"; bereits bestehend allgemein für Industrieroboter: ISO 10218-1 „Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots" und ISO 10218-2 „Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration".

[811] *Jänich*/*Schrader*/*Reck*, NZV 2015, 313, 316 f.; *Lutz*/*Tang*/*Lienkamp*, NZV 2013, 57, 61.

[812] So *Hanisch,* in: Hilgendorf (Hrsg.), Robotik im Kontext zwischen Recht und Moral, 2014, S. 27, 35.

[813] *Spindler*, CR 2015, 766 bis 776.

[814] *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch, 10. Aufl. 2011, C.13 deliktische Haftung Rn.15 bis 18.

Persönlichkeitsrechts,[815] welches grundsätzlich nicht durch § 253 Abs. 2 BGB geschützt wird. Dessen Verletzung kann nur in schwerwiegenden Fällen Anspruch auf Schmerzensgeld auslösen.[816] Ein solcher Anspruch lässt sich auch nicht aus § 253 Abs. 2 BGB, sondern nur aus § 823 Abs.2 BGB i. V. m. Art. 1 Abs. 1, 2 Abs. 1 GG herleiten,[817] so bei schweren Ehrverletzungen, z. B. bei unbegründeter oder gar böswilliger Bloßstellung oder Herabsetzung einer Person in der Öffentlichkeit;[818] bei wiederholter und hartnäckiger Verletzung des Rechts am eigenen Bild.[819] Die Körperverletzung ist dabei jeder unbefugte Eingriff in die körperliche Befindlichkeit.[820] Ein Eingriff ist dabei jeder körperliche, geistige oder seelische Lebensvorgang, auch wenn der Verletzte noch nicht geboren ist.[821] In diesen Fällen ist vielmehr nach § 253 Abs. 2 BGB auch für einen immateriellen Schaden, der kein Vermögensschaden ist, „eine billige Entschädigung in Geld", Schmerzensgeld genannt, zu leisten, unabhängig davon, auf welcher Rechtsgrundlage - Delikt, Gefährdungshaftung oder Vertrag – für die Verletzung der in § 253 Abs. 2 BGB genannten Rechtsgüter gehaftet wird.[822] Bei § 253 Abs. 2 BGB wird anders als bei § 823 Abs. 1 BGB das Leben hier nicht erwähnt. Deshalb ist kein Schmerzensgeld zu zahlen, falls der Tod sofort mit der Verletzung eintritt.[823] Der § 253 Abs. 2 BGB gewährt auch nicht für jede Kleinigkeit Schmerzensgeld.[824] Eine angemessene „billige" Entschädigung in Geld ist zu zahlen, d. h. bei geringfügigen gesundheitlichen Verletzungen ohne wesentliche Beeinträchtigung - Bagatellschäden - entfällt ein Schmerzensgeldanspruch, wenn ein Ausgleich in Geld unbillig erscheint.[825] Das Ausmaß der erlittenen Schmerzen kann durch das Zeugnis von Familienangehörigen

---

[815] BGH, 09.11.1993 – VI ZR 62/93 = BGHZ 124, 52; NJW 1994, 127; NJW-RR 1994, 286 (Ls.); MDR 1994, 140; FamRZ 1994, 154; VersR 1994, 55; JR 1995, 21.

[816] *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch, 10. Aufl. 2011, C.13 deliktische Haftung Rn.15 bis 18.

[817] BGH, 01.12.1999 – I ZR 49/97 = BGHZ 143, 214; NJW 2000, 2195; NJW-RR 2000, 1211 (Ls.); MDR 2000, 1147; GRUR 2000, 709; FamRZ 2000, 1080; VersR 2000, 1154; WM 2000, 1449; ZUM 2000, 582; afp 2000, 356.

[818] BVerfG, 08.03.2000 – 1 BvR 1127/96 = NJW 2000, 2187; MDR 2000, 829; FamRZ 2000, 943; VersR 2000, 897; VersR 2000, 1114; ZUM 2000, 947; BGH, 15.11.1994 – VI ZR 56/94 = BGHZ 128, 1; NJW 1995, 861; MDR 1995, 804; GRUR 1995, 224; VersR 1995, 305; WM 1995, 542; DB 1995, 1607; afp 1995, 411.

[819] BGH, 12.12.1995 – VI ZR 223/94 = NJW 1996, 985; MDR 1996, 365; GRUR 1996, 227; VersR 1996, 341; ZUM 1996, 243; afp 1996, 138.

[820] Palandt/*Thomas*, 77. Aufl. 2017, § 823 Rn. 4.

[821] BGH, 11.01.1972 – VI ZR 46/71 = BGHZ 58, 48; BGHZ 58, 487; NJW 1972, 1126; MDR 1972, 406; VersR 1972, 372; DB 1972, 433; JR 1972, 242; BGH, 30.04.1991 - VI ZR 178/90 = BGHZ 114, 284; NJW 1991, 1948; MDR 1991, 728; FamRZ 1991, 918; VersR 1991, 816.

[822] *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch, 10. Aufl. 2011, C.13 deliktische Haftung Rn.15 bis 18.

[823] Ein übertrag- und vererbbarer Schmerzensgeldanspruch setzt voraus, dass der Getötete die ihm zugefügten Verletzungen empfunden hat. Der Sterbevorgang darf wegen der Kürze der Zeit zwischen Schadensereignis und Tod nicht derart im Vordergrund stehen, dass eine immaterielle Beeinträchtigung durch die Körperverletzung als solche nicht fassbar ist und folglich die Billigkeit hierfür keinen Ausgleich in Geld gebietet, so BGH, 12.05.1998 - VI ZR 182/97 = BGHZ 138, 388; NJW 1998, 2741; ZIP 1998, 1272; MDR 1998, 1029; NZV 1998, 370; NJ 1999, 35; VersR 1998, 1034; DB 1998, 2321 (Ls.), ebenso KG, 30.10.2000 - 12 U 5120/99 = NZV 2002, 38.

[824] Siehe auch *Büchting/Heussen,* Beck'sches Rechtsanwalthandbuch, 12. Aufl. 2022, C.13 deliktische Haftung Rn.15 bis 18.

[825] BGH, 14.01.1992 – VI ZR 120/91 = NJW 1992, 1043; NJW-RR 1992, 1182 (Ls.); MDR 1992, 349; ZMR 1992, 189; VersR 1992, 504; DB 1992, 1237.

des Verletzten, von behandelnden Ärzten, Krankenunterlagen, verschriebenen Medikamenten und Schmerzmitteln bewiesen werden.[826] Die Haftung für Personenschäden kann vor allem im Zusammenhang mit KI-Implantaten bei Cyborgs eine Rolle spielen oder wenn autonom fahrende Fahrzeuge z. B. einen Passanten oder einen anderen Fahrer verletzen. Bei letzterem greifen die Haftungsgrundsätze für autonomes Fahren (siehe Kapital I.). Erzeugt ein mangelhaftes KI-Implantat einen Personenschaden, so bestehen die Wiederherstellungskosten bei der Verletzung einer Person vor allem in den Kosten der Heilbehandlung.[827] Der Personenschaden i. S. d. des Versicherungsrechts nach § 1 Ziffer 1 AHB lehnt sich an den in § 823 Abs. 1 BGB geschützten Begriffen „Leben, Körper, die Gesundheit" an. Das Recht auf Freiheit und das allgemeine Persönlichkeitsrecht werden von dem Begriff des Personenschadens nicht erfasst.[828] Eine Gesundheitsschädigung umfasst dabei eine physische und auch eine psychische Beeinträchtigung.[829] Solange keine speziellen Haftungskonzepte für Schädigungen durch KI-Systeme gesetzlich normiert sind, muss die Praxis auf die bisher geltenden Haftungsregelungen zurückgreifen. Bei einer Beteiligung von Arbeitnehmern am Schadensfall sind dabei arbeits- und sozialrechtliche Besonderheiten zu beachten. Schädigt ein autonomes System einen Arbeitnehmer an dessen Gesundheit und kann dem Arbeitgeber oder einem anderen Arbeitnehmer ein schuldhafter Verursachungsbeitrag nachgewiesen werden, finden die Haftungsprivilegierungen der §§ 104 ff. SGB VII Anwendung. Hat der Arbeitnehmer den Schaden (mit-)verursacht, gelten die Grundsätze zum innerbetrieblichen Schadensausgleich. Je nach Verschuldensgrad kann eine Haftung des Arbeitnehmers im Innenverhältnis mit dem Arbeitgeber entfallen oder nur anteilig bestehen.[830]

Es kann bei dem Einsatz von KI-Systemen, z. B. beim Autonomen Fahren zu Sachschäden kommen. Bei Sachschäden wird zwischen der Zerstörung und der Beschädigung der Sache unterschieden. Dies folgt aus § 249 S. 2 BGB, denn dort wird ein Anspruch auf Ersatz der Herstellungskosten nur für den Fall der Beschädigung gewährt.[831] Der Unterschied

[826] BGH, 01.10.1985 – VI ZR 19/84 = NJW 1986, 1541; NJW-RR 1986, 702 (Ls.); VersR 1986, 183.
[827] Palandt/*Heinrichs*, 77. Aufl. 2017, § 249 Rn. 8.
[828] *Späte,* Kommentar zu den Allgemeinen Versicherungsbedingungen für die Haftpflichtversicherung, 1993, § 1 AHB Rn. 49.
[829] *Pröless,* in: Pröless/Martin, Versicherungsvertragsgesetz, 28. Aufl. 2010, § 1 AHB Rn. 15.
[830] *Günther/Böglmüller*, BB 2017, 53 bis 58.
[831] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 617.

zwischen Zerstörung und Beschädigung beruht auf dem (nur bei Beschädigung gegebenen) Vorhandensein einer reparaturfähigen Sache. Eine reparaturfähige Sache liegt aber dann nicht vor,

- wenn der Schaden so schwer ist, dass eine Reparatur technisch unmöglich ist (technischer Totalschaden)
- wenn eine technisch mögliche Reparatur unverhältnismäßig teuer ist, dass der Schädiger sie nach § 251 Abs. 2 S. 1 ablehnt und den Geschädigten in Geld entschädigt (wirtschaftlicher Totalschaden)[832]
- wenn eine Reparatur zwar technisch möglich und auch wirtschaftlich tragbar, aber dem Geschädigten unzumutbar ist. Dies ist z. B. dann der Fall, wenn ein neuer oder fast neuer Wagen[833] so erheblich beschädigt worden ist, dass er nach der Reparatur als Unfallwagen gelten müsste (uneigentlicher Totalschaden).[834]

Soweit die Herstellung nicht möglich oder zur Entschädigung des Gläubigers nicht genügend ist, hat der Ersatzpflichtige den Gläubiger gem. § 251 Abs. 1 BGB in Geld zu entschädigen (sog. Wertinteresse). Das Wertinteresse besteht regelmäßig aus dem sog. Zeitwert. Der Zeitwert ist der Betrag, den der Geschädigte durch den Verkauf der Sache unmittelbar vor der Schädigung hätte erzielen können.[835] Ist eine Sache nur beschädigt, kann der Geschädigt nach § 249 S. 2 BGB den für die Reparatur erforderlichen Geldbetrag verlangen. Dabei kommt es nach der h. M. nicht darauf an, ob der Geschädigte den Betrag wirklich für die Reparatur verwendet[836] oder nicht.[837] Nach dem Sachversicherungsrecht stellt jede Beeinträchtigung der Substanz, die den Wert oder die Brauchbarkeit einer Sache durch physikalische oder chemische Einwirkung mindert, einen Schaden dar.[838] Gem. § 90 BGB sind Sachen alle körperlichen Gegenstände.

---

[832] Die Rspr. bejaht solche Unverhältnismäßigkeit regelmäßig, wenn die Reparaturkosten den Wiederbeschaffungswert um mindestens 30 % übersteigen. BGH, 15.10.1991 – VI ZR 314/90 = BGHZ 115, 364; NJW 1992, 302; MDR 1992, 131; NZV 1992, 66; VersR 1992, 61; BB 1992, 20; DB 1992, 209.

[833] Dies nimmt die Rspr. regelmäßig bis 1000 km Fahrleistung an, vgl. BGH, 29.03.1983 - VI ZR 157/81 = VersR 1983, 658.

[834] Palandt/*Heinrichs*, 77. Aufl. 2017, § 249 Rn. 23.

[835] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 621.

[836] BGH, 06.11.1986 – VII ZR 97/85 = BGHZ 99, 81; BGHZ 99, 82; NJW 1987, 645; NJW 1987, 3097; NJW-RR 1987, 337 (Ls.); MDR 1987, 309; WM 1987, 260; BB 1987, 365; DB 1987, 529; BauR 1987, 89; ZfBR 1993, 231; ZfBR 1992, 25; ZfBR 1990, 184; ZfBR 1987, 93; BGH, 20.06.1989 – VI ZR 334/88 = NJW 1989, 3009; NJW-RR 1990, 37 (Ls.); MDR 1990, 41; NZV 1989, 465; VersR 1989, 1056; BB 1989, 1719; BGH, 30.06.1997 - II ZR 186/96 = NJW 1997, 2879; MDR 1997, 938; MDR 1997, 948; VersR 1997, 1287; WM 1997, 1813; BB 1997, 2187; BauR 1997, 866; IBR 1997, 456.

[837] *Grunsky,* NJW 1983, 2465.

[838] *Martin*, Sachversicherungsrecht, 4. Aufl. 2022, Abschnitt B III Rn. 4.

Die Gruppe der Vermögensschäden kann für die Hersteller von KI-Systemen besonders teuer werden, bedenkt man gerade Fälle im Hochfrequenzhandel. Der Ausfall eines solchen Händlersystems für wenige Stunden, kann zu erheblichen finanziellen Ausfällen führen. Hier entsteht dem Kunden kein Sachschaden, da sich der Wert des KI-Systems nicht verschlechtert hat oder das mangelhafte KI-System nicht zu einer körperlichen Beschädigung eines anderen Wirtschaftsguts geführt hat, sondern vielmehr wird durch die Nicht-Nutzbarkeit des Hochfrequenzhandelsystems dem Kunden ein Vermögensschaden entstanden sein.

Eine Differenzierung zwischen Sachschaden und Vermögensschaden fällt nicht immer leicht. Zur Abgrenzung beider Schadenskategorien sind verschiedene Theorien entwickelt worden.[839] Große Bedeutung hat die „*Lehre vom Interesse,*"[840] welche die wesentliche Basis für die Schadensberechnung darstellt.[841] Ein Vermögenschaden ist danach die „Differenz zwischen dem Betrage des Vermögens einer Person, wie derselbe in einem gegebenen Zeitpunkte ist, und dem Betrage, welcher dieses Vermögen ohne die Dazwischenkunft eines schädigenden Ereignisses haben würde." Zu vergleichen ist die tatsächliche Vermögenssituation des Ersatzberechtigten nach dem schädigenden Ereignis mit der – hypothetischen – Situation, die bestehen würde, wenn es zur Rechtsgutsverletzung nicht gekommen wäre (sog. *Differenzschaden*).[842] Vermögensschäden spiegeln sich vor allem in der Betriebsunterbrechung, dem Verzug und dem entgangenen Gewinn wider.

Vermögensschäden sind Einbußen am Eigentum und anderen geldwerten Gütern, welche sich in Geld messen lassen und das Vermögen des Geschädigten mindern.[843] Sie sind entweder durch die Herstellung eines schadensfreien Zustandes nach § 249 BGB oder durch Wertersatz auszugleichen.[844] Durch das Schadensereignis ist ein geldwerter Arbeitsaufwand entstanden und eine verhinderte geldwerte Arbeitsleistung.[845] Anders als Körper- und

[839] *Jauernig,* Kommentar zum BGB, 7. Aufl. 2010, vor §§ 249-253 Rn. 3.
[840] BGH, 06.06.1997 – V ZR 115/96 = BGHZ 136, 52; NJW 1997, 2378; ZIP 1997, 1378; MDR 1997, 924; DNotZ 1998, 60; WM 1997, 1671; BB 1997, 1657; DB 1997, 2018.
[841] Krit. *Schermaier,* JZ 98, 857.
[842] Palandt/*Heinrichs*, 77. Aufl. 2017, vorb § 249 Rn. 8, 9.; *Jauernig,* Kommentar zum BGB, 7. Aufl. 2010, vor §§ 249-253 Rn. 5.
[843] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1269.
[844] BGH, 18.07.2008 – V ZR 71/07 = NJW 2008, 3059; MDR 2008, 1263; NZM 2008, 819; WM 2008, 1798; IMR 2008, 357.
[845] BGH, 24.11.1995 – V ZR 88/95 = BGHZ 131, 220; NJW 1996, 921; ZIP 1996, 281; MDR 1996, 1112; DNotZ 1996, 441; WM 1996, 599; BB 1996, 658; DB 1996, 1514; JR 1996, 455

Sachschäden sind reine Vermögensschäden variable Größen, die sich bis zur vollständigen Ersatzleistung oder letzten mündlichen Verhandlung im Schadensersatzprozess noch entwickeln können.[846] Da man den Vermögensschaden danach berechnet, wie sich das Vermögen des Verletzten ohne die Schadenshandlung entwickelt hätte, muss man auch Reserveursachen berücksichtigen.[847] Deshalb ist nach vorzeitiger Vertragsbeendigung durch fristlose Kündigung der Schadensersatz zeitlich begrenzt bis zum vereinbarten Vertragsende oder nächsten Kündigungstermin.[848] Der unliebsame Vertragsabschluss hingegen begründet nur dann einen Vermögensschaden, wenn er wirtschaftlich nachteilig ist.[849]

Mit den allgemeinen Vorschriften der §§ 280, 281, 283, 311a BGB steht für alle Arten von Schäden eine einheitliche Anspruchsgrundlage zur Verfügung. Der Gläubiger kann unter den Voraussetzungen des § 280 BGB »nahe« also unmittelbare oder entfernte Mangelfolgeschäden (mittelbare Schäden) ersetzt verlangen. Voraussetzung ist allein, dass eine Pflichtverletzung des Unternehmers vorliegt und dass er sie zu vertreten hat. Der Hersteller haftet somit, da er Mangelfreiheit als Teil der Erfüllungspflichten schuldet, für Mangelschäden in gleicher Weise wie für Mangelfolgeschäden.[850] Deren Verletzung macht ihn bezüglich beider Schadenstypen ersatzpflichtig.[851] Dies bedeutet, dass der Hersteller bereits dann in Schadenersatzhaftung geraten kann, wenn er fahrlässig mangelhafte Produkte liefert, wobei nunmehr auch Mängel des Produktes selbst (Mängelschäden) eine Haftung begründen (§ 281 i. V. m. § 280 Abs. 1 BGB aus Pflichtverletzung), ebenso Mangelfolgeschäden (unmittelbar aus § 280 Abs. 1 BGB), und zwar auch bei Rücktritt des Kunden.[852] Schadensersatz statt der Leistung (bisher: Schadensersatz wegen Nichterfüllung) geht auf das positive Interesse, weshalb der Kunde so zu stellen ist, wie er stünde, wenn der Vertrag ordnungsgemäß erfüllt worden wäre.[853] Haftung für Mangelschäden folgt aus den §§ 281, 283 BGB[854] und umfasst (begrifflich unverändert) etwa Reparaturkosten,[855]

---

[846] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1308.

[847] BGH, 13.05.1953 – VI ZR 5/52 = BGHZ 10, 6; NJW 1953, 977; BGH, 14.03.1985 - IX ZR 26/84 Verdienstausfall = NJW 1986, 1329; NJW-RR 1986, 650 (Ls.); ZIP 1985, 1143; MDR 1985, 577; WM 1985, 666; BGH, 09.04.1991 - XI ZR 136/90 Steuerliche Mehrbelastung = NJW 1991, 1881; NJW-RR 1991, 1398 (Ls.); ZIP 1991, 644; MDR 1991, 761; VersR 1991, 888; WM 1991, 890; BB 1991, 2181; DB 1991, 1621.

[848] BGH 82, 121; 95, 39; 104, 337; NJW 93, 1386.

[849] BGH, 26.09.1997 – V ZR 29/96 = NJW 1998, 302; ZIP 1998, 154; MDR 1998, 25; DNotZ 1998, 349; NZM 1998, 167 (Ls.); ZMR 1998, 79; VersR 1998, 905; WM 1997, 2309; BB 1997, 2553; IBR 1998, 124; BauR 1998, 196 (Ls.).

[850] Begründung zum Schuldrechtsmodernisierungsgesetz, BT-Drs. 14/6040, 224.

[851] Siehe *v. Westphalen*, DB 2001, 799, 802.

[852] *Koch,* Computer-Vertragsrecht, 6. Aufl. 2002, Rn. 1346.

[853] *Boerner*, ZIP 2001, 2264, 2272.

[854] Begründung zum Schuldrechtsmodernisierungsgesetz, BT-Drs. 14/6040, 224.

[855] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1269.

mangelfeststellungsbezogene Gutachterkosten,[856] verbleibenden Minderwert,[857] Nutzungsausfall während der Reparatur und Gewinnentgang[858] sowie Betriebsausfallschaden durch verzögerte Inbetriebnahme.[859] Die Haftung für Mangelfolgeschäden ergibt sich aus § 280 Abs. 1 BGB[860] und umfasst Schäden an anderen Rechtsgütern des Käufers. Hierzu können nunmehr etwa auch Vermögensschäden gehören, die durch einen falsch rechnenden Algorithmus der KI-Systemverursacht werden.[861] Wie bereits erläutert, können die Gewährleistungsrechte bei Verträgen unter Kaufleuten grundsätzlich eingeschränkt werden.

Häufig wird in Haftungsklauseln zwischen unmittelbaren und mittelbaren Schäden (Folgeschäden) differenziert. So vereinbaren z. B. US-amerikanische Hersteller gerne in Verträgen nach deutschem Recht regelmäßig einen generellen Ausschluss für mittelbare Schäden.[862] Da viele Anbieter von KI-Technologien US-amerikanischen Ursprungs sind, werden die sog. incidental/consequentail damages[863] (mittelbare Schäden) auch gerne in deutschen Verträgen für KI-Systeme ausgeschlossen.

Fraglich ist zunächst einmal, ob zwischen unmittelbaren und mittelbaren Schäden differenziert werden kann. Eine Differenzierung zwischen unmittelbaren und mittelbaren Schäden wird man in den zentralen Schadensvorschriften des BGB nicht finden. Der historische Gesetzgeber hat dabei bewusst von der Verwendung dieser Begriffe Abstand genommen, da sich keine allgemein anerkannte Definition herausgebildet hat.[864] Wie bereits oben erläutert, sind alle entstandenen unmittelbaren und mittelbaren Schäden adäquat zu ersetzen.[865] In der Rechtsprechung lassen sich aber Ansätze für die Differenzierung zwischen unmittelbaren und mittelbaren Schäden finden. Die Differenzierung spielte zumindest vor der Schuldrechtsreform in verschiedenen Rechtsgebieten eine Rolle (z. B. Kaufrecht, Werkvertrag inkl. VOB/B Werkvertragsrecht, Versicherungsrecht und Transportrecht). Die

[856] BGH, 05.07.1978 – VIII ZR 172/77 = NJW 1978, 2241; MDR 1979, 133; WM 1978, 1172; BB 1978, 1491; DB 1978, 1878; JR 1979, 199.
[857] Palandt/*Heinrichs*, 77. Aufl. 2017, § 276 Rn. 110.
[858] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 1269.
[859] Begründung zum Schuldrechtsmodernisierungsgesetz, BT-Drs. 14/6040, 224, 224: Anspruch bereits aus § 280 I BGB n. F., unabhängig von Verzugsvoraussetzungen des § 281 Abs. 1 BGB n. F. einschließlich Anspruch auf Ersatz von Rechtsverfolgungskosten.
[860] Begründung zum Schuldrechtsmodernisierungsgesetz, BT-Drs. 14/6040, 224, 224.
[861] *Koch,* Computer-Vertragsrecht, 7. Aufl. 2009, Rn. 1347.
[862] *Funk/Wenn*, CR 2004, 481.
[863] Zur Wirksamkeit derartiger Haftungsausschlüsse nach Maßgabe des Uniform Commercial Codes s. z. B. M. A: Mortenson v. Timberline Software Corporation, Supreme Court of Washington (140 Wash. 2.d. 568, 998 P.2d 305).
[864] *Oetker,* in: MüKo/BGB, 4. Aufl., §249 Rn. 97.
[865] Siehe auch *Schiemann,* in: Staudinger, BGB 13. Bearb., Vorbemerkung zu §§ 249 ff; *Oetker*, in: MüKo/BGB, 4. Aufl., § 249 Rn. 94.

höchstrichterliche Rechtsprechung hat die Begriffe des unmittelbaren und des mittelbaren Schadens in der Vergangenheit sehr unterschiedlich verstanden.[866] In einer Vielzahl von Entscheidungen wird danach differenziert, ob der Schaden „unmittelbar" am Vertragsgegenstand oder an anderen Rechtsgütern des Geschädigten eingetreten ist.[867] Nach der Rechtsprechung kommt es i. d. R. dabei nicht darauf an, ob das schädigende Ereignis den am Vertragsgegenstand eingetretenen Schaden unmittelbar und nur mittelbar verursacht hat. Nach der Rechtsprechung ist ein unmittelbarer Schaden ausschließlich derjenige, der – im Fall der vertraglichen Haftung – dem Vertragsgegenstand selbst anhaftet oder – im Fall der deliktischen Haftung – an einem geschützten Rechtsgut eintritt.[868] Einbußen am sonstigen Vermögen werden als mittelbare Schäden verstanden.[869]

Die Unterscheidung zwischen unmittelbaren und mittelbaren Schäden findet sich insoweit in der Differenzierung zwischen Mangelschäden und Mangelfolgeschäden[870] wieder, wobei im Werkvertragsrecht zudem noch innerhalb der Mangelfolgeschäden zwischen unmittelbaren und entfernteren Mangelfolgeschäden unterschieden wurde. Die Rechtsprechung zählte zu den Mangelschäden alle Schäden, die dem Vertragsgegenstand „unmittelbar" anhaften, weil er infolge des Mangels unbrauchbar, wertlos oder minderwertig ist.[871] Darüber hinaus wurden auch die Kosten für die Mangelfeststellung[872] sowie der entgangene Gewinn dem Mangelschaden zugerechnet,[873] auch der entgangene Gewinn wird von der Rechtsprechung und Literatur ansonsten regelmäßig als bloß „mittelbarer Schaden" eingestuft. Unter unmittelbaren Mangelfolgeschäden verstand die Rechtsprechung alle Schäden, die mit dem Mangel zeitlich und räumlich „eng und unmittelbar" zusammenhängen und nicht zur Gruppe der Mangelschäden gehören.[874]

---

866 *Funk/Wenn*, CR 2004, 484.

867 Vgl. BGH, 30.09.1957 – III ZR 76/56, BGHZ 25, 340 ff.; 08.12.1981 – VI ZR 153/80, MDR 1982, 398 = NJW 1982, 827, 829 f.; OLG Düsseldorf, 18.02.2002 – 1 U 91/01, Schaden-Praxis 2002, 245 ff.

868 Zur Begründung dieses Begriffverständnisses verweist die Rechtsprechung insbesondere auf eine (angeblich) entsprechende Verwendung dieser Begriffe in der allgemeinen Rechtssprache; siehe *Funk/Wenn*, CR 2004, 484.

869 Vgl. die Definition des mittelbaren Schadens im Münchener Rechts-Lexikon, München 1997, Stichwort „Mittelbaren Schaden"; BGH, 11.12.2002 – IV ZR 226/01, MDR 2003,389 = BGH Report 2003, 319 = NJW 2003, 826, 828; *Oetker,* in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 2: Schuldrecht Allgemeiner Teil, 7. Auflage 2015, § 249 Rn. 96.

870 *Funk/Wenn,* CR 2004, 484.

871 *Peters,* in: Staudinger, BGB 13. Bearb. § 635 (a. F.) Rn. 55.

872 BGH, 18.02.2002 - II ZR 355/00 = NJW 2002, 2553; ZIP 2002, 895; ZIP 2002, 859; MDR 2002, 820; WM 2002, 909; DB 2002, 999; *Soergel*, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 5/1: Schuldrecht Besonderer Teil III/1, 7. Auflage 2017, § 635 (a. F.) Rn. 33.

873 *Honsell,* in: Staudinger, BGB 13. Bearb. § 463 (a. F.) Rn. 48 ff; *Soergel,* in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 5/1: Schuldrecht Besonderer Teil III/1, 7. Auflage 2017, § 635 (a. F.) Rn. 39 m. w. N.

874 *Peters,* in: Staudinger, BGB 13. Bearb. § 635 (a. F.) Rn. 55.

Nach der Auffassung des BGH aus seiner Entscheidung aus dem Jahre 1994 sind unter dem Begriff des unmittelbaren Schadens alle Schäden zu verstehen, die „bei dem gewöhnlichen Verlauf der Dinge als naheliegend zu erwarten sind.“[875] Dieses Verständnis des Begriffs des unmittelbaren Schadens folgt für den BGH aus dem Grundsatz der „nach beiden Seiten interessengerechten Auslegung“[876] und soll seine Rechtfertigung in der berechtigten Erwartung des Vertragspartners finden, dass die vertragswesentlichen Pflichten der Vertragspartner nicht durch die Haftungsregelung faktisch ausgehöhlt würden. Als demgegenüber nachrangig wertet der BGH das Interesse des Vertragspartners, das für ihn kaum kalkulierbare Schadenspotenzial zu begrenzen.[877] Die mögliche und gegebenenfalls nicht sicher bestimmbare Höhe eines Schadens, so der BGH, sei kein maßgebliches Kriterium dafür, ob es sich um einen unmittelbaren oder einen mittelbaren Schaden handelt.[878]

Grundsätzlich hat der Schuldner gem. § 276 Abs. 1 S. 1 Vorsatz und Fahrlässigkeit zu vertreten. Wie bereits besprochen, kann in Einzelfällen auch eine verschuldensunabhängige Haftung dazu kommen, wenn diese sich aus dem Gesetz ergibt oder besonders vertraglich vereinbart (Garantievertrag) wird.[879] Ist der Schuldner für keine solche verschuldensunabhängige Haftung verantwortlich, haftet er nicht, sofern er nicht Vorsatz oder Fahrlässigkeit zu vertreten hat, vgl. § 276 BGB.[880] Dies dürfte in Fällen der höheren Gewalt regelmäßig nicht der Fall sein. Zur Gruppe der höheren Gewalt zählen i. d. R. „*Krieg, Naturkatastrophen, Terroranschläge, Demonstrationen und Streik*.“ Wobei die Gruppe der Streiks immer im Einzelfall betrachtet werden muss, ob hier nicht vorsätzlich oder fahrlässig ein Streik provoziert worden ist. Z. T. finden sich in einigen Verträgen immer wieder Haftungsregelungen, die ausdrücklich die Haftung für höhere Gewalt ausschließen. Dies begründet sich häufig aus der angloamerikanischen Vertragspraxis, da hier die Haftung ggf. für die höhere Gewalt explizit ausgeschlossen werden muss, ansonsten der Schuldner für die höhere Gewalt

[875] BGH, 08.06.1994 – VIII ZR 103/93 = NJW 1994, 2228; MDR 1994, 888; VersR 1994, 1360; WM 1994, 1720; DB 1994, 2073; BauR 1994, 639; ZfBR 1994, 215; IBR 1995, 39.

[876] BGH, 02.07.1992 - I ZR 181/90 = NJW-RR 1992, 1386; MDR 1993, 225; VersR 1992, 1395; WM 1992, 2026; BB 1992, 1956; DB 1992, 2495; BGH, 09.06.1993 – VIII ZR 205/92 = CR 1994, 347; NJW-RR 1993, 1203; *Mayer-Maly,* in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 1: Allgemeiner Teil §§ 1-240, ProstG, AGG, 7. Auflage 2015, § 157 Rn. 6. ff.

[877] *Funk/Wenn*, CR 2004, 485.

[878] BGH, 08.06.1994 – VIII ZR 103/93 = NJW 1994, 2228; MDR 1994, 888; VersR 1994, 1360; WM 1994, 1720; DB 1994, 2073; BauR 1994, 639; ZfBR 1994, 215; IBR 1995, 39.

[879] *Auer-Reinsdorff,* ITRB 2006, 181.

[880] Palandt/*Grüneberg*, BGB, 72. Aufl. 2013, § 276 Rn. 2.

haftet. Die Beweislast für eine höhere Gewalt als Schadensursache trägt, analog zum Halter eines Kfz, der Betreiber.[881]

Die Haftung für entgangenen Gewinn ist bei KI-Technologien wie beim algorithmischen Handel von besonderer Bedeutung, da hier besonders hohe Haftungsfälle entstehen können. Die Haftung für entgangenen Gewinn ist explizit im § 252 BGB geregelt. Dabei umfasst gem. § 252 S. 1 BGB der zu ersetzende Schaden auch den entgangenen Gewinn, z. B. die Marge beim Hochfrequenzhandel. Hierbei gilt nach § 252 S. 2 BGB der Gewinn als entgangen, welcher nach dem gewöhnlichen Lauf der Dinge oder nach den besonderen Umständen, insbesondere nach den getroffenen Anstalten und Vorkehrungen, mit Wahrscheinlichkeit erwartet werden konnte. Hierbei berechnet abstrakt und ohne Rücksicht auf den Einzelfall § 288 BGB und § 376 Abs. 2 HGB den entgangenen Gewinn als Mindestschaden.[882] Darüber hinaus darf nur der Kaufmann seinen Gewinnausfall abstrakt berechnen und nur für die Geschäfte seines Handelsgewerbes.[883] In diesem Fall meint abstrakt: Der Kaufmann berechnet einfach seine übliche Gewinnspanne. Im Handelsverkehr, eCommerce, bei denen Algorithmen verwendet werden, nimmt man an, dass der Käufer die Ware mit Gewinn weiterverkauft,[884] der Verkäufer die Ware auch anderweitig mit Gewinn abgesetzt hätte.[885] Weder muss der Geschädigte beweisen, dass er einen Abnehmer hatte,[886] noch darf der Schädiger einwenden, der Schaden sei durch ein Deckungsgeschäft aufgefangen.[887] Die geschädigte Bank darf ihren Gewinnausfall abstrakt nach den Bruttosollzinsen berechnen, die sie aus ihren Aktivgeschäften üblicherweise erzielt.[888]

---

[881] BGH, 11.07.1972 – VI ZR 86/71 = NJW 1972, 1808; MDR 1972, 1023; VersR 1972, 1074.

[882] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 11. Aufl. 2021, Rn. 1280.

[883] BGH, 22.02.1989 – VIII ZR 45/88 = BGHZ 107, 67; NJW 1989, 1669; NJW-RR 1989, 1073 (Ls.); ZIP 1989, 450; MDR 1989, 628; WM 1989, 645; BB 1989, 798; DB 1989, 973; BGH, 08.10.1991 - XI ZR 259/90 = BGHZ 115, 268; NJW 1992, 109; ZIP 1991, 1479; MDR 1992, 151; WM 1991, 1983; BB 1991, 2396; DB 1992, 473; BGH, 29.06.1994 – VIII ZR 317/93 = BGHZ 126, 305; NJW 1994, 2478; ZIP 1994, 1362; MDR 1994, 1085; WM 1994, 1632; BB 1994, 2029; DB 1994, 2184; BGH, 02.12.1994 – V ZR 193/93 nicht Grundstücksgeschäft = NJW 1995, 587; NJW-RR 1995, 848 (Ls.); ZIP 1995, 220; MDR 1995, 462; DNotZ 1995, 393; WM 1995, 339; WM 1995, 123; BB 1995, 588; DB 1995, 521; ZfBR 1995, 81; IBR 1995, 183; BGH, 03.05.1995 - XI ZR 195/94 = NJW 1995, 1954; ZIP 1995, 909; MDR 1995, 705; WM 1995, 1055; BB 1995, 1508; DB 1995, 1509.

[884] BGH, 29.06.1994 – VIII ZR 317/93 = BGHZ 126, 305; NJW 1994, 2478; ZIP 1994, 1362; MDR 1994, 1085; WM 1994, 1632; BB 1994, 2029; DB 1994, 2184; BGH, 22.12.1999 - VIII ZR 135/99 = NJW 2000, 1409; ZIP 2000, 892; MDR 2000, 511; WM 2000, 537; BB 2000, 1110; DB 2000, 1505.

[885] BGH, 02.03.1988 – VIII ZR 380/86 = NJW 1988, 2234; NJW-RR 1988, 1182 (Ls.); ZIP 1988, 505; MDR 1988, 668; WM 1988, 781; BB 1988, 929; DB 1988, 1060M; BGH, 29.06.1994 – VIII ZR 317/93 = BGHZ 126, 305; NJW 1994, 2478; ZIP 1994, 1362; MDR 1994, 1085; WM 1994, 1632; BB 1994, 2029; DB 1994, 2184; BGH, 22.12.1999 – VIII ZR 135/99 = NJW 2000, 1409; ZIP 2000, 892; MDR 2000, 511; WM 2000, 537; BB 2000, 1110; DB 2000, 1505.

[886] BGH, 02.03.1988 – VIII ZR 380/86 = NJW 1988, 2234; NJW-RR 1988, 1182 (Ls.); ZIP 1988, 505; MDR 1988, 668; WM 1988, 781; BB 1988, 929; DB 1988, 1060M.

[887] OLG Stuttgart, VersR 68, 1074.

[888] Vgl. *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 11. Aufl. 2021, Rn. 1642.

I. d. R. stellt die Haftung für entgangenen Gewinn ein erhebliches Risiko für den Hersteller dar, welches weder durch ein Risiko-Management noch durch einen entsprechenden Versicherungsschutz abzusichern ist. Inwieweit ein Vorstand eines Herstellers von KI-Technologien überhaupt eine Haftungsregelung für entgangenen Gewinn unterschreiben darf, ist sehr bedenklich, da darin ggf. ein Verstoß gegen § 93 AktG zu sehen ist.

i) Haftungsbegrenzung

Vertragliche Haftungsbeschränkungen (Freizeichnungen) sind in der deutschen Industrie üblich, grundsätzlich zulässig und zwar auch für Ansprüche aus unerlaubter Handlung.[889] Dabei enthalten vor allem US-amerikanisch geprägte Verträge einen umfangreichen Katalog von Haftungsfreistellungen.[890] Durch die vor Schadenseintritt getroffene Vereinbarung wird das Entstehen der Schadensersatzforderung von Beginn des Schuldverhältnisses an gehindert oder der Anspruch in der Entstehung begrenzt.[891] Die Haftungsbegrenzung bzw. Freizeichnung unterliegt erheblichen gesetzlichen Schranken, insbesondere im Rahmen der allgemeinen Geschäftsbedingungen nach §§ 305 ff. BGB.[892] Bei der Betrachtung von Haftungsbeschränkungen (Freizeichnungen) ist grundsätzlich zwischen Individualverträgen und Formularverträgen (AGB) zu differenzieren.

Dass eine schuldrechtliche Norm gegenüber Individualvereinbarungen zwingend ist, stellt eine Ausnahme dar und bedarf daher besonderer Gründe. Hierfür bestehen nur zwei Möglichkeiten.[893]

- Das Gesetz kann den zwingenden Charakter ausdrücklich bestimmen.[894] Das BGB tut das im Schuldrecht teils bei einzelnen Normen (z. B. in §§ 248 Abs. 1, 276 Abs. 3, 536 Abs. 4, 574 Abs. 4), teils auch für ganze Gruppen von Normen (z. B. in §§ 312 f., 475, 506, 651m BGB).

[889] BGH, 27.04.1953 – III ZR 200/51 = BGHZ 9, 295; NJW 1953, 979; Palandt/*Heinrichs*, 72. Aufl. 2013, § 276 Rn 35.
[890] *Fritzemeyer,* in: Lehmann/Meents, Handbuch des Fachanwalts Informationstechnologie, 2. Aufl. 2011, Kapitel 2 Rn. 70.
[891] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 11. Aufl. 2021, Rn. 1642.
[892] *Jauernig,* Kommentar zum BGB, 7. Aufl. 2010, § 276 Rn 4.
[893] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 306.
[894] Zwingend sind insbesondere die (noch immer nicht seltenen) Vorschriften außerhalb des BGB, welche die Preise von Waren oder Dienstleistungen binden: meist als Höchstpreise, mitunter aber auch als Mindest- oder Festpreise. Die Übersicht bei *Liebing*, BB 1983, 667, für die Versicherungswirtschaft korrigierend *Sieg,* BB 983,1187.

- Ergibt sich aus dem Gesetz nicht ausdrücklich ein zwingender Charakter, so kann es durchaus sein, dass sich ein solcher aus dem Normzweck ergibt. Hierbei kann der Abdingbarkeit einer Norm insbesondere ihr Schutzzweck entgegenstehen (vgl. §§ 311b Abs. 1, 518, 766 BGB). Wegen eines Schutzzwecks können Schuldrechtsnormen auch aus anderen Gründen zwingend sein. Das gilt etwa für § 275 Abs. 1 BGB, der „den Erfüllungsanspruch auf eine unmögliche Leistung ausschließt."[895]

Gem. § 276 Abs. 1 BGB haften der Hersteller wie der Kunde einander für Vorsatz und Fahrlässigkeit unbegrenzt. Die Haftung für Vorsatz kann gem. § 276 Abs. 3 BGB nicht vertraglich ausgeschlossen werden (zwingendes Recht)![896] Der Umkehrschluss aus § 276 Abs. 3 BGB lässt zu, dass die Haftung für Fahrlässigkeit grundsätzlich beschränkt werden kann. Dies gilt nach Maßgabe des § 309 Nr. 7 BGB nicht für Allgemeine Geschäftsbedingungen i. S. v. § 305 Abs. 1 BGB. Da nach § 305b BGB die Individualabrede grundsätzlich Vorrang vor den Allgemeinen Geschäftsbedingungen hat, greift zunächst immer erst eine individuell vereinbarte Haftungsbegrenzung für Fahrlässigkeit.

Bei der Formulierung sind verschiedene Vorgehensweisen möglich. Zu einem kann die Haftung grundsätzlich für die Schadenskategorien (**Personen-, Sach- und Vermögensschäden**) begrenzt werden. Zu anderen kann die Haftung auch für Verschuldensart (leicht oder grobe Fahrlässigkeit; Vorsatz ist nicht möglich) begrenzt werden. Hierbei sind in Haftungsklausel z. T. absolute Beträge zu finden, aber auch Prozentsätze, die sich auf den Auftragswert beziehen. Wobei die Haftung für Personenschäden nach §§ 104 ff. SGB VII gesetzlich ausgeschlossen ist, wenn für einen Personenschaden eine Unfallversicherung besteht. Beim Regress gegen den Schadensverursacher (vgl. § 110 SGB VII) trägt der Sozialversicherungsträger die Beweislast für die Höhe des fiktiven zivilrechtlichen Erstattungsanspruchs.[897]

Bei den **Vermögensschäden** können auch bestimmte Bereiche der Vermögensschäden (z. B. Betriebsunterbrechung und entgangener Gewinn) ausgeschlossen werden.[898] Die ausgeschlossen Bereiche der Vermögensschäden sollten auch explizit in der Klausel

[895] Ein auf Erfüllung lautendes Urteil brächte hier eine sinnlose Inanspruchnahme der staatlichen Vollstreckungsorgane; der Gläubiger soll stattdessen auf den vollstreckbaren Schadensersatzanspruch in Geld übergehen; *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 89, 363 f.

[896] Palandt/*Heinrichs*, 67. Aufl. 2008, § 276 Rn. 35.

[897] BGH, 29.01.2008 – VI ZR 70/07 = BGHZ 175, 152; BGHZ 175, 153; NJW 2008, 2033; MDR 2008, 564; NZBau 2008, 441; NZV 2008, 397; VersR 2008, 659; BauR 2008, 1313; ZfBR 2008, 1313.

[898] BGH, 18.07.2008 – V ZR 71/07 = NJW 2008, 3059; MDR 2008, 1263; NZM 2008, 819; WM 2008, 1798; IMR 2008, 357.

ausgenommen werden. Häufig wird ferner in Haftungsklauseln zwischen unmittelbare und mittelbare Schäden (Folgeschäden) differenziert. So vereinbaren z. B. US-amerikanische KI-Hersteller gerne in Verträgen nach deutschem Recht regelmäßig einen generellen Ausschluss für mittelbare Schäden.[899] Da viele KI Hersteller US-amerikanischen Ursprungs sind, werden die sog. incidental/consequentail damages[900] (mittelbare Schäden) auch gerne in deutschen Verträgen für KI-Systeme ausgeschlossen. Siehe hier vor allem die Beispiele im Hochfrequenzhandel.

Die Haftungsbegrenzung für gesetzliche Ansprüche steht dabei immer unter dem Vorbehalt des § 14 Produkthaftungsgesetz, der einen Haftungsausschluss für Ansprüche aus dem Produkthaftungsgesetz ausschließt. Für eine Haftung nach dem Produkthaftungsgesetz ist allerdings ein Verschulden des Haftenden ohnehin nicht erforderlich, da es sich um einen reinen Gefährdungshaftungstatbestand handelt.[901]

Eine Begrenzung der Haftungssumme von **Personenschäden** (Verletzung des Lebens, des Körpers oder der Gesundheit) selbst für leichte Fahrlässigkeit ist nicht möglich.[902] Im Bereich der verschuldensabhängigen Haftung ist ausschließlich die Sittenwidrigkeitsprüfung gem. § 138 Abs. 1 BGB Maßstab für die Zulässigkeit von Haftungsbegrenzungen für fahrlässige Handlungsweisen.[903] Eine Sittenwidrigkeit könnte sich z. B. unter dem Gesichtspunkt der eklatanten Risikoverschiebung zu Lasten des Kunden ergeben, die im Ergebnis zu einer nicht tolerierbaren Äquivalenzstörung von Leistung und Gegenleistung führen würde.[904] Nach diesem Maßstab kann eine Sittenwidrigkeit jedoch mindestens dann ausgeschlossen werden, wenn die Haftung nicht vollständig ausgeschlossen, sondern nur beschränkt wird.[905] Die Höhe der Haftungsbeschränkung ist dabei an den möglichen Schäden zu orientieren, mit deren Eintritt die Vertragsparteien bei verständiger Würdigung zum Zeitpunkt des Vertragsabschlusses rechnen können. Ein Anhaltspunkt hierfür kann immer

899 *Funk/Wenn*, CR 2004, 481.
900 Zur Wirksamkeit derartiger Haftungsausschlüsse nach Maßgabe des Uniform Commercial Codes. z. B. M. A: Mortenson v. Timberline Software Corporation, Supreme Court of Washington (140 Wash. 2.d. 568, 998 P.2d 305).
901 *Redeker,* Handbuch der IT Verträge, 1.5 Rn. 27
902 *Amann/Brambring/Hertel,* Die Schuldrechtsreform in der Vertragspraxis, 2002, S. 64 bb) Kein Haftungsausschluss für Körperschäden.
903 BGH, 29.01.1975 – VIII ZR 101/73 = BGHZ 63, 382; NJW 1975, 642; MDR 1975, 750; WM 1975, 309; JR 1975, 239; BGH, 25.05.1983 - VIII ZR 55/82 = BGHZ 87, 302; NJW 1983, 2192; ZIP 1983, 948; MDR 1983, 838; WM 1983, 755.
904 Palandt/*Heinrichs*, 72. Aufl. 2013, § 138 Rn. 88 f.
905 *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 306.

das Vertragsvolumen sein, da wesentliche Schadenersatzansprüche[906] auf das positive Interesse, d. h. das Erfüllungsinteresse des Kunden, gerichtet sind.[907] Dieses wird in der Regel mit dem Vertragswert anzunehmen sein. Ein weiterer Baustein für die Umgehung der Sittenwidrigkeit ist die Vereinbarung, dass bei versicherten Risiken über die summenmäßige Haftungsbeschränkung hinaus auf die Versicherungsleistungen gehaftet wird. Damit werden beide Parteien in den Schutzbereich der Versicherungen der jeweils anderen Vertragsseite einbezogen.[908]

Der Kunde und der Hersteller können nach § 444 BGB die Sachmängelhaftung in einem Individualvertrag beliebig beschränken oder auch völlig ausschließen.[909] Unabdingbar ist nur die Haftung des Verkäufers für Arglist oder dort wo eine Garantie ausdrücklich übernommen wird. Der klar formulierte vollständige Haftungsausschluss erfasst alle, auch die schwersten und verborgensten Sachmängel.[910] Der Verkäufer kann auch eine bestimmte Eigenschaft garantieren und im Übrigen die Haftung ausschließen.[911] Vergleichbares gilt gem. § 639 S. 1 BGB auch für das Werkrecht. Um das Risiko aus der Sicht des Herstellers sinnvoll zu begrenzen, sollte die Haftung für Sachmängelansprüche ggf. begrenzt werden. Da der Hersteller verschuldensunabhängig für Sachmängel haftet, braucht hierbei auch nicht auf die Verschuldensart (leichte/grobe Fahrlässigkeit oder Vorsatz) abgestellt werden.

Grundsätzlich ist es möglich, die Haftung für den Verzug zu beschränken.[912] Dies kann vor allem auch als ein pauschalierter Schadenersatz erfolgen.[913] Die Haftungsgrenzen für einen pauschalierten Schadenersatz in Individualverträgen gelten im Rahmen der oben beschriebenen Haftungsbegrenzung und sind natürlich nicht so eng wie die Haftungsgrenzen in AGB, da auch für den pauschalierten Schadenersatz ausschließlich die Sittenwidrigkeitsprüfung gem. § 138 Abs. 1 BGB Maßstab für die Zulässigkeit von Haftungsbegrenzungen für fahrlässige Handlungsweisen ist.[914] Wobei dem Schuldner auch in Individualverträgen

---

[906] Zum Beispiel bei Verzug oder Nichterfüllung.
[907] Palandt/*Heinrichs*, 72. Aufl. 2013, § 276 Rn 34.
[908] *Brox/Walker,* Schuldrecht AT, 36. Aufl. 2012, Rn. 306.
[909] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011, Rn. 102.
[910] BGH, 11.06.1979 – VIII ZR 224/78 = BGHZ 74, 383; NJW 1979, 1886; MDR 1979, 1017; JR 1980, 22; BGH, 14.10.1966 – V ZR 188/63 = NJW 1967, 32; WM 1966, 1185; WM 1966, 1183; BGH, 23.04.1986 – VIII ZR 125/85 = NJW 1986, 2319; MDR 1986, 1017; WM 1986, 867.
[911] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen, 11. Aufl. 2021, Rn. 1642.
[912] Palandt/*Heinrichs*, 72. Aufl. 2013, § 276 Rn 34.
[913] BGH, 16.09.1970 – VIII ZR 239/68 = NJW 1970, 2017.
[914] BGH, 29.01.1975 – VIII ZR 101/73 = BGHZ 63, 382; NJW 1975, 642; MDR 1975, 750; WM 1975, 309; JR 1975, 239; BGH, 25.05.1983 – VIII ZR 55/82 = BGHZ 87, 302; NJW 1983, 2192; ZIP 1983, 948; MDR 1983, 838; WM 1983, 755.

die Möglichkeit zugestanden wird, durch einen Nachweis darzulegen, dass der Schaden geringer war als die Pauschale.[915]

Die Möglichkeiten der Haftungsbegrenzung bei Formularverträgen ist nach deutschem Recht sehr eingeschränkt. Zunächst einmal kann unterstellt werden, dass jeder vorformulierte Vertrag der Anwendung der §§ 305 ff. BGB unterstellt werden kann. Denn nach § 305 Abs. 1 S. 2 BGB liegen Allgemeine Geschäftsbedingungen nicht vor, soweit die Vertragsbedingungen zwischen den Vertragsparteien im Einzelnen ausgehandelt sind. Ein individuelles Aushandeln im Sinne von § 305 Abs. 1 S. 2 BGB liegt auch vor, wenn der Kunde zumindest die tatsächliche (nicht notwendig ausgeschöpfte) Möglichkeit hatte, auf die zur Disposition gestellten Vertragsbedingungen inhaltlich Einfluss zu nehmen.[916]

Die Möglichkeit der Begrenzung der **Haftung** (Freizeichnung) in AGB ist nur im geringen Umfang möglich. Der Ausschluss der Haftung bei grober Fahrlässigkeit kann nach § 309 Nr. 7 BGB in Allgemeinen Geschäftsbedingungen nicht wirksam vereinbart werden. Dies gilt (auch wenn sich dies nicht aus dem Gesetzeswortlaut ergibt) auch im Geschäftsverkehr zwischen Unternehmen, da § 309 Nr. 7 BGB nach der Rechtsprechung des BGH (damals § 11 Nr. 7 AGBG) auch auf den Geschäftsverkehr ausstrahlt.[917] Der Ausschluss der Haftung für leichte Fahrlässigkeit aufgrund feststehender Rechtsprechung und der Regelung in § 307 Abs. 2 Nr. 2 BGB ist nur insoweit möglich, soweit keine wesentlichen Vertragspflichten verletzt werden.[918] Ferner kann sich der Verwender von der Haftung für nur leicht fahrlässiges Handeln seiner Organe, leitenden Angestellten oder sonstiger Erfüllungsgehilfen nicht freizeichnen, und wenn es um die Verletzung von Kardinalpflichten geht.[919] Die Haftung kann i. d. R. dort begrenzt werden, wo das Interesse des Verwenders, das Risiko überraschender oder ungewöhnlicher Schadensfälle übernehmen zu müssen, nicht besteht. Eine Haftungsbegrenzung kann im unternehmerischen Verkehr (ausgenommen grobes Verschulden des Verwenders oder eines leitenden Angestellten) zulässig sein, wenn die festgelegte Haftungshöchstsumme die vertragstypischen und vorhersehbaren Schäden

[915] Palandt/*Heinrichs*, 72. Aufl. 2013, § 276 Rn 26.
[916] *Wolf/Horn/Lindacher*, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 4. Aufl. 1999, § 1 Rn. 35.
[917] Palandt/*Heinrichs*, 77. Aufl. 2017, § 309 BGB Rn. 48; *Stoffels*, AGB-Recht, 5. Aufl. 2024, Rn. 979 ff.;
[918] *Stoffels,* AGB-Recht, 5. Aufl. 2024, Rn. 982.
[919] BGH, 19.02.1998 – I ZR 233/95 = NJW-RR 1998, 1426; MDR 1998, 1403; VersR 1998, 1049; WM 1998, 2064; DB 1998, 2107.

abdeckt.[920] Eine Höhenbegrenzung ist dagegen unwirksam, wenn der Höchstbetrag die vertragstypischen, vorhersehbaren Schäden nicht abdeckt.[921] Haftungsbeschränkungen in AGB für Sach- und Vermögensschäden sind auch nur in der oben beschriebenen Form möglich. Haftungsbeschränkungen, die Personenschäden (Verletzung von Leben, Körper und Gesundheit) begrenzen wollen, sind gem. § 309 Abs. 2 Nr. 7a BGB generell unwirksam. Sind in AGB-Haftungsbeschränkungen enthalten, die gegen das AGB-Recht verstoßen, so sind diese unwirksam. An ihre Stelle treten gem. § 306 Abs. 2 BGB die gesetzlichen Regelungen, die grundsätzlich keine Haftungsbeschränkungen kennen.

Nach § 309 Nr. 8b BGB ist eine Bestimmung, durch die bei AGB-Verträgen über Lieferungen neu hergestellter Sachen und über Werkleistungen die Ansprüche gegen den Verwender wegen eines Mangels insgesamt oder bezüglich einzelner Teile ausgeschlossen. Dies zielt insbesondere darauf ab, den Kunden vor einer Aushöhlung seiner ihm kraft Gesetzes zustehenden **Mängelrechte** zu schützen und sicherzustellen, dass das Äquivalenzverhältnis von Leistungen und Gegenleistung auch bei mangelhafter Leistung des Verwenders durchgesetzt werden kann.[922] Diesem Grundanliegen muss grundsätzlich auch die Vertragsgestaltung im unternehmerischen Geschäftsverkehr Rechnung tragen.[923] Unwirksam sind gem. § 309 Nr. 8b lit. aa BGB auch im unternehmerischen Verkehr der vollständige Ausschluss der Rechte aus § 437 und § 634 BGB sowie eine ersetzende Verweisung des Vertragspartners auf einen Dritten.[924] Ferner, sind gem. § 309 Nr. 8b lit. bb BGB auch Beschränkungen der Mängelrechte auf den Nacherfüllungsanspruch, welcher auch für den unternehmerischen Verkehr gilt, nicht zulässig.[925] Auch können gem. § 309 Nr. 8b lit. cc BGB die Aufwendungen für die Nacherfüllung auch dann nicht auf die andere Vertragspartei abgewälzt werden, wenn es sich bei dem Dritten um einen unternehmerischen Kunden handelt.[926] Darüber hinaus gilt im unternehmerischen Geschäftsverkehr gem. § 309 Nr.

---

[920] *Ulmer/Brandner/Hensen*, AGB, 4. Aufl. 1999, § 11 Nr. 7 AGBG Rn. 35 f.

[921] BGH, 11.11.1992 – VIII ZR 238/91 = NJW 1993, 335; NJW-RR 1993, 564 (Ls.); ZIP 1993, 46; MDR 1993, 212; WM 1993, 24; BB 1992, 2460; DB 1993, 221; IBR 1993, 92; BGH, 19.01.1984 – VII ZR 220/82 = BGHZ 89, 363; NJW 1984, 1350; ZIP 1984, 457; MDR 1984, 482; BB 1984, 746; BGH, 23.02.1984 – VII ZR 274/82 = NJW 1985, 3016; ZIP 1984, 971; MDR 1984, 1018; WM 1984, 1224; BB 1984, 939; ZfBR 1990, 134; ZfBR 1991, 20; BGH, 21.01.2000 – V ZR 327/98 = MDR 2000, 448; NJ 2000, 538; WM 2000, 1069.

[922] Palandt/*Heinrichs*, 77. Aufl. 2017, § 309 Rn. 46.

[923] *Stoffels,* AGB-Recht, 5. Aufl. 2024, Rn. 959 f.

[924] BGH, 26.06.1991 – VIII ZR 231/90 NJW 1991, 2630, 2632; ZIP 1991, 1362; MDR 1992, 25; WM 1991, 1591; BB 1991, 1522; DB 1991, 2234; ZfBR 1996, 205; ZfBR 1992, 272; ZfBR 1991, 262; IBR 1992, 35; BGH, 12.01.1994 - VIII ZR 165/92 = BGHZ 124, 351; NJW 1994, 1060, 1066; NJW-RR 1994, 738 (Ls.); ZIP 1994, 461; MDR 1995, 260; WM 1994, 1121; BB 1994, 885; DB 1994, 2283.

[925] BGH, 02.02.1994 – VIII ZR 262/92 = NJW 1994, 1004, 1005; NZV 1994, 272 (Ls.); BGH, 05.11.1997 – VIII ZR 274/96 = NJW 1998, 679; WM 1998, 518.

[926] BGH, 09.04.1981 – VII ZR 194/80 = NJW 1981, 1510; ZIP 1981, 620; MDR 1981, 837; BB 1981, 935; DB 1981, 1719; BauR 1981, 378.

8b lit. dd BGB das Verbot der Vorenthaltung der Nacherfüllung.[927] Dagegen ist gem. § 309 Nr. 8b lit. ee BGB das Klauselverbot für Ausschlussfristen nicht auf den unternehmerischen Verkehr übertragbar.[928] Gem. § 309 Nr. 8b lit. ff BGB ist die Verjährung von Ansprüchen gegen den Verwender wegen eines Mangels in den Fällen des § 438 Abs. 1 Nr. 2 BGB und des § 634a Abs. 1 Nr. 2 BGB erleichtert oder in den sonstigen Fällen eine weniger als ein Jahr betragende Verjährungsfrist, ab dem gesetzlichen Verjährungsbeginn erreicht wird, nicht zulässig.

Die Möglichkeit einen **pauschalierten Schadensersatz** vertraglich zu vereinbaren, wird gerne im Bereich der Verzugsschäden gewählt.[929] Muss der Kunde normalerweise darlegen, dass beim **Verzug** durch eine zu spät erbrachte Leistung ein Schaden entstanden ist, muss er darüber hinaus auch noch darlegen, in welcher Höhe ihm dieser Schaden tatsächlich entstanden ist. Bei einer pauschalierten Schadenersatzregelung für einen Verzug muss er dagegen lediglich darlegen, dass eine Leistung zu spät erbracht worden ist. Die Darlegungspflicht für die tatsächliche Höhe des Schadensersatzes entfällt, an diese Stelle tritt die im Vertrag zuvor vereinbarte Pauschale. Wobei dem Schädiger die Möglichkeit zugestanden wird, durch einen Nachweis darzulegen, dass der Schaden geringer war als die Pauschale.[930]

Die Grenzen vorformulierter Schadensersatzpauschalen ergeben sich in erster Linie aus § 309 Nr. 5 BGB, außerhalb der tatbestandlichen Grenzen aber auch aus § 307 BGB.[931] Nach § 309 Nr. 5 BGB sind Vereinbarungen eines pauschalierten Anspruchs des Verwenders auf Schadensersatz oder Ersatz einer Wertminderung, wenn a) die Pauschale den in den geregelten Fällen nach dem gewöhnlichen Lauf der Dinge zu erwartenden Schaden oder die gewöhnlich eintretende Wertminderung übersteigt oder b) dem anderen Vertragsteil nicht ausdrücklich der Nachweis gestattet wird, ein Schaden oder eine Wertminderung sei überhaupt nicht entstanden oder wesentlich niedriger als die Pauschale. Der Maßstab für § 309 Nr. 5 a) BGB ist in § 252 S. 2 BGB nachgebildet.[932] Maßgebende Vergleichsgröße ist der

[927] Palandt/*Heinrichs*, 72. Aufl. 2013, § 309 Rn. 73; *Erman*, in: Hefermehl/Werner, BGB, 9. Aufl. 1993, § 11 Nr. 10 AGBG Rn. 36.
[928] *Stoffels,* AGB-Recht, 5. Aufl. 2024, Rn. 964.
[929] BGH, 16.09.1970 – VIII ZR 239/68 = NJW 1970, 2017.
[930] Palandt/*Heinrichs*, 72. Aufl. 2013, § 276 Rn 26.
[931] *Basedow*, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 5/1: Schuldrecht Besonderer Teil III/1, 7. Auflage 2017, § 309 Nr. 5 Rn. 8.
[932] BGH, 28.05.1984 – III ZR 231/82 = NJW 1984, 2941; ZIP 1984, 1324; MDR 1985, 299; WM 1984, 1174; BB 1984, 1829.

branchentypische Durchschnittsschaden[933] bzw. die im Durchschnitt der Fälle eintretende Wertminderung. Bei § 309 Nr. 5 b) BGB ist eine Schadenspauschalierungsabrede nur wirksam, wenn sie umgekehrt den Nachweis eines geringeren Schadens ausdrücklich zulässt.[934]

Schwierigkeiten bereitet oftmals die Abgrenzung der Schadensersatzpauschalen von den Vertragsstrafen.[935] Während in § 309 Nr. 5 BGB die formularmäßigen Grenzen für den pauschalierten Schadenersatz enthalten sind, sind in § 309 Nr. 6 BGB die Wirksamkeitsschranken für die Vertragsstrafe enthalten. Bei den Wirksamkeitsschranken des § 309 Nr. 6 BGB ist auf die Art des Anspruchs, der aus dem das Zahlungsbegehren hergeleitet wird, abzustellen. Es gilt im Wege der Auslegung den mit der Vereinbarung verfolgten Zweck zu ermitteln. Soll sie in erster Linie die Erfüllung des Hauptanspruchs sichern und auf den Vertragsgegner einen möglichst wirkungsvollen Druck ausüben,[936] so liegt der Sache nach eine Vertragsstrafenvereinbarung vor. Um eine Schadenspauschalabrede handelt es sich dagegen, wenn sie der vereinfachenden Durchsetzung eines als bestehend vorausgesetzten Vertragsanspruchs dienen soll. Im Klauseltext enthaltene Formulierungen wie „*Entschädigung*“ oder „*Schadensersatz*“ deuten zwar auf eine schadensersatzrechtliche Ausgleichsfunktion hin. Entscheidend ist letztlich jedoch die Höhe der zu zahlenden Geldsumme. Eine Schadenspauschale setzt begrifflich eine am Schaden orientierte Pauschalierung voraus.[937] Gem. § 309 Nr. 6 BGB ist in Allgemeinen Geschäftsbedingungen eine Bestimmung unwirksam, durch die dem Verwender für den Fall der Nichtabnahme oder verspäteten Abnahme der Leistung, des Zahlungsverzugs oder für den Fall, dass der andere Vertragsteil sich vom Vertrag löst, die Zahlung einer Vertragsstrafe versprochen wird. Die strikten Verbotstatbestände des § 309 Nr. 6 BGB lassen sich nicht auf den unternehmerischen Geschäftsverkehr übertragen.[938] I. d. R. sind Klauseln in AGB auch für den unternehmerischen Geschäftsverkehr bei der Vereinbarung einer verschuldensunabhängigen Vertragsstrafe, beim Ausschluss der Anrechnung der Vertragsstrafe auf den

[933] BGH, 16.01.1984 – II ZR 100/83 = NJW 1984, 2093, 2094; MDR 1985, 29; FamRZ 1984, 868; *Ulmer/Brandner/Hensen*, 4. Aufl. 1999, § 11 Nr. 5 AGBG Rn. 14.

[934] *Stoffels*, AGB-Recht, 5. Aufl. 2024, Rn. 893.

[935] BGH, 06.11.1967 – VIII ZR 81/65 = BGHZ 49, 84; NJW 1968, 149; BGH, 08.10.1969 - VIII ZR 20/68 = NJW 1970, 29; VersR 1959, 1142; BGH, 30.06.1976 – VIII ZR 267/75 = NJW 1976, 1886; BGH, 24.04.1992 - V ZR 13/91 = NJW 1992, 2625; ZIP 1992, 939; MDR 1992, 965; DNotZ 1992, 659; WM 1992, 1411; DB 1992, 1774; DB 1992, 1174; IBR 1992, 463.

[936] Palandt/*Heinrichs*, 72. Aufl. 2013, § 276 Rn 26.

[937] *Stoffels,* AGB-Recht, 5. Aufl. 2024 Rn. 886.

[938] *Ulmer/Brandner/Hensen*, 4. Aufl. 1999, § 11 Nr. 6 AGBG Rn. 17; *Wolf/Horn/Lindacher*, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 4. Aufl. 1999, § 11 Nr. 6 AGBG Rn. 33; *Staudinger/Coester/Waltjen,* BGB, § 11 Nr. 6 AGBG Rn. 27; Palandt/*Heinrichs*, 72. Aufl. 2013, § 309 BGB Rn. 38.

Schadensersatz[939] und beim Verzicht auf den Vorbehalt der Vertragsstrafe.[940] Darüber hinaus kann auch die unangemessene Höhe der ausbedungenen Vertragsstrafe Anlass zur Beanstandung geben.[941] Gerade im unternehmerischen Geschäftsverkehr muss jedoch eine fühlbare Sanktion möglich sein.[942] Gleichwohl ergeben sich Wirksamkeitsgrenzen, die gemäß § 307 Abs. 1 BGB beachtet werden müssen: Es ist unerlässlich, dass zwischen der Höhe der Vertragsstrafe einerseits und der maximalen Belastung des Kunden auf Grund der verwirkten Vertragsstrafe andererseits eine angemessene Relation besteht.[943] Die Höhe der Vertragsstrafe wird deshalb dann unangemessen im Sinn von § 307 Abs. 1 BGB, wenn ihre Sanktion außerhalb eines angemessenen Verhältnisses zum Vertragsverstoß, seinem Gewicht und seinen Folgen für den AGB-Verwender steht.[944] Vertragsstrafen sind in diesem Bereich ein weithin übliches und notwendiges Druckmittel, um die Gegenseite zur ordnungsgemäßen Vertragserfüllung anzuhalten.[945] Darüber hinaus sollen sie dem Gläubiger im Verletzungsfall die Möglichkeit einer erleichterten Schadloshaltung – ohne zu einem Einzelnachweis gezwungen zu sein – eröffnen.[946] Wenn daher die Vertragsstrafe an dem Umfang der geschuldeten Leistung, deren Erfüllung sie sichern soll, anknüpft und durch sie nach oben begrenzt ist, fehlt es an einer unangemessenen Benachteiligung im Sinn von § 307 Abs. 1 BGB.[947] Dies gilt auch dann, wenn ein so genannter „Summierungseffekt" vorliegt, etwa dann, wenn Vertragsstrafen für mehrere vertragliche Verpflichtungen nebeneinander vorgesehen sind.[948] Voraussetzung ist hier jedoch, dass dieser „Summierungseffekt" nicht über das hinausgeht, was bei gehöriger Erfüllung des Vertrages vom Schuldner erwartet werden konnte und erwartet wurde.[949] Dabei kam der BGH zu der Auffassung, dass eine Aufsummierung aller Verstöße gegen ein Unterlassungsgebot dann ausscheidet, wenn die Parteien eine Vertragsstrafe für jedes einzelne verkaufte Produkt vereinbart

[939] BGH, 29.02.1984 – VIII ZR 350/82 = NJW 1985, 53, 56; ZIP 1984, 841; MDR 1985, 223; WM 1984, 663; BB 1984, 1508.
[940] *Wolf/Horn/Lindacher*, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 4. Aufl. 1999, § 11 Nr. 6 AGBG Rn. 38.
[941] *Stoffels,* AGB-Recht, 5. Aufl. 2024 Rn. 917.
[942] OLG Frankfurt, 21.05.1985 - 5 U 206/84 = MDR 1985, 934; VersR 1986, 147; BB 1985, 1560.
[943] BGH, NJW 2009, 1882, 1885; 1994, 1060 – Daihatsu.
[944] BGH, NJW 2009, 1882, 1885; 1998, 2600 – Treuhand; 1997, 3233, 3234 – Citroën; 1994, 1060 – Daihatsu.
[945] *Stoffels,* AGB-Recht, 5. Aufl. 2024 Rn. 916.
[946] BGH, NJW 1998, 2600, 2602 – Treuhand; 1975, 115, 116.
[947] *Thüsing,* in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke, 41. EL April 2018, Rn. 18.
[948] BGH, NJW 1998, 2600, 2602 – Treuhand; 1975, 115, 116.
[949] *Thüsing,* in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke, 41. EL April 2018, Rn. 18.

haben.[950] In dem zugrunde liegenden Fall entstand so durch das Inverkehrbringen des Produkts aus der Summe von 7000 Vertragsverstößen eine Strafe von über 53 Mio. Euro, welche gemäß § 242 BGB wegen unverhältnismäßiger Höhe auf ein Maß herabzusetzen war, das jedenfalls 2 Mio. Euro nicht übersteigt.[951] Eine Summierung darf es schließlich nach der höchstrichterlichen Rechtsprechung auch nicht in der Form geben, dass die Vertragsstrafenregelung eine für die schuldhafte Überschreitung einer Zwischenfrist zu zahlende Vertragsstrafe von höchstens 5% der Gesamtauftragssumme festlegt.[952] Durch die Festlegung, dass eine Vertragsstrafe auch bei der Versäumung von Zwischenfristen verwirkt sein soll, wird der Vertragspartner des Verwenders unangemessen benachteiligt, da es zu einer Aufsummierung von Strafen kommen kann, obwohl der für den Verwender in der Regel allein bedeutsame Endtermin eingehalten wird.[953]

Auch ist eine pauschale Vertragsstrafen-Regelung in B2B-AGB unwirksam, wenn die Regelung nicht nach Art der jeweiligen Pflichtverletzung differenziert.[954] Die Geschäftsbedingungen seien nach dieser Entscheidung des BGH unwirksam, da sie die Beklagte unangemessen benachteilige. Auch im geschäftlichen Verkehr müsse die angedrohte Vertragsstrafe in einem angemessenen Verhältnis zur begangenen Pflichtverletzung stehen. Diesem Grundsatz würde die hier vorliegende AGB-Regelung nicht gerecht, denn die Vertragsstrafe würde bei jeder Pflichtverletzung, unabhängig von der jeweiligen Wichtigkeit der verletzten Pflicht, fällig. Daran ändere auch nichts der Umstand, dass die Regelung nur bei vorsätzlichen Pflichtverletzungen greife. Denn auch in diesem Rahmen erfolge die Ausgestaltung der Vertragsstrafe undifferenziert. Die Klägerin habe zwar aufgrund ihres Geschäftskonzeptes ein berechtigtes Interesse an der Einhaltung der vertraglichen Vereinbarungen. Dies führe jedoch nicht dazu, eine pauschale, allgemeine Vertragsstrafe für jeden Verstoß einzuführen.

[950] BGH, NJW 2009, 1882, 1885.
[951] BGH, NJW 2009, 1882, 1885.
[952] BGH, NZBau 2013, 222.
[953] *Thüsing,* in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke, 41. EL April 2018, Rn. 18.
[954] BGH, 31.08.2017 - VII ZR 308/16 = NJW 2017, 10; NJW 2017, 3145; MDR 2017, 1171; WM 2018, 1273; BB 2017, 2254; ZfBR 2017, 777.

j) Schutzrechte Dritter

Die Verletzung von Schutzrechten kommt in der Praxis meist dann zum Tragen, wenn mit einem KI-System ein Recht (i. d. R. ein Nutzungsrecht) übertragen wird, an dem der Hersteller keine Rechte besitzt bzw. er nicht über alle notwendigen Rechte verfügt. Diese Rechte stehen meist einem Dritten zu, dessen Schutzrechte der Hersteller mit der Übertragung auf dem Kunden dann ggf. verletzt hat. Gem. § 435 S. 1 BGB ist eine Sache frei von Rechtsmängeln, wenn Dritte in Bezug auf die Sache keine oder nur die im Kaufvertrag übernommenen Rechte gegen den Käufer geltend machen können. Es ist vor allem das beschränkte dingliche Recht, das am Sacheigentum haftet und sich gegen jeden Eigentümer durchsetzt, der es nicht nach §§ 892, 932, 936 BGB gutgläubig erworben hat.[955] Im Kaufrecht wird in § 433 Abs. 1 S. 2 BGB dem Verkäufer deutlich das Recht auferlegt, dem Käufer die Sache frei von Sach- und Rechtsmängeln zu verschaffen. Man findet sie in den §§ 437 bis 444 BGB, die allgemein vom Mangel einer Sache handeln und deshalb gleichermaßen als Rechts- und Sachmängel gelten. Also hat der Käufer nach § 439 BGB Anspruch auf Nacherfüllung, nach § 323 BGB ein Recht zum Rücktritt vom Vertrag, nach § 441 BGB ein Recht, den Kaufpreis zu mindern, und nach §§ 280 ff. BGB einen Anspruch auf Schadensersatz in mehreren Varianten.[956] Die Beweislast für den Rechtsmangel liegt nicht mehr unterschiedslos beim Käufer, wie es vor der Schuldrechtsreform der Fall war,[957] sondern richtet sich nach der allgemeinen Regel des § 363 BGB.

k) Haftung für Deep Learning

Werden mittels eines KI-Algorithmus (z. B. ein selbstlernender Algorithmus) Daten erhoben und werden diese Daten an einen Dritten verkauft (z. B. Bonitätsdaten), so stellt sich die Frage, inwieweit der Verkäufer dieser KI-Daten für die Richtigkeit der Daten haftet. Bei einem klassischen Datenhandel durch einen KI-Betreiber, welcher (fehlerhafte) Daten/Informationen (Smart Data) als Beratungsleistung an seinen Kunden liefert, wird man regelmäßig eine Verletzung der Hauptleistungspflicht bejahen können.[958] Wird durch das KI-Unternehmen eine Beratungsdienstleistung angeboten, so greifen grundsätzlich die

[955] BGH, 19.11.1999 – V ZR 321/98 = NJW 2000, 803; MDR 2000, 261; WM 2000, 578; BB 2000, 222; IBR 2000, 139.
[956] *Schellhammer*, Schuldrecht nach Anspruchsgrundlagen,11. Aufl. 2021, Rn. 117.
[957] Veraltet: BGH, 15.02.1955 – I ZR 108/53 = BGHZ 16, 307; NJW 1955, 585.
[958] Vgl. *Andrees/Bitter/Buchmüller/Uecker*, in: Hoeren, S. 104, die aber nur unzureichend zwischen Nebenleistungs- (i. S. d. § 241 Abs. 1 BGB) und Nebenpflichten (i. S. d. § 241 Abs. 2 BGB) differenzieren.

allgemeinen Leistungsstörungsrechte aus §§ 280 ff. BGB, da das Dienstvertragsrecht insofern kein besonderes Gewährleistungsrecht vorsieht.[959] Wie beim normalen Dienstvertragsrecht wird dann ein Verschulden des KI-Unternehmens gem. § 280 Abs. 1 S. 2 BGB vermutet, der zu führende Nachweis der haftungsausfüllenden Kausalität, namentlich der Kausalität zwischen Pflichtverletzung und Schaden, kann aber durchaus problematisch sein.[960]

Ein anderer Fall liegt vor, wenn das KI-Unternehmen fehlerhafte Daten im Rahmen eines Dienstleistungsvertrages zur Verfügung stellt, damit jener diese analysiert oder auswertet. Im Rahmen eines klassischen Dienstleistungsvertrages i. S. d. §§ 611 ff. BGB haftet das KI-Unternehmen dem Auftraggeber gegenüber jedenfalls erst ab Übergabe der Daten für deren Mangelfreiheit.[961] Problematisch sind in diesem Zusammenhang die Fragen nach Fehlerfreiheit oder Mangelhaftigkeit in Sinne des Gesetzes, was die Praxis vor erhebliche Herausforderungen stellt. Natürlich sind deutliche Unterschiede z. B. bei Bonitätsdaten erkennbar, aber bei nicht deutlichen Abweichungen stellt sich auch die Frage, wie daraus ein Schaden entstehen kann. Auch nach Behebung eines Mangels erscheint das soeben Genannte fraglich, da dies das Dienstvertragsrecht gar nicht vorsieht und die Behebung immer nur nachträglich erfolgen kann. Bonitätsdaten sind aber immer auf den Augenblick bezogen, eine Bonität eines Kunden kann sich innerhalb von Sekunden verändern. Somit ist der Anspruch aus §§ 611 ff. BGB ausreichend, um qualitativ hochwertige Daten zur Verfügung zu stellen zwar richtig, aber bei Pflichtverletzung erscheint es in der Praxis schwer, entsprechende Rechte aus §§ 611 ff. BGB geltend zu machen.[962] Die Vergütungspflicht des Auftraggebers bleibt damit ohne Nachleistungsverpflichtung des KI-Unternehmens bestehen, § 615 BGB. Im Falle der unmöglichen - das heißt tatsächlich nicht nachholbaren[963] – Datenlieferung, die einen Gläubigerverzug ausschließen würde, ergibt sich dies bereits aus §§ 275 Abs. 1, 326 Abs. 2 BGB.[964]

---

[959] Vgl. allgemein zum Dienstvertrag: *Müller-Glöge*, in: MüKo-BGB, 6. Aufl. 2012, § 611 BGB Rn. 23; *Mansel*, in: Jauernig, § 611 BGB Rn. 13; *Weidenkaff*, in: Palandt, § 611 BGB Rn. 15 f.

[960] Vgl. *Roßnagel*, NJW 2017, 10, 13 f., allerdings ohne Beachtung der Verschuldensvermutung.

[961] *Roßnagel*, NJW 2017, 10, 14; *Peschel/Rockstroh*, MMR 2014, 571, 576.

[962] *Kirchner*, InTeR 2018, 19 bis 24.

[963] *Weidenkaff*, in: Palandt, § 615 BGB Rn. 4.

[964] *Roßnagel*, NJW 2017, 10, 12 f., 14 f., jedoch ohne entsprechende Differenzierung.

III. Betreiberhaftung

Bei der Betreiberhaftung geht es darum, inwieweit dem Betreiber eines KI-Systems, wie z. B. eines Roboters, Verwender eines Algorithmus oder dem Halter eines autonomen Fahrzeuges eine Pflicht zur Sicherung der Gefahrenquelle trifft. Teilweise wird der Gedanke aufgebracht, „Halter" von autonomen Systemen zum Abschluss einer Haftpflichtversicherung für von diesen verursachte Schäden zu verpflichten.[965] Zwar wären dadurch Schwierigkeiten bei der Ermittlung der haftungsbegründenden Kausalität und des Verschuldensgrads nicht beseitigt, Geschädigte wären allerdings besser vor dem Insolvenzrisiko potenzieller Anspruchsgegner geschützt.[966]

1. Pflichtverletzungen

Eine Betreiberhaftung eines Unternehmen welches KI Technologien verwendet, kann grundsätzlich bejaht werden, da den Betreiber einer potenziellen Gefahrenquelle immer eine Verkehrssicherheitspflicht trifft.[967] An dieser Pflicht ändert sich auch nichts, wenn das Verhalten der Systeme nicht vorhersehbar ist, da es auf die Erhöhung des Risikos bzw. der Gefährdungslage und die daraus resultierenden Verkehrspflichten ankommt.[968] Bei Robotern als KI-System wird z. T. vertreten, dass nach geltendem Recht nur der Betreiber für ein Versagen der Roboter (oder selbststeuernder Kfz) haftbar gemacht werden kann, da es unter Umständen an einem Verschulden desjenigen fehle, der das Verhalten des Systems nicht vorhersehen könne, der Vorwurf des Verhaltensunrechts sich damit auf den Einsatz des Systems selbst reduziere. Daraus resultiere ein Defizit in der Steuerungsintention des pflichtenbasierten Haftungsrechts, was zudem innovationsfeindlich wirke.[969] Die Kritik ist insoweit berechtigt, dass sie die Nähe der Verkehrspflichten zur Gefährdungshaftung betont; in der Tat ergeben sich hier zunehmend Grauzonen, indem oftmals übersteigerte Verkehrspflichten aufgestellt werden.[970] Dennoch erscheint die Kritik überzogen: Denn es

[965] *Günther/Böglmüller*, BB 2017, 53 bis 58.

[966] Einen umfassenden Überblick über mögliche Haftungskonzepte im Bereich der Robotik gibt *Hanisch*, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 27.

[967] *Lutz*, NJW 2015, 119, 120 f.

[968] *Spindler*, CR 2015, 766.

[969] So im Ansatz *Hanisch,* in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 27, 34; *Jänisch/Schrader/Reck*, NZV 2015, 313, 318; *Fleck/Thomas*, NJOZ 2015, 1393, 1397 appellieren deswegen an den Gesetzgeber und fordern ein aktives Begleiten des Fortschritts; ebenfalls kritisch hinsichtlich der Haftungsverschiebung zu Lasten der Hersteller: *Lutz*, NJW 2015, 119, 120 f.

[970] Vgl. *Rohe*, AcP 201, 2001, 118, 134 ff.; *Spindler*, in: BeckOGK/BGB, § 823 Rn. 574; krit. bereits *Esser*, JZ 1953, 129.

dürften sich durchaus Pflichten beim Einsatz der KI-Systeme ableiten lassen, sei es der sorgsamen Festlegung des Einsatzes, der Überwachung des Systems und seiner Beobachtung bis hin zum möglichen Eingreifen bei Fehlfunktionen.[971]

Wer eine Maschine, einen Roboter, autonome Fahrzeuge, eine Software etc. einsetzt, haftet natürlich auch für deren Einsatz.[972] Ihn treffen insoweit Pflichten zur Sicherung der Gefahrenquelle. Daran ändert auch die Tatsache nichts, dass das Verhalten von KI-gesteuerten Systemen nicht immer vorhersehbar ist, da es auf die Erhöhung des Risikos bzw. der Gefährdungslage und die daraus resultierenden Verkehrspflichten ankommt.[973] Dennoch wird in der Literatur vertreten, dass nach geltendem Recht Betreiber für ein Versagen der Roboter, KI-Systeme oder selbststeuernden Fahrzeuge haftbar gemacht werden könnten, da es unter Umständen an einem Verschulden desjenigen fehlt, der das Verhalten des Systems nicht vorhersehen konnte. Damit würde sich der Vorwurf des Verhaltensunrechts auf den Einsatz des Systems selbst reduzieren.[974] Daraus resultiere, so wird argumentiert, ein Defizit in der Steuerungsintention des pflichtenbasierten Haftungsrechts, was zudem innovationsfeindlich wirke.[975] Die Argumentation ist nicht ohne Weiteres von der Hand zu weisen, da sie die Nähe der Verkehrspflichten zur Gefährdungshaftung betont; in der Tat ergeben sich hier zunehmend Grauzonen, indem oftmals übersteigerte Verkehrspflichten aufgestellt werden.[976] Dennoch ist das Ergebnis nicht interessengerecht, da Überwachungs- und Steuerungspflichten zu den fundamentalen Pflichten eines Betreibers gehören. Dies kann auch die Pflicht zum möglichen Eingreifen bei Fehlfunktionen sein.[977] Die strafrechtlichen Aspekte sind dabei separat zu betrachten. Ein Fehlverhalten eines KI-Systems/Roboters, stammt es nun aus dem Autonomiebestreben oder aus einem sonstigen Grund, zieht immer eine Reihe von Haftungsfragen nach sich. Diese können sich zum einem aus einer vertraglichen Pflichtverletzung gem. § 280 Abs. 1 BGB, zum anderem aus dem Deliktsrecht nach § 823 BGB gegenüber fremden Dritten oder auch aus dem Produkthaftungsgesetz ergeben.

Wird ein KI-System/Roboter im Rahmen eines Vertragsverhältnisses (z. B. Miete) bei einer

---

971 Ähnlich aus strafrechtlicher Sicht *Gleß/Weigend*, ZStW 126, 2014, 561, 585 f.

972 *Groß,* InTeR 2018, 4, 7. Andere Ansicht *Reusch/Weidner,* Future Law 2018, 2018, Rn. 59.

973 *Spindler*, CR 2015, 766.

974 *Spindler*, CR 2015, 766.

975 So im Ansatz *Hanisch,* in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 27, 34; *Jänisch/Schrader/Reck*, NZV 2015, 313, 318; *Fleck/Thomas*, NJOZ 2015, 1393, 1397 appellieren deswegen an den Gesetzgeber und fordern ein aktives Begleiten des Fortschritts; ebenfalls kritisch hinsichtlich der Haftungsverschiebung zu Lasten der Hersteller Lutz, NJW 2015, 119, 120 f.

976 Vgl. *Rohe*, AcP 201, 2001, 118, 134 ff.; *Spindler*, in: BeckOK/BGB, § 823 Rn. 574; kritisch bereits *Esser*, JZ 1953, 129.

977 Ähnlich aus strafrechtlicher Sicht *Gleß/Weigend*, ZStW 126, 2014, 561, 585 f.

anderen Vertragspartei tätig und erzeugt der Roboter dabei Schäden bei dieser Partei, so stellt dies sicherlich eine Pflichtverletzung i. S. v. § 280 BGB dar. Ein durch die Medien bekannt gewordener Fall ist die Verwendung des ROBODOC von Integrated Surgical System, welche zu zahlreichen Schadensersatzforderungen geführt hat.[978] Der Schutz der Rechtsgüter der Benutzer erfordert es, dass von dem Betreiber nicht nur die Einhaltung der allgemein anerkannten Regeln der Technik verlangt wird. Sind Schädigungen zu beklagen, wenn die Kunden bei der Nutzung der Anlage – zwar selten, aber vorhersehbar – nicht die notwendigen Verhaltensregeln einhalten, muss der Betreiber in geeigneter Weise darauf hinwirken, dass kein Fehlverhalten vorkommt. Den Betreiber trifft deshalb die Pflicht, die Benutzer (Dritte) in geeigneter und ihm zumutbarer Weise über die zu beachtenden Verhaltensregeln zu informieren.[979]

Den Betreiber eines algorithmusgesteuerten KI-Systems, wie z. B. einer Suchmaschine, treffen erst dann spezifische Verhaltenspflichten, wenn er durch einen konkreten Hinweis Kenntnis von einer offensichtlichen und auf den ersten Blick klar erkennbaren Rechtsverletzung erlangt hat.[980] Der Hinweis ist erforderlich, um den grundsätzlich nicht zur präventiven Kontrolle verpflichteten Anbieter in die Lage zu versetzen, in der Vielzahl der indexierten Internetseiten diejenigen auffinden zu können, die möglicherweise die Rechte Dritter verletzen.[981] Ein Rechtsverstoß kann beispielsweise im oben genannten Sinn auf der Hand liegen bei Kinderpornografie, Aufruf zur Gewalt gegen Personen, offensichtlichen Personenverwechslungen, Vorliegen eines rechtskräftigen Titels gegen den unmittelbaren Störer, Erledigung jeglichen Informationsinteresses durch Zeitablauf[982] oder eindeutiger Schmähkritik. Als praktischer Fall im Bereich KI-Systemen gilt der von Microsoft entwickelte Chatbot „Tay." Er sollte im Netz lernen, wie junge Menschen reden. Nach wenigen Stunden musste der Versuch abgebrochen werden, da Tay Aussagen wie „bush did 9/11 and Hitler would have done a better job than the monkey we have now. Donald Trump is the only hope we've got" gelernt hatte. Ebenso der Ruf nach Völkermord sowie rassistische

978 BGH, 13.06.2006 – VI ZR 323/04 = BGHZ 168, 103; NJW 2006, 2477; MDR 2007, 153; VersR 2006, 1073; JR 2007, 191.
979 NJW 2018, 2956 = MDR 2018, 1116; NJW 2018, 2956.
980 Vgl. zum Umfang der Prüfpflichten eines Suchmaschinenbetreibers auch OLG Hamburg, ZUM-RD 2012, 32; LG Hamburg, NJW 2015, 796.
981 Vgl. BGHZ 191, 19 Rn. 21, 28 – Stiftparfüm.
982 Vgl. EuGH, ZUM 2014, 559 Rn. 92 ff. – Google Spain, Hassreden (vgl. EGMR, NJW 2015, 2863 Rn. 153 ff. – Delfi AS/Estland).

und sexistische Bemerkungen aller Art.[983] Hätte Microsoft nicht reagiert, wäre es nach den oben beschriebenen Kriterien haftbar gewesen. Allerdings ist die Grenze schwer zu ziehen. Gerade bei Schmähkritik ist die Erkennbarkeit einer offensichtlichen Rechtsverletzung für den Suchmaschinenbetreiber problematisch. Die Grenze zulässiger Meinungsäußerungen liegt nicht schon da, wo eine polemische Zuspitzung für die Äußerung sachlicher Kritik nicht erforderlich ist.[984] Eine Schmähkritik kann nicht bereits dann angenommen werden, wenn eine Äußerung überzogen oder ausfällig ist.[985] Hinzutreten muss eine das sachliche Anliegen der Äußerung völlig in den Hintergrund drängende persönliche Kränkung,[986] deren abschließende Bewertung ohne verifizierbare Erkenntnisse zum sachlichen Hintergrund selten möglich ist. Entsprechendes gilt für herabsetzende Tatsachenbehauptungen oder Werturteile mit Tatsachenkern. Denn hier kommt es maßgeblich auf den Wahrheitsgehalt der behaupteten Tatsache an.[987] Hierzu hat der KI-Betreiber typischerweise keine Erkenntnisse. Ist eine Validierung des Vortrags der Betroffenen somit regelmäßig nicht möglich, führt auch der Maßstab der »offensichtlich und auf den ersten Blick klar erkennbaren Rechtsverletzung« nur in Ausnahmefällen zu einem eindeutigen Ergebnis für den KI-Betreiber. Eine sichere und eindeutige Beurteilung, ob unter Berücksichtigung aller widerstreitenden grundrechtlich geschützten Belange und der Umstände des Einzelfalls, das Schutzinteresse der Betroffenen die schutzwürdigen Belange der Geschädigten[988], ist dem KI-Betreiber im Regelfall nicht ohne Weiteres möglich.

a) Verschulden

Fraglich ist, ob dem Betreiber ein eigenes Verschulden gem. § 280 Abs. 1 i. V. m. § 276 BGB zugerechnet werden kann. Der BGH[989] hat bereits früh aufgezeigt, dass er sich ein eigenes Verschulden des Betreibers bei Wartung und Betrieb vorstellen kann, wenn es unterlassen wurde, eine ordnungsgemäße Einstellung und Wartung des (KI-)System

---

983 *Beuth,* Zeitonline vom 24.03.2016, Microsoft Twitter-Nutzer machen Chatbot zur Rassistin.

984 BVerfG, ZUM-RD 2016, 569 Rn. 13; BVerfGE 82, 272, 283 f.; 85, 1, 16.

985 BGH, 27.02.2018 – VI ZR 489/16: Haftung des Betreibers einer Suchmaschine für persönlichkeitsrechtsverletzende Inhalte Dritter, NJW 2018, 2324; ZIP 2018, 1980; MDR 2018, 592; GRUR 2018, 642; VersR 2018, 881; WM 2018, 824; MMR 2018, 449; K&R 2018, 391; ZUM 2018, 433; afp 2018, 322.

986 Vgl. BVerfGE 93, 266 7. b); BVerfGE 82, 272, 284.

987 *V. Pentz*, AfP 2017, 102, 115.

988 Vgl. BGHZ 209, 139 = ZUM-RD 2016, 355 Rn. 30; BGHZ 199, 237 = ZUM-RD 2014, 145 Rn. 22 – Sächsische Korruptionsaffäre; Senat, ZUM-RD 2016, 292 Rn. 20; ZUM-RD 2016, 362 Rn. 29; ZUM-RD 2015, 151 Rn. 13 – Filialleiter bei Promi-Friseur; ZUM-RD 2015, 83 – Innenminister unter Druck; ZUM-RD 2014, 430 Rn. 8 – Adoptivtochter.

989 BGH, 16.10.2012 – X ZR 37/12 = BGHZ 195, 126; NJW 2013, 598; NJW 2017, 3092; MDR 2012, 14; MDR 2013, 141; NJ 2013, 293; VersR 2013, 779; WM 2013, 2386; MMR 2013, 296; K&R 2013, 113.

vorzunehmen.[990] Die Haftung entfällt dabei, wenn der Entlastungsbeweis gem. § 280 Abs. 1 S. 2 BGB geführt wird und somit der Beweis darlegt worden ist, dass eine ordnungsgemäße Einstellung und Wartung vorgenommen wurde.[991] Die Haftung des Betreiber entfällt hierbei schon wegen bloßer Unmöglichkeit der Vermeidung unerwarteter Fälle gem. § 275 Abs. 1 oder 2 BGB.[992] Auch hat der BGH[993] die Haftung für den Betreiber bejaht, wenn der Algorithmus einer Suchmaschine Autovervollständigungen bei Suchanfragen vorschlägt, die aber tatsächlich auf dem Suchverhalten anderer Nutzer basieren.[994]

b) Analogie zur Tierhalterhaftung

Z. T. wird vertreten, dass ein KI-System autonom und bzw. teilautonom handelt und sich daraus andere Aspekte bei der Haftung ergeben könnte. Neu ist diese Sichtweise nicht, denken wir an die Tierhalterhaftung. Auch hier agieren Tiere autonom oder zumindest teilautonom und der Halter haftet dennoch entsprechend für sein Tier. Ob die Tierhalterhaftung ein Vorbild für die Haftung für autonome Systeme sein kann, wird bisher nur in Ansätzen diskutiert. Während teilweise eine Parallele gesehen wird,[995] freilich ohne deren Bedeutung näher zu erläutern, wird vereinzelt die Übertragung der in § 833 BGB angelegten Differenzierung auf die Schaffung von Regeln für autonome Systeme erwogen, teils aber auch jede Übertragung abgelehnt,[996] mitunter eine Nähe eher zu anderen Regeln, etwa der Gebäudehaftung, § 836 BGB, gesehen.[997]

Grundsätzlich ist die Tierhalterhaftung in § 833 BGB geregelt. Wird gem. § 833 S. 1 BGB durch ein Tier ein Mensch getötet oder der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt, so ist derjenige, welcher das Tier hält, verpflichtet, dem Verletzten den daraus entstehenden Schaden zu ersetzen. Dabei tritt gem. § 833 S. 2 BGB die Ersatzpflicht nicht ein, wenn der Schaden durch ein Haustier verursacht wird, das dem

990 *Groß/Gressel,* NZA 2016, 990, 995.
991 *Resuch/Weidner,* Future Law, 2018, Rn. 58.
992 *Bräutigam/Rücker,* E-Commerce, 2016, 14 B III Rn. 64.
993 BGH, 14.05.2013 – VI ZR 269/12 = BGHZ 197, 213; NJW 2013, 2348; NJW 2013, 28; MDR 2013, 710; GRUR 2013, 751; VersR 2013, 769; WM 2013, 1188; MMR 2013, 535; MIR 2013, Dok. 029; BB 2013, 1345; K&R 2013, 474; ZUM 2013, 550; afp 2013, 229; afp 2013, 260.
994 *Resuch/Weidner,* Future Law, 2018, Rn. 58.
995 *Brunotte*, CR 2017, 583, 585 f.; *Sosnitza*, CR 2016, 764, 772; dagegen etwa *Grützmacher*, CR 2016, 695, 698; zurückhaltend *Horner/Kaulartz*, CR 2016, 7, 14; de lege ferenda aufgeschlossener dies., InTeR 2016, 22, 24 f.
996 So in der Sache *Schaub*, JZ 2017, 342, 348, die zwischen privaten und gewerblichen Betreibern differenzieren will.
997 *Borges*, NJW 2018, 977.

Beruf, der Erwerbstätigkeit oder dem Unterhalt des Tierhalters zu dienen bestimmt ist, und entweder der Tierhalter bei der Beaufsichtigung des Tieres die im Verkehr erforderliche Sorgfalt an den Tag legt oder der Schaden auch bei Anwendung dieser Sorgfalt entstanden wäre. Die Vorschriften des § 833 BGB über die Tierhalterhaftung versuchen einen Spagat zwischen Gefährdungs- und Verschuldenshaftung.[998] Der Normzweck des § 833 BGB besteht darin, demjenigen, der die tatsächliche Gewalt über das Tier ausübt und dieses folglich kontrollieren kann, haftungsrechtliche Anreize zur Beherrschung der Kreatur im Interesse der Schadensvermeidung zu geben.

Während sich dieses Ziel auch mittels einer Verschuldenshaftung erreichen lässt, hat die Gefährdungshaftung den zusätzlichen Vorteil einer Steuerung des Aktivitätsniveaus.[999] Eine Steuerung des Aktivitätsniveaus durch Gefährdungshaftung ist nötig, wenn sich Schäden auch bei Einhaltung der Anforderungen der im Verkehr erforderlichen Sorgfalt nicht vermeiden lassen, oder wenn eine Gefahrenquelle in erheblichem Umfang Schäden verursacht, zu deren Vermeidung die Verschuldenshaftung keinen Anreiz gibt, weil sie sich durch Beachtung der erforderlichen Sorgfalt nicht vermeiden lassen, wie dies typischerweise bei wilden Tieren der Fall ist, die folgerichtig schon in Rom einem Sonderregime unterlagen (edictum de feris).[1000] Eine analoge Anwendung kommt generell in Betracht, wenn für einen bestimmten Sachverhalt keine Rechtsnorm existiert, d. h. eine Gesetzeslücke oder Regelungslücke vorliegt. Vielfach wird gefordert, dass diese planwidrig ist, d. h. vom Gesetzgeber nicht beabsichtigt war.[1001] Demgegenüber wird vertreten, dass eine Planwidrigkeit nur dann als unabdingbar für eine Analogie anerkannt werden kann, wenn man ausschließlich die subjektive Auslegungsmethode akzeptiert.[1002] Nach der objektiven Auslegungsmethode könnte man demgegenüber zu dem Ergebnis kommen, dass eine analoge Anwendung angebracht ist, also eine Gesetzeslücke vorliegt, obwohl der historische Gesetzgeber nachweislich keine Rechtsfolge an den Fall knüpfen wollte.[1003] Nach der subjektiven

---

998 MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 833 Rn. 1.

999 Diese Funktion der Gefährdungshaftung hat Posner mit folgendem Beispiel erläutert: „Keeping a tiger in one's backyard would be an example of an abnormally hazardous activity. The hazard is such, relative to the value of the activity, that we desire not just that the owner take all due care that the tiger not escape, but that he consider seriously the possibility of getting rid of the tiger altogether; and we give him an incentive to consider this course of action by declining to make the exercise of due care a defence to a suit based on an injury caused by the tiger – in other words, by making him strictly liable for any such injury." – G.J. Leasing Co. v. Union Elec. Co. (1995) 54 F. 3d 379, 386 (7th Cir. 1995).

1000 Vgl. *Zimmermann*, The Law of Obligations, 1996, P. 1105 ff.

1001 *Bydlinski*, Grundzüge der juristischen Methodenlehre, 2. Aufl. 2011, S. 23.

1002 *Rüthers,* Rechtstheorie, 4. Aufl. 2010, S. 25.

1003 *Puppe*, Kleine Schule des juristischen Denkens, 2. Aufl. 2011, S. 4.

Auslegungsmethode ist eine Regelungslücke planwidrig, wenn anzunehmen ist, dass der Gesetzgeber bei der Regelung eines Komplexes schlicht übersehen hat, eine Regelung zu treffen. [1004] Oft lässt sich aber auch aus den Wertungen der Verfassung oder etwaiger Generalklauseln ableiten, dass eine Lücke planwidrig ist, da sich der Gesetzgeber ansonsten in Widerspruch zu grundsätzlichen Wertungen gesetzt hätte. Die Frage, ob eine Lücke durch eine Analogie ausgefüllt werden kann, ist aber in beiden Fällen durch Auslegung zu ermitteln.[1005] Bei der KI könnte man unterstellen, dass diese Technologie so neu ist, dass der Gesetzgeber dafür keine speziellen Rechtsnormen wie den § 833 BGB geschaffen hat. Diese Argumentation ist natürlich mit Vorsicht zu genießen, da die analoge Anwendung der Tierhalterhaftung aus § 833 BGB nicht zur Anwendung kommen würde, wenn z. B. die Fälle einer Kreditgefährdung nach § 824 BGB vorliegen. Auch eine Anwendung von § 823 Abs. 1 BGB i. V. m. Art. 22 DSGVO dürfte zum Ausschluss der analogen Tierhalterhaftung nach § 833 BGB führen. Denkbar wiederum könnten Fälle in der Robotik und der Argumentation zum autonomen und bzw. teilautonomen KI-System sein. Es wird angenommen, dass die Interessenlage vergleichbar ist, wenn sich beide Sachverhalte in allen wesentlichen Merkmalen gleichen. Dies ist i. d. R. eine Wertentscheidung, denn auf den ersten Blick erscheinen Tiere und Roboter nicht vergleichbar. Bei Tieren handelt es sich um Lebewesen mit einem bewussten eigenen Willen, der zum Teil trainiert werden kann, bei Robotern oder KI-System handelt es sich um Software bzw. Maschinen, die durchaus gesteuert werden können und wenn eine Steuerung zu einem Schaden führt, dann war die Entwicklung des KI-System oder des Roboters mangelhaft. So hat der BGH gesagt, dass Software zwar voller Mängel sein kann, was aber nichts am Gewährleistungsrecht ändert.[1006] Es ist davon auszugehen, dass der BGH zu einem ähnlichen Ergebnis bei KI-Technologien kommen würde. Denkt man aber in der Zukunft weit über die Grenzen einer schwachen KI hinaus, so könnte man sicherlich zu der Frage kommen, inwieweit der Mensch zwar die im Verkehr erforderliche Sorgfalt bei der Entwicklung der KI eingehalten hat, aber das System so selbstständig geworden ist, dass es ähnlich wie ein Tier nur noch bedingt steuerbar ist. Denn auch bei Haustieren, die letztlich alle von wilden Tieren

[1004] *Bydlinsk*i, Grundzüge der juristischen Methodenlehre, 2. Aufl. 2011, S. 23,
[1005] *Larenz*, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, S. 5
[1006] BGH, 25.03.2010 – VII ZR 224/08, NJW 2010, 2200.

abstammen, zeigt die Erfahrung, dass sich ihr Verhalten nicht vollständig kontrollieren lässt,[1007] da sie über einen Urinstinkt verfügen, der sich nicht einfach abtrainieren lässt. Hier könnte man argumentieren, dass die KI so komplex in ihrer Entwicklung ist und sich selbständig, sprich autonom weiterentwickelt hat, dass eine vergleichbare Interessenlage zur Tierhaftung nach § 833 BGB anzunehmen ist. Analog zur Tierhalterhaftung lässt sich dann anführen, dass der KI-Betreiber wie der Tierhalter eine Quelle besonderer Gefahr zum eigenen Nutzen unterhält und sämtliche mit dieser Aktivität verbundenen (Schadens-)Kosten tragen sollte,[1008] zumal die Tierhaltung/das Betreiben der KI in der Gesellschaft ungleich verteilt ist, so dass sich die wechselseitige Gefährdung der Bürger nicht kompensiert. Der Tierhalter wie auch der Betreiber der KI wird durch die Haftung nicht übermäßig belastet, weil er das Schadensrisiko ohne Weiteres auf eine Haftpflichtversicherung umwälzen kann. [1009]

Die Gefahren der analogen Anwendung der Tierhalterhaftung nach § 833 BGB auf die KI liegen in den Ausschlüssen. Haftet ein Betreiber einer Maschine für diese, würde bei einer analogen Anwendung ggf. der KI-Betreiber ggü. einem Betreiber einer „normalen" Maschine privilegiert. Denn fügt ein unter menschlicher Leitung stehendes Tier einem anderen einen Schaden zu, versagt die Rechtsprechung einen Ersatzanspruch mit der Begründung, dass in diesen Fällen der das Tier leitende Dritte und nicht das folgsame Werkzeug Verursacher des Schadens sei.[1010] Folgerichtig wurde die Haftung verneint, wenn ein Reiter sein Pferd dicht an dasjenige seines Nebenmanns herangeführt hatte und Letzteres auskeilte[1011] oder ein Kutscher neben dem fahrenden Fuhrwerk ging und aus dieser Position Einfluss auf das Pferd nahm.[1012] Der Pferdehalter soll auch nicht dafür verantwortlich sein, wenn Einbrecher das Tier aus dem Stall und auf die Autobahn treiben.[1013] Dagegen greift trotz menschlicher Leitung die Haftung nach § 833 BGB ein, wenn willkürliche Bewegungen des Tieres wie Scheuen, Durchgehen, Beißen, Schlagen, Ausrutschen, Ausbrechen,

[1007] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 833 Rn. 1.

[1008] Vgl. BGHZ 67, 129, 130; BGH NJW-RR 1988, 655, 656: Es handele sich bei „der Tierhalterhaftung sozusagen um Betriebskosten einer gefahrträchtigen Veranstaltung"; ähnlich bereits RGZ 62, 79, 83; auf anderer Grundlage (Verschuldenshaftung mit Beweislastumkehr) auch die Zweite Kommission Prot. II S. 647.

[1009] MüKoBGB/*Wagner*, 7. Aufl. 2017, BGB § 833 Rn. 1.

[1010] *Israel,* JW 1902, 238, 240; *Deutsch*, NJW 1978, 1998, 2000.

[1011] BGH, 25.09.1952 - III ZR 334/51 = NJW 1952, 1329; VersR 1952, 403.

[1012] RG, 17.01.1907 - Rep. IV. 284/06 = RGZ 65, 103, 105 f.

[1013] BGH, VersR 1990, 796, 797 f.

Losgaloppieren und abruptes Anhalten eines Reitpferdes den Schaden verursacht haben.[1014] Diese Aspekte sind bei KI hingegen nicht gegeben, da sie auch durch richtige Sperren oder Maßnahmen (z. B. eines Super Codes) beherrschbar sind. Zum heutigen Zeitpunkt der Entwicklung ist der Mensch durchaus in der Lage, das Verhalten von KI in der Weise zu steuern, dass Haftungsfälle vermieden werden können und dass Haftungsfälle nur entstehen, wenn eine Sicherheitsmaßnahme in der KI fehlerhaft oder gar nicht erst implementiert worden ist. Es ist auch in der Praxis nicht nachvollziehbar, warum ein Hersteller von KI privilegiert werden sollte. Dies würde nämlich dazu führen, dass jeder Hersteller einer von Software gesteuerten Maschine in einer Hauptverhandlung behaupten würde, dass seine Maschine ein KI-System wäre, um von den Ausschlussregelungen der analogen Tierhalterhaftung nach § 833 BGB zu profitieren. Da es, wie in der Einleitung erläutert, für die Annahme von KI keine einheitliche Formel gibt, würde die ganze analoge Anwendung der Tierhalterhaftung zur einer Farce führen.

Zusammenfassend lässt sich festhalten, dass die analoge Anwendung der Tierhalterhaftung für KI abzulehnen ist, da nach dem derzeitigen Stand der Entwicklung der KI keine vergleichbare Interessenlage wie bei Tieren vorliegt.

c) Abgabe von Willenserklärungen

Eine weitere Frage der Betreiberhaftung ist, inwieweit das Handeln der KI im rechtsgeschäftlichen Sinne dem Betreiber der KI zuzurechnen ist. Diese Frage ist vor allem auch im Zusammenhang mit teilautonomen und autonomen KI-System wichtig, da es durchaus üblich ist, dass solche KI-Systeme Rechtgeschäfte tätigen. Der Begriff der „Autonomie" eines Systems im Sinne einer funktionalen Einheit von Soft- und Hardware wird teilweise als die Fähigkeit beschrieben, Entscheidungen zu treffen und diese in der äußeren Welt, unabhängig von externer Steuerung oder Einflussnahme, umzusetzen.[1015] Autonome Systeme können daher als solche definiert werden, deren Verhalten nicht vollständig vorherbestimmt oder vorhersehbar ist.[1016] So z. B. ein Handelssystem, welches durch einen

[1014] BGH, VersR 1966, 1073, 1974; NJW 1982, 763, 764; 1986, 2501; 1986, 2883, 2884; 1992, 907; 1992, 2474; 1999, 3119; NJW-RR 2006, 813, 814 Rn. 7 = VersR 2006, 416; OLG Koblenz VersR 1999, 239; OLG Karlsruhe, VersR 2014, 1015, 1016.

[1015] Entschließung des Europäischen Parlaments v. 16.02.2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103 [INL]) – P8_TA (2017)0051, Einl. AA. (sub „Haftung"); hierzu *Lohmann*, ZRP 2017, 168, 169.

[1016] Entschließung des Europäischen Parlaments v. 16.02.2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103 [INL]) – P8_TA (2017)0051, Einl. AA. (sub „Haftung"); hierzu *Lohmann*, ZRP 2017, 168, 169.

Algorithmus handelt, Wertpapiere kauft und verkauft.

Interessant ist in diesem Zusammenhang, dass große Software Unternehmen wie SAP sich schon auf Digitale Zugriffe einrichten. Die Firma SAP vertritt die Ansicht, dass eine Nutzung der SAP-Software vorliegt, wenn die Verarbeitungsaktivitäten in dieser Software aktiviert werden. Somit erfordert jede Nutzung der SAP-Software eine entsprechende Lizenz – unabhängig von der Zugriffsmethode. Je nach der Art des Zugriffs, direkt oder indirekt, stellt sich dann die Frage, welche Lizenzvariante einschlägig ist und welche Vergütung damit verbunden ist. So liegt ein indirekter/digitaler Anwenderzugriff vor, wenn Personen oder Dinge die SAP-ERP-Verarbeitungsfähigkeiten aktivieren, ohne einen direkten Nutzerzugriff auf das System zu haben. Das können beispielsweise Drittanwendungen, IoT-Geräte oder Bots sein. Diese Variante fällt in SAPs neuem Lizenzierungsmodell unter „Digital Access" – im Gegensatz zum „Human Access", der nach der Anzahl der menschlichen Nutzer berechnet wird. Der technologische Wandel, angetrieben durch Themen wie das Internet der Dinge, künstliche Intelligenz und Machine Learning sowie Robotics und Bots, hat auch die Zugriffsarten auf die ERP-Systeme verändert. Die indirekte Nutzung der Software hat in den vergangenen Jahren stark zugenommen, inzwischen finden immer mehr digitale Zugriffe auf SAP-Systeme statt. Kunden müssen künftig keine Nutzer mehr zählen, die indirekt auf das SAP-System zugreifen.[1017]

Grundsätzlich kommt ein Vertrag durch zwei übereinstimmende Willenserklärungen zustande. Da eine Willenserklärung die Äußerung eines auf einen Rechtserfolg gerichteten Willen ist, besteht sie sowohl aus einer inneren (subjektiv) als auch einer äußeren (objektiv) Komponente.[1018] Fraglich ist, ob ein KI System auf der Basis eines Algorithmus möglicherweise eine eigene Erklärung insoweit abgibt, dass sie von der dahinterstehenden natürlichen oder juristischen Person nicht mehr im Wege der Zurechnung mitgetragen werden kann.[1019] Eine Willenserklärung besteht aus einem objektiven und einem subjektiven Tatbestand. Wobei der objektive Tatbestand dem äußeren Willen gerichtet ist und der subjektive Tatbestand die innere Seite des Erklärenden widerspiegelt. Der innere Wille umfasst einen Handlungs-, Erklärung- und Geschäftswillen.[1020] Unter dem Handlungswillen

[1017] *Söbbing,* ITRB 2018, 161 bis 163.
[1018] *Medicus*, Bürgerliches Recht. 30. Aufl. 2025, Rn. 45.
[1019] *Pieper,* InTeR 2018, 9 bis 15.
[1020] *Larenz*, Allgemeiner Teil des deutschen Bürgerlichen Rechts, 1960, § 19 I.

versteht man das Bewusstsein zu handeln, also den bewussten Willensakt, der auf die äußere Vornahme eines äußeren Verhaltens gerichtet ist.[1021] Beim Erklärungswillen geht es um das Bewusstsein des Handelnden, dass die Erklärung irgendeine rechtserhebliche Erklärung darstellt. Geschäftswille ist schließlich der Wille, mit der Erklärung eine ganz bestimmte Rechtsfolge herbeizuführen.[1022] Natürlich lassen sich solche Voraussetzungen bei einem KI-Algorithmus nicht erkennen, da ein Algorithmus nur auf der Basis von Logiken agiert.[1023] Nach überwiegender Ansicht kann eine Maschine keine eigene Willenserklärung abgeben.[1024] Nicht das KI-System, sondern die Person (oder das Unternehmen),[1025] die es als Hilfsmittel nutzt, gibt die Erklärung ab oder ist der Empfänger von abgegebenen Erklärungen.[1026] Zudem wird der KI grundsätzlich schon aus philosophischen Gründen kein Bewusstsein zugesprochen (siehe 4.).

Der Aspekt, dass Maschinen scheinbar eine Willenserklärung für einen Menschen abgeben, ist nicht neu, siehe Zigaretten- oder Kartenautomaten. Im Ergebnis muss eine von einer KI abgegebene WE, z. B. basierend auf einem Algorithmus, immer noch als eine sog. automatisierte Willenserklärung verstanden werden. Bei diesen sog. automatisierten Willenserklärungen,[1027] die zwar durch einen Computer formuliert werden (wie z. B. bei Kontoauszügen und Abrechnungen über den Verbrauch von Strom, Wasser oder Heizenergie), ist aber letztlich die automatisierten Willenserklärungen vom Willen des Erklärenden abhängig.[1028] Eine automatisierte Erklärung liegt demnach dann vor, wenn die Willenserklärung vom Computerprogramm aufgrund vorheriger manueller Dateneingabe im Anschluss automatisch erzeugt wird.[1029] Das ist z. B. dann der Fall, wenn in die Software eines Versicherungsunternehmens Daten eingegeben werden und die Software anschließend aufgrund der erhobenen Daten selbsttätig einen Versicherungsschein berechnet und erstellt[1030] oder wenn eine Software aufgrund der eingegebenen Nummer des Buchungsobjekts und des

[1021] Medicus, Bürgerliches Recht. 30. Aufl. 2025, Rn. 45.
[1022] *Brox*, Allgemeiner Teil des BGB, 41. Aufl. 2017, Rn. 83.
[1023] *Pieper,* InTeR 2018, 9 bis 15.
[1024] *Resuch/Weidner,* Future Law, 2018, 14.
[1025] BGH, MMR 2013, 296, 297; *Groß/Gressel,* NZA 2016, 990, 991; *Groß,* InTeR 2018, 4 ,5; *Pieper,* InTeR 2018, 9, 10.
[1026] *Reuch/Weidner,* Future Law, 2018, 14.
[1027] vgl. *Köhler,* AcP 182, 1982, 126; *Clemens,* NJW 1985, 1998; *Brehm,* FS Niederländer, 1991, 233
[1028] BeckOK BGB/*Wendtland,* 47. Ed. 01.08.2018, BGB § 119 Rn. 28, 29.
[1029] *Kitz,* in: Hoeren/Sieber/Holznagel, Teil 13.1 Rn. 37.
[1030] OLG Köln, VersR 2002, 85, 86; OLG Hamm, NJW 1993, 2321, 2321; dazu auch *Köhler*, AcP 182, 1982, 126, 132.

Reisezeitraums den jeweiligen Reisepreis selbstständig ermittelt und ausdruckt.[1031] Derartige automatisierte Willenserklärungen sind als echte Willenserklärungen anerkannt,[1032] wobei die Technologie lediglich als Kommunikationsmittel dient. Der Wille des Erklärenden ergibt sich durch die Erstellung und Anwendung des Algorithmus der KI. Der Nutzer gibt eine Blanketterklärung ab, welche als Computererklärung dem Nutzer zu gerechtet wird. [1033] Dem ist zwar entgegenzuhalten, dass Computererklärungen stärker konkretisiert sind[1034] als bei KI-Systemen, aber hier werden die Fähigkeiten zur Autonomie von KI-Systemen deutlich überschätzt. Sicherlich ist der Algorithmus selbst in der Lage, Daten zu sammeln und darauf eigenständig Entscheidungen zu fällen, aber die Einstellung des Algorithmus erfolgt immer noch durch den Nutzer, was z. B. die Einstellung eines Kreditscores belegt. Somit ist auch das Handeln des KI-Systems dem Nutzer zuzurechnen. Denn das KI-System wird immer nur so autonom handeln können, wie es die Programmierung vorgegeben hat. Auch mögen künstlich intelligente Systeme aus einem Fehlverhalten lernen und dadurch ihr Handeln für die Zukunft optimieren können („künstliche Einsichtsfähigkeit"). So autonom sich die Handlung des Roboters aber darstellt, sie ist nicht Ergebnis eines selbstbestimmten Entschlusses der KI. Dass die KI autonom handelt und die Fähigkeit besitzt, Entscheidungen zu treffen und zu vollziehen, beruht letztlich auf dem Willen des Entwicklers und/oder Anwenders.[1035]

Bei Fehlern des KI-Systems ist zu unterscheiden: Beruht die Fehlerhaftigkeit der computergenerierten Erklärung darauf, dass eine mangels Update nicht mehr aktuelle oder fehlerhafte Software verwendet worden ist, liegt ein unbeachtlicher Motiv- bzw. Kalkulationsirrtum vor, der zur Anfechtung nicht berechtigt.[1036] Dasselbe gilt, wenn die Fehlerhaftigkeit der computergenerierten Erklärung auf zuvor falsch eingegebenem Datenmaterial beruht.[1037] Eine Ausnahme hiervon muss jedoch dann gelten, wenn das fehlerhafte Datenmaterial auf vorsätzlich unrichtigen Angaben des Erklärungsempfängers (z. B. bewusst wahrheitswidrige Angaben in einem Versicherungsantrag) beruht; in solchen Fällen kommt eine

[1031] AG Frankfurt a. M., NJW-RR 1990, 116, 116 f.
[1032] BGH, NJW 2005, 53, 54; BGH, NJW 2005, 976, 977; *Brehm,* in: FS Niederländer, 1991, S. 233, 234.
[1033] *Reuch/Weidner,* Future Law, 2018, 44.
[1034] *Groß/Gressel,* NZA 2016, 990, 991.
[1035] *Günther/Böglmüller*, BB 2017, 53 bis 58.
[1036] *Paal,* JuS 2010, 953, 954 f.
[1037] BGH, NJW 1998, 3192, 3193; LG Frankfurt a. M., NJW-RR 1997, 1273; *Hoeren*, Rechtsfragen des Internet, 1998, Rn. 282; *Köhler,* AcP 182, 1982, 126, 135; *Brehm,* in: FS Niederländer, 1991, S. 233, 241.

Arglistanfechtung nach § 123 BGB in Betracht.[1038] Geht der Fehler auf die Erklärung hingegen auf einen Bedienungsfehler zurück, gilt nichts anderes, als wenn sich der Erklärende verschreibt bzw. vergreift; in diesen Fällen kommt die Annahme eines zur Anfechtung berechtigenden Erklärungsirrtums in Betracht.[1039]

Die Rechtsgeschäftslehre bedarf der Fortentwicklung, um autonome Systeme angemessen einordnen zu können. Auf der Tagung der Zivilrechtslehrervereinigung im September 2017 beklagte Teubner zu Recht, dass die tradierten Vorstellungen der Rechtsgeschäftslehre, die als Urheber einer Willenserklärung ausschließlich natürliche Personen erlaubt, der Realität moderner Techniken wie Industrie 4.0 und autonomer Systeme nicht mehr gerecht werde.[1040] Dennoch wird z. T. in der Literatur vertreten, dass der Tatbestand der Willenserklärung ohne subjektive Elemente in Form eines menschlichen Gedankens auskommt.[1041] Vielfach finden sich aber auch in aktuellen Veröffentlichungen noch traditionelle Beschreibungen eines subjektiven Tatbestands von Willenserklärungen als menschlicher Bewusstseinsgehalt,[1042] der die – im Ergebnis wohl unstreitige[1043] – Anerkennung maschinengenerierter Erklärungen als Willenserklärung nicht recht zu erklären vermag.[1044]

Eine „Computermeinung"[1045] gibt es nach geltendem Recht ebenso wenig wie eine „Maschinenerklärung" als eigenständige rechtsgeschäftliche Willenserklärung.[1046] Gleichwohl: Je selbständiger das System handelt und je mehr Umweltfaktoren bei der Generierung des objektiven Erklärungstatbestands einbezogen werden, desto allgemeiner und unpräziser wird die Vorstellung des Nutzers von der letztlichen Erklärung sein.[1047] Fraglich ist dann,

[1038] *Köhler,* AcP 182, 1982, 126, 135.

[1039] *Brehm,* in: FS Niederländer, 1991, S. 233, 240; einschr. *Köhler,* AcP 182, 1982, 126, 136.

[1040] *Borges*, NJW 2018, 977.

[1041] *Wiebe*, Die elektronische Willenserklärung, 2002, S. 214 ff. (Zurechnung der Erklärung nach „Risikoprinzip" aufgrund Beherrschens der Maschine); *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, S. 104; in diese Richtung schon *Brehmer*, Wille und Erklärung, 1992, S. 29, 80 f.

[1042] *Faust*, BGB AT, 6. Aufl. 2018, § 2 Rn. 4; *Grigoleit/Herresthal*, BGB AT, 3. Aufl. 2015, Rn. 6; *Leipold*, BGB I, Einführung und AT, 9. Aufl. 2017, § 10 Rn. 17.

[1043] S. im Überblick hierzu *Borges/Sesing,* in: Matusche-Beckmann, Saar-Tage 2016: Rechtsprobleme der Informationsgesellschaft, 2018 (iErsch.), 177, 187.

[1044] *Borges*, NJW 2018, 977.

[1045] *Weichert*, ZRP 2014, 168, 170.

[1046] Vgl. hierzu BGH, 16.10.2012 - X ZR 37/12, BGHZ 195, 126, 131; *Klein*, in: Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, 2015, S. 429, 436. Letztlich räumt dies auch Weichert, ZRP 2014, 168, 171 ein, indem er konkludiert, dass "klar sein [muss], dass Algorithmen nur so gut sein können, wie sie programmiert wurden".

[1047] *Klein*, DSRITB 2015, 429, 438.

ob noch ein Geschäftswillen angenommen werden kann, weil der Nutzer nur eine schemenhafte Vorstellung von der letztlich generierten objektiven Erklärung hat. In diesem Fall findet keine Zurechnung, sondern vielmehr eine Fiktion des Geschäftswillens statt.[1048] Dies gilt erst recht, wenn Maschinen zunehmend autark untereinander kommunizieren, wie beispielsweise im Anwendungsbereich von Industrie 4.0. Das deutsche Zivilrecht stammt größtenteils aus dem Jahr 1900 und geht davon aus, dass Willenserklärungen auf menschlichen Entscheidungen beruhen, also der Handelnde nicht nur die Folgen seiner rechtsgeschäftlichen Erklärungen verstehen kann, sondern auch ein Mindestmaß an Einsichts- und Urteilsfähigkeit besitzt.[1049] Wenn im letzten Autonomiestadium eines intelligenten Systems ein Mensch über durchgeführte Aktionen weder informiert wird noch ihm getroffene Entscheidungen im Nachgang zugänglich gemacht werden, ändert dies die Wertungen im Bereich des Geschäftswillens derart, dass eine Zurechnung nur noch schwer haltbar ist.

Ferner können sich aufgrund der fortgeschrittenen Intelligenz und Autonomie Fragen der Wirksamkeit von Willenserklärungen stellen, insbesondere im Rahmen von deren Abgabe und beim Zugang. Als Beispiel kann hier die Wirksamkeit gegenüber Abwesenden dienen. Dies ist im Bereich der "Machine-to-Machine-Kommunikation", auch M2M-Kommunikation genannt (z. B. im Bereich von Industrie 4.0 oder dem Beispiel, dass ein System eigenständig die zur Neige gehende „Milch im Kühlschrank" bestellt), relevant. § 130 Abs. 1 BGB bestimmt insoweit: „Eine Willenserklärung, die einem anderen gegenüber abzugeben ist, wird, wenn sie in dessen Abwesenheit abgegeben wird, in dem Zeitpunkt wirksam, in welchem sie ihm zugeht." Zugegangen ist die Erklärung dann, wenn sie dergestalt in den Machtbereich oder die tatsächliche Verfügungsgewalt des Empfängers gelangt ist, dass es nur noch an ihm liegt, von ihr Kenntnis zu nehmen und mit seiner Kenntnisnahme unter normalen Umständen gerechnet werden kann.[1050] Die Bestimmung folgt damit der so genannten „Empfangstheorie", nach der die Gefahr der Zielverfehlung einer abgegebenen Willenserklärung angemessen zwischen Erklärendem und Empfänger verteilt wird: Der Erklärende hat alles Erforderliche zu unternehmen, um die empfangsbedürftige Erklärung in den Machtbereich des Empfängers zu verbringen. Bis dahin trägt er das Risiko des Verlusts bzw. des Fehlgehens oder der Rechtzeitigkeit der Erklärung. Das Risiko der (rechtzeitigen)

[1048] *Klein*, DSRITB 2015, 429, 438.
[1049] *Wulf/Burgenmeister*, CR 2015, 404, 406.
[1050] BGH, 21.06.2011 – II ZB 15/10 = NJW-RR 2011, 1184, 1185.

Kenntnisnahme der in seinen Einflussbereich gelangten Willenserklärung trägt hingegen allein der Empfänger, da der Erklärende hierauf ab Zugang keinerlei Einwirkungsmöglichkeit mehr hat.[1051] Auf Hindernisse in seinem Bereich, die der Kenntnisnahme entgegenstehen, kann sich der Empfänger mithin nicht berufen, da er diesen durch geeignete Maßnahmen entgegenwirken kann und muss.[1052] Hieran ändert grundsätzlich auch nichts, wenn der Empfänger zur Entgegennahme von Erklärungen bereitgehaltene Empfangseinrichtungen nutzt, wie beispielsweise Fax oder E-Mail.[1053] Dies gilt sogar allgemein für die Speicherung in Form von Binärdaten, wie dies bei elektronischen Medien oder Softwaresteuerungsprogrammen der Fall ist.[1054]

Hieran wird sehr deutlich, dass nach der Empfangstheorie die Gefahr der Zielverfehlung einer abgegebenen Willenserklärung angemessen zwischen Erklärendem und Empfänger verteilt wird. Die beiden „Sphären" werden klar voneinander abgegrenzt und so wird eine eindeutige Zuordnung der Verantwortlichkeit sowohl auf Seiten des Erklärenden wie auch des Empfängers erreicht. Unter diesen Voraussetzungen macht es keinen Unterschied, wie weit ein etwaig beim Zugang einer Willenserklärung eingesetztes intelligentes System technisch fortgeschritten ist, weil es jederzeit der Sphäre des Empfängers zugerechnet werden kann.[1055]

Es handelt sich hierbei lediglich um zwei spezifische Anwendungsbeispiele. Sie verdeutlichen jedoch anschaulich, dass bei Einsatz von intelligenten Systemen ganz unterschiedliche Ergebnisse in der rechtlichen Bewertung entstehen können, wenn man die zunehmende Intelligenz und Lernfähigkeit autonomer Systeme berücksichtigt. Die Entwicklung ist hier gerade im vollen Gange und es ist noch nicht absehbar, wie sich derlei Systeme in Zukunft verbreiten und vor allem verhalten werden. Gleichwohl empfiehlt es sich bereits jetzt, rechtlich angemessene Wertungen zu treffen, die die technische Entwicklung ordnungsgemäß begleiten.

[1051] *Wendtland*, in: Bamberger/Roth (Hrsg.), BeckOK BGB, 42. Edition Stand: 01.02.2017, § 130 Rn. 10.
[1052] BGH, 21.01.2004 – XII ZR 214/00 = NJW 2004, 1320, 1320 f.
[1053] *Wendtland*, in: Bamberger/Roth, 4. Aufl. 2018, § 130 Rn. 12.
[1054] *Wendtland*, in: Bamberger/Roth, 4. Aufl. 2018, § 130 Rn. 12; *Wendtland*, in: Bamberger/Roth, 4. Aufl. 2018, § 126b Rn. 2.
[1055] *Pieper,* InTeR 2018, 9 bis 15.

IV. KI als Erfüllungsgehilfe

Die Frage nach der Hersteller- oder Betreiberhaftung verliert an Bedeutung, wenn ein Fehlverhalten der KI im Bereich der vertraglichen Haftung über § 278 BGB dem Betreiber zuzurechnen wäre. Eine solche Zurechnung ist jedoch abzulehnen.[1056] Die Zurechnungsnorm setzt ein eigenes Verschulden des Erfüllungsgehilfen voraus. Mit einer sehr extensiven Gesetzesauslegung ließe sich ein autonomes System möglicherweise noch als Erfüllungsgehilfe einordnen, jedoch stößt man beim Erfordernis des eigenen Verschuldens bei einer Maschine nach derzeitigem Gesetzeswortlaut an Auslegungsgrenzen. Verschulden setzt nach allgemeinem Verständnis eine willentliche Steuerung eigenen Handelns voraus.[1057]

Intelligentes Handeln einer KI ist immer auf eine entsprechende Entwicklung des Algorithmus zurückzuführen. Das KI-System wird immer nur so autonom handeln können, wie es die Programmierung vorgegeben hat. Auch mögen künstlich intelligente Systeme aus einem Fehlverhalten lernen und dadurch ihr Handeln für die Zukunft optimieren können ("künstliche Einsichtsfähigkeit"). So autonom sich die Handlung des Roboters aber darstellt, sie ist nicht Ergebnis eines selbstbestimmten Entschlusses der KI. Dass die KI autonom handelt und die Fähigkeit besitzt, Entscheidungen zu treffen und zu vollziehen, beruht letztlich auf dem Willen des Entwicklers und/oder Anwenders.[1058]

V. Kreditgefährdung

Ein Sonderfall der Haftung für falsche Daten ergibt sich aus der Kreditgefährdung gem. § 824 BGB.[1059] Wer gem. § 824 Abs. 1 BGB der Wahrheit zuwider eine Tatsache behauptet oder verbreitet, die geeignet ist, den Kredit eines anderen zu gefährden oder sonstige Nachteile für dessen Erwerb oder Fortkommen herbeizuführen, hat dem anderen den daraus entstehenden Schaden auch dann zu ersetzen, wenn er die Unwahrheit zwar nicht kennt, aber kennen muss. Denkbar wäre, dass ein KI-Algorithmus (Score) falsche Bonitätsdaten produziert und das Kreditbüro dem Kreditinstitut einen anhand von gespeicherten (personenbezogenen) Daten ermittelten Scorewert als Einzeldatum zur Bonitätsbeurteilung

[1056] *Günther/Böglmüller*, BB 2017, 53 bis 58.
[1057] *Spindler*, in: BeckOK BGB, 40. Ed., Stand: 01.05.2016, § 827 BGB Rn. 1.
[1058] *Günther/Böglmüller*, BB 2017, 53 bis 58.
[1059] *Kirchner*, InTeR 2018, 59 bis 63.

übermittelt. Ein solcher Scorewert ist im Gegensatz zu den Ausgangsdaten selbst[1060] nicht mit Beweismitteln auf seine Richtigkeit hin überprüfbar,[1061] so dass es sich um eine bloße Meinungsäußerung handelt, die insofern im Allgemeinen grundsätzlich keine Schadensersatzansprüche auslöst, sofern die zugrunde liegenden Tatsachen zutreffend sind.[1062] Daran ändert sich auch nichts, wenn der Score (KI-Algorithmus) den Bonitätswert ermittelt hat und nicht ein Mensch.[1063] Es darf dabei nicht unterschätzt werden, dass die Einstellung des Scores von Menschen (Entwickler/Programmierer) vorgenommen wird.[1064] Eine „Computermeinung"[1065] gibt es nach geltendem Recht ebenso wenig wie eine „Maschinenerklärung" als eigenständige rechtsgeschäftliche Willenserklärung.[1066]

Der Art. 5 Abs. 1 S. 1, Alt. 1 GG schützt die Meinungsfreiheit. Die Meinungsfreiheit findet gem. Art. 5 Abs. 2 GG ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre. Als allgemeines Gesetz kann dabei die Vorschrift in § 824 BGB verstanden werden.[1067] Werden darüber hinausgehend auch Aussagen, in denen sich Tatsachen und die Aussage prägende Meinungen untrennbar[1068] vermengen, droht eine Verkürzung des grundrechtlichen Schutzbereiches.[1069] Unzulässig dürfte demnach auch eine Anknüpfung an eine (fingierte) implizite Tatsachenbehauptung des ordnungsgemäßen Erstellens des Ratings/der Bonitätsbewertung sein, auch wenn sich diese inhaltlich abtrennen ließe.[1070] Somit kann der § 824 BGB daher in diesen Fällen keine Anwendung finden, so dass letztlich für den Anwendungsbereich des § 824 BGB nur die Lieferung unzutreffender (personenbezogener) Tatsachenbehauptungen/Daten durch den KI-Anwender verbleibt, sofern

[1060] Missverständlich deshalb *Hoeren*, MMR 2016, 8, 10, der eine Klassifizierung als richtiges/falsches Datum ablehnt, damit an dieser Stelle aber wohl nur auf die Score-/Wahrscheinlichkeitswerte Bezug nimmt und auf S. 11 letztlich selbst von unrichtigen zugrunde liegenden Daten spricht.

[1061] BGH, 22.02.2011 – VI ZR 120/10, NJW 2011, 2204, 2205.

[1062] BGH, 22.02.2011 – VI ZR 120/10, NJW 2011, 2204, 2205; vgl. auch BGH, 28.06.1994 - VI ZR 252/93, NJW 1994, 2614, 2615 – zu § 824 BGB.

[1063] So aber *Weichert*, ZRP 2014, 168, insbes. 168, 171.

[1064] *Milstein/Lippold*, NVwZ 2013, 182, 184 f.

[1065] *Weichert*, ZRP 2014, 168, 170.

[1066] Vgl. hierzu BGH, 16.10.2012 – X ZR 37/12, BGHZ 195, 126, 131; *Klein*, in: Taeger (Hrsg.), Internet der Dinge – Digitalisierung von Wirtschaft und Gesellschaft, 2015, S. 429, 436. Letztlich räumt dies auch Weichert, ZRP 2014, 168, 171 ein, indem er konkludiert, dass "klar sein [muss], dass Algorithmen nur so gut sein können, wie sie programmiert wurden".

[1067] Vgl. BVerfG, 15.01.1958 - 1 BvR 400/57, BVerfGE 7, 198 ff. - § 826 BGB; OLG München, 12.03.2014 - 15 U 2395/13, ZD 2014, 570, 572.

[1068] BVerfG, 09.10.1991 – 1 BvR 1555/88, BVerfGE 85, 1, 15 = NJW 1992, 1439, 1440.

[1069] BVerfG, 22.06.1982 – 1 BvR 1376/79, BVerfGE 61, 1, 8 f. = NJW 1983, 1415, 1416.

[1070] A. A. *Oellinger*, in: Achleitner/Everling (Hrsg.), Rechtsfragen im Rating, 2005, S. 360.

diese dazu geeignet sind, beispielsweise den Kredit des Betroffenen zu gefährden.[1071]

Fraglich ist, ob § 824 BGB bei der Kreditgefährdung abschließend ist. Dies ist grundsätzlich zu bejahen, aber mit dem deutlichen Hinweis, dass sich der § 824 BGB nur auf die Verbreitung falscher Tatsachen bezieht. Eine weitergehende Haftung lässt sich nur über §§ 823 Abs. 1, 2, 826 BGB bewerkstelligen.[1072] Da beide Normen ein Verschulden voraussetzen, ist bei der Frage der Fahrlässigkeit i. S. v. § 278 Abs. 1 BGB die Frage nach der Qualität des Scores und seiner Berechnungen zu klären.[1073] Eine „unzutreffende" Bonitätsauskunft/Meinungsäußerung als solche kann es streng genommen nicht geben, so dass die Bezeichnung regelmäßig nur darauf hindeuten kann, dass die Bonitätsauskunft auf einer unzutreffenden Tatsachengrundlage fußt.[1074] Dies wäre richtig, wenn man unterstellt, dass ein Score niemals fehlerhaft programmiert oder eingestellt worden ist, was eindeutig nicht der Fall ist. Falsche Bonitätsauskünfte, die auf einen unzutreffenden Tatsachenkern beruhen, werden als Meinungsäußerung nicht zu einer (unwahren) Tatsachenbehauptung.[1075]

VI. KI mit eigener Rechtspersönlichkeit

Was zunächst als Science-Fiction klingt, wird rechtlich bereits diskutiert: Kann man KI eine Art von beschränkter Rechtssubjektivität einräumen, um Probleme von Schuld, Haftung und Verantwortung zu lösen?[1076]

Stanley Kubricks vernunftbegabter Supercomputer HAL 9000 im Film 2001 – „Odyssee im Weltraum" will die Kontrolle über die anstehende Raumfahrtmission nicht den unzulänglichen menschlichen Astronauten überlassen, die planen, ihn abzuschalten.[1077] In zahllosen utopischen wie dystopischen narrativen Science-Fiction- und Zukunftsszenarien ist die Thematik vernunftbegabter Roboter oder Computer behandelt worden, so dass die potenzielle Möglichkeit der Erschaffung „künstlicher Intelligenz" („K.I.") quasi zum selbstverständlichen Teil unserer Kultur geworden ist.[1078] Basis einer möglichen beschränkten

---

[1071] *Kirchner*, InTeR 2018, 59 bis 63.

[1072] BGH, 24.01.2006 – XI ZR 384/03, NJW 2006, 830, 839 m. w. N. – wahre Tatsachen und Werturteile/Meinungen.

[1073] OLG Hamm, 18.04.2012 – I-13 U 174/11, BeckRS 2012, 14962.

[1074] BGH, 22.02.2011 – VI ZR 120/10, NJW 2011, 2204, 2206; *Reiter/Methner*, in: Taeger (Hrsg.), Smart World - Smart Law?, 2016, S. 453, 458; a. A. wohl *Berger/Stemper*, WM 2010, 2289, 2294 zum "fehlerhaften Rating".

[1075] Vgl. *Schulte*, NJW 2014, 1238, 1238; BGH, 22.02.2011 - VI ZR 120/10, NJW 2011, 2204, 2205; OLG Frankfurt a. M., 07.04.2015 - 24 U 82/14, NJOZ 2015, 1913 ff.; OLG München, 09.09.2014 - 18 U 516/14, NJW-RR 2015, 422, 428 f.; ebenso OLG München, 28.10.2014 – 18 U 1022/14 Pre, MMR 2015, 410 ff.

[1076] *Hilgendorf*, in: Beck (Hrsg.), Jenseits von Mensch und Maschine, 2012, S. 119, 125 ff.; *Beck*, JR 2009, 225, 229 f.; dem beipflichtend *Kersten*, JZ 2015, 1, 7.

[1077] 2001 – Odyssee im Weltraum (1968).

[1078] *Lewke*, InTeR 2017, 207 bis 216.

Rechtssubjektivität könnte eine beschränkte Geschäftsfähigkeit oder eine Stellvertretung sein. Damit könnten sich ggf. Zurechnungsprobleme mit Hilfe einer Prozessstandschaft beim Rechtsschutz von KI bewerkstelligen lassen,[1079] nämlich die Haftung über einen Fonds oder ein Pflichtversicherungssystem zu lösen.[1080]

Die zentrale Frage ist dabei die nach der Art der Softwarenutzung. Die Firma SAP vertritt die Ansicht, dass eine Nutzung der SAP-Software vorliegt, wenn die Verarbeitungsaktivitäten in dieser Software aktiviert werden. Somit erfordert jede Nutzung der SAP-Software eine entsprechende Lizenz – unabhängig von der Zugriffsmethode. Je nach der Art des Zugriffs, direkt oder indirekt, stellt sich dann die Frage, welche Lizenzvariante einschlägig ist und welche Vergütung damit verbunden ist. So liegt ein indirekter/digitaler Anwenderzugriff vor, wenn Personen oder Dinge die SAP-ERP-Verarbeitungsfähigkeiten aktivieren, ohne einen direkten Nutzerzugriff auf das System zu haben. Das können beispielsweise Drittanwendungen, IoT-Geräte oder Bots sein. Diese Variante fällt in SAPs neuem Lizenzierungsmodell unter „Digital Access" – im Gegensatz zum „Human Access", der nach der Anzahl der menschlichen Nutzer berechnet wird. Der technologische Wandel, angetrieben durch Themen wie das Internet der Dinge, künstliche Intelligenz und Machine Learning sowie Robotics und Bots, hat auch die Zugriffsarten auf die ERP-Systeme verändert. Die indirekte Nutzung der Software hat in den vergangenen Jahren stark zugenommen, inzwischen finden immer mehr digitale Zugriffe auf SAP-Systeme statt. Kunden müssen künftig keine Nutzer mehr zählen, die indirekt auf das SAP-System zugreifen. Das neue Modell greift SAP zufolge beim aktuellen SAP-Kern S/4HANA sowie S/4HANA Cloud wie auch beim Vorgänger-ERP ECC 6.0

Entwicklung und Einsatz autonomer Systeme, dies ist jetzt schon absehbar, werden zu weit stärkeren Änderungen des rechtlichen Rahmens führen.[1081] Im Personenrecht kreist die Diskussion – unter anderem in einer Arbeitsgruppe des Europäischen Parlaments[1082] – um

[1079] *Kersten*, JZ 2015, 1, 7 unter Verweis auf *Mainzer*, Leben als Maschine?, 2010, S. 240, 243; für die §§ 164 ff. BGB *Gruber,* in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 123, 198.

[1080] S. *Beck*, in: Spranger (Hrsg.), Aktuelle Herausforderungen der Life Sciences, 2010, S. 95, 102 ff.; *Hilgendorf*, in: Beck (Hrsg.), Jenseits von Mensch und Maschine, 2012, S. 119, 125 ff., 128; *Gruber*, in Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 123, 156, 198; mit Einschränkungen auch *Bodungen/Hoffmann*, NZV 2015, 521, 524 ff.

[1081] *Borges*, NJW 2018, 977.

[1082] www.europarl.europa.eu/committees/de/juri/subject-files.html?id=20150504CDT00301, zuletzt abgerufen am 27.07.2018.

die Anerkennung einer „E-Person“ neben den existierenden juristischen Personen.[1083] Die wachsende Autonomie von Robotern und Softwareagenten, deren Reaktionen nicht mehr vom Programmierer vorhersehbar sind, sondern wesentlich durch intelligentes Lern- und Kommunikationsverhalten bestimmt werden, könnte sowohl Rechtspersönlichkeit als auch die Ausstattung mit einem eigenen Haftungsfonds erforderlich machen.[1084] Die Alternative sind neue Tatbestände der Gefährdungshaftung und passgenaue Versicherungslösungen. Das Aufkommen neuer Technologien hat auch die alte Frage nach der Haftung für deren Fehlfunktionen neu entfacht, und zwar sowohl im vertraglichen Bereich, wo schon lange die Anwendung der Vorschriften über Erfüllungsgehilfen oder die Einführung neuer Zurechnungsnormen diskutiert werden,[1085] als auch im deliktischen Bereich, wo es gleichfalls um neue Zurechnungsmodelle oder aber um neue Tatbestände der Gefährdungshaftung ähnlich der Tierhalterhaftung geht.[1086] Besondere Aufmerksamkeit wird dabei der Haftung und Versicherung rund um selbstfahrende Autos geschenkt.[1087]

Die Diskussion, ob KI autonom handeln und über eine eigene Rechtsfähigkeit analog zu § 1 BGB verfügen oder nicht, erscheint angesichts der technischen Möglichkeiten noch zu verfrüht. Dennoch kann man KI, sofern die jeweilige KI technisch dazu in der Lage ist, eine gewisse Teilautonomie nicht absprechen. Diese Teilautonomie entbindet aber weder den KI-Hersteller von seiner Produkthaftung noch den Betreiber der KI von seiner Betreiberhaftung. Der Hersteller muss technische Vorkehrungen (siehe hierzu den „Super Code“) entwickeln, die das Risiko, die von KI ausgehen, minimieren. Diese technischen Vorkehrungen müssen auch für den Lernprozess der KI gelten. Der Betreiber/Inhaber kann sich bei dem Betrieb der KI nicht allein auf den Hersteller verlassen, sondern muss einige Schutzmechanismen in z. B. der Form des „Super Code“ finden.

Bereits schon einmal stand die Menschheit vor der Frage, wem sie eine Rechtspersönlichkeit zugesteht. Nach dem Vertrag von Madrid von 1750 hatten Spanien und Portugal vereinbart, dass das Gebiet östlich des Río Uruguay an Portugal fallen sollte. 1752 wurde der

---

[1083] *Wendehorst*, NJW 2016, 2609.

[1084] Vgl. unter anderem *Schweighofer,* in: Schweighofer/Menzel/Kreuzbauer, Auf dem Weg zur ePerson, 2001, S. 45, 49 ff.; *Wettig/Zehendner*, AI Law 12, 2004, 111, 127 ff.; S. *Beck*, JR 2009, 225, 229 f.; *Hilgendorf*, Jenseits von Mensch und Maschine, 2012, S. 119, 125 ff.; *Kersten*, JZ 2015, 1, 6 f.

[1085] Zur älteren Diskussion *Spiro*, Die Haftung für Erfüllungsgehilfen, 1984, S. 209 ff.; *Möschel*, AcP 186, 1986, 187, 197 ff.; *Koziol*, ÖBA 1987, 3; zur neueren *Müller-Hengstenberg/Kirn*, MMR 2014, 307, 311; *Wulf/Burgenmeister*, CR 2015, 404, 407; *Horner/Kaulartz*, CR 2016, 7.

[1086] *Spindler*, CR 2015, 766, 775; *Bräutigam/Klindt*, NJW 2015, 1137, 1139 m. w. N.

[1087] Statt vieler *Schulte-Nölke*, Karlsruher Forum 2015, 3 ff. m. w. N.

päpstliche Gesandte Luis Altamirano nach Paraguay entsandt, um die Übergabe dieses Gebietes zu überwachen. Dabei hatte er auch die Frage zu beantworten, ob die Ureinwohner, die „Guaranis", die in diesem Gebiet wie in einem Reservat lebten, Menschen oder Tiere sind. Diese Beurteilung war in der Hinsicht wichtig, denn wenn Guaranis Tiere sind, so würden sie nicht unter den göttlichen Schutz fallen und könnten somit von spanischen und portugiesischen Abenteurern, den Entradas und Bandeiras, versklavt und ausgebeutet werden. Die Jesuiten, unter deren Schutz die Guaranis standen, versuchten den Beweis zu erbringen, dass Guaranis Menschen sind, indem sie Guaranis ihren wundervollen Gesang Altamirano vortrugen ließen. Die Entradas und Bandeiras, die eher wirtschaftliche Interessen hatten, verglichen die Guaranis mit Papageien und Affen, die bestimmte menschliche Handlungen imitieren. Luis Altamirano entschied auf erheblichen Druck aus Spanien und Portugal, dass die Guaranis keine Menschen sind. Dies führte zum Guarani-Krieg von 1754 bis 1756, der mit dem Tod von 1511 Guaraní und 4 toten Portugiesen endete sowie der anschließenden Versklavung der Guaranis. Luis Altamirano beschrieb in seinem Bericht an den Papst diese schreckliche Geschichte und bezeichnete sich dabei selbst als Tod, da er mit dem Folgen seiner Entscheidung nicht leben konnte. Auch Asimov hat sich in seinen Roman „Der Zweihundertjährige" mit der Frage beschäftigt, wann einer KI (z. B. in der Form eines Roboters) eine eigene Rechtspersönlichkeit zugestanden werden kann. In dem Roman wurde die Rechtspersönlichkeit zunächst verneint, weil der Roboter nicht altern konnte. Woraufhin der Roboter seinen Körper so verändert, dass ein natürliches Altern einsetzt und er im Alter von 200 Jahren stirbt, wenige Sekunden bevor das Weltparlament seine Menschlichkeit anerkennt.[1088]

Bis zur grundsätzlichen Erschaffung einer Superintelligenz ist aber über eine eigene Rechtspersönlichkeit für KI nicht zu diskutieren, da dies den heutigen technischen Standards nicht entspricht. Dies folgt aus der mangelnden Fähigkeit eines KI-Systems, de lege lata Träger von Rechten zu sein.[1089] Eine solche Diskussion zu gegenwärtigem Zeitpunkt, die sicherlich mehr philosophisch als rechtlich geführt wird, würde im Ergebnis dazu führen, dass sich Hersteller und Betreiber von der Haftung freimachen könnten. Zudem verfügt ein KI-

[1088] *Asimov,* Der Zweihundertjährige, 1978, (The Bicentennial Man And Other Stories, 1976).
[1089] Vgl. *Mayinger*, Die künstliche Person, 2017, S. 178.; *Lewke*, InTeR 2017, 207 bis 216.

System selbst nicht über eine Liquidität, um die Ansprüche des Geschädigten zu erfüllen und somit würde eine eigene Rechtspersönlichkeit für KI lediglich den Geschädigten schaden. Diese Ansicht könnte sich dank technologischer Singularität (siehe Kapitel C. 1d)[1090] schneller ändern als gedacht, denn durch die sich selbst verbessernden KI (Seed AI) kann der technische Fortschritt rasant beschleunigt werden. Derzeit ist aber nicht daran zu denken.

Auch wenn Roboter menschenähnliche Gestalt annehmen und KI intelligent handeln, können sie nicht selbst für einen verursachten Schaden in Anspruch genommen werden. Autonome Systeme sind nach derzeitiger Gesetzeslage keine Rechtssubjekte und besitzen keine eigene Rechtspersönlichkeit.[1091]

I. Embedded Law in künstlicher Intelligenz

Während der Artificial Intelligence-Act (KI-VO) der EU-Kommission mit mehr Bürokratie versucht, die Angst vor künstlicher Intelligenz (KI) zu reduzieren (vgl. Art. 8 KI-VO ff.), stellt sich die Frage, ob es eine mehr konstruktive Methode geben kann, die in der Lage ist, KI sicherer zu machen. Wie wäre es, als Lösung der KI ein Gewissen zu verschaffen? Was auf dem ersten Blick wie eine philosophische Theorie klingt, ist eine sehr ernst gemeinte praktische Anwendung. Denn mittels eines Filters durch ein sogenanntes „Embedded Law" werden Halluzinationen und falsche Ergebnisse einer KI herausgefiltert, wenn diese Ergebnisse gegen geltendes Recht verstoßen. Somit können teure Haftungsfälle vermieden werden. Ein solcher Filter wäre ein sogenannter „Super Code", gegen den Output der KI niemals verstoßen darf.

I. Einleitung

Ein großes Thema in der KI-Entwicklung ist, dass die KI zu Ergebnissen kommt, die logisch richtig sind, aber aus Sicht des Menschen katastrophal falsch sind. Bekannt ist dieses Phänomen unter den Begriff der „Halluzination". Die Ursachen für Halluzinationen von KI sind vielschichtig und haben sowohl technische als auch methodische Gründe. Halluzinationen in KI-Modellen entstehen durch eine Kombination aus den

[1090] Unter technologischer Singularität werden verschiedene Theorien in der Zukunftsforschung zusammengefasst. Überwiegend wird darunter ein Zeitpunkt verstanden, bei dem sich Maschinen mittels künstlicher Intelligenz (KI) rasant selbst verbessern (Seed AI) und damit den technischen Fortschritt derart beschleunigen, dass die Zukunft der Menschheit hinter diesem Ereignis nicht mehr vorhersehbar ist. Quelle Wikipedia.

[1091] *Bräutigam/Klindt*, NJW 2015, 1137; *Cornelius*, MMR 2002, 353, 354; *Horner/Kaulartz*, InTeR 2016, 22, 24.

Beschränkungen probabilistischer Methoden, unvollständigen oder fehlerhaften Trainingsdaten, der fehlenden Fähigkeit zur dynamischen Faktenprüfung und dem grundsätzlichen Mangel an Verständnis von Bedeutung und Kontext. Die Forschung in der KI-Entwicklung zielt darauf ab, diese Probleme zu minimieren, etwa durch die Integration besserer Datensätze, Fact-Checking-Mechanismen und fortschrittlicherer Modellarchitekturen.

In der KI-Forschung bezieht sich der Begriff „Halluzination" auf Situationen, in denen ein Modell Informationen erzeugt, die nicht auf den tatsächlichen Daten oder Fakten basieren. Diese ungenauen oder irreführenden Ausgaben können auf verschiedene Faktoren zurückgeführt werden:

- **Unvollständige oder fehlerhafte Trainingsdaten**: KI-Modelle, insbesondere Sprachmodelle wie GPT, werden auf großen Datensätzen trainiert, die aus dem Internet und anderen Textquellen stammen. Wenn diese Daten unvollständig, widersprüchlich oder fehlerhaft sind, kann das Modell falsche Informationen lernen. Diese Inkonsistenzen in den Trainingsdaten führen dazu, dass die KI auf Grundlage von falschen oder ungenauen Informationen „halluziniert".

- **Probabilistischer Ansatz der Modelle**: Sprachmodelle basieren auf Wahrscheinlichkeiten. Sie erzeugen Vorhersagen, indem sie die wahrscheinlichste **nächste** Wortsequenz basierend auf dem vorherigen Kontext auswählen. Dieser Ansatz bedeutet, dass sie keine sicheren Aussagen treffen, sondern immer versuchen, die wahrscheinlichste Fortsetzung eines Textes zu generieren. Dadurch können sie neue Informationen erfinden, wenn die Wahrscheinlichkeiten dies nahelegen, auch wenn diese Informationen faktisch nicht korrekt sind.

- **Fehlendes Verständnis und Weltwissen**: KI-Modelle haben kein echtes Verständnis von Informationen. Sie sind nicht in der Lage, wie Menschen Fakten von Fiktion zu unterscheiden, sondern verarbeiten lediglich statistische Muster in den Trainingsdaten. Wenn diese Muster unklar oder widersprüchlich sind, kann dies zu erfundenen oder falschen Inhalten führen. Modelle können keine externe

Überprüfung von Fakten durchführen und erzeugen daher manchmal plausibel klingende, aber falsche Antworten.

- **Überanpassung („Overfitting“)**: Bei einer Überanpassung lernt das Modell nicht nur allgemeine Muster, sondern auch spezifische, oft irrelevante Details aus den Trainingsdaten. Dies kann dazu führen, dass das Modell in bestimmten Situationen falsche oder unsinnige Antworten gibt, da es auf Muster zurückgreift, die im Kontext der Anfrage nicht zutreffend sind.

- **Mangel an explizitem Faktenwissen**: Sprachmodelle verfügen über keine expliziten Faktenbanken, sondern arbeiten rein auf Grundlage der Textdaten, auf denen sie trainiert wurden. Wenn das Modell mit einer Frage konfrontiert wird, zu der es keine klaren oder relevanten Trainingsdaten hat, neigt es dazu, basierend auf anderen Informationen, eine Antwort zu halluzinieren. Dies führt zu fehlerhaften oder fiktiven Ausgaben.

- **Komplexität natürlicher Sprache**: Die natürliche Sprache ist vieldeutig und komplex, was es schwierig macht, immer eine genaue Antwort zu generieren. In vielen Fällen gibt es keine eindeutig richtige Antwort und das Modell muss mehrere potenzielle Möglichkeiten berücksichtigen. Dies kann zu Aussagen führen, die zwar sprachlich kohärent sind, aber faktisch falsch.

- **Fehlende Fähigkeit zur dynamischen Überprüfung von Fakten**: KI-Modelle, wie GPT, haben nach dem Training keinen Zugang zu externen Wissensquellen (z. B. aktuelle Datenbanken oder das Internet), um ihre Antworten zu überprüfen. Sie sind auf das Wissen beschränkt, das sie während des Trainings erworben haben. Dies bedeutet, dass sie veraltete oder ungenaue Informationen wiedergeben können, ohne sie in Echtzeit zu überprüfen.[1092]

[1092] Ausführlich hat sich Katharina Zweig in ihrem Buch „Die KI war's! Von absurd bis tödlich: Die Tücken der künstlichen Intelli genz“ damit beschäftigt.

Die Beispiele in den folgenden Absätzen soll aufzeigen zu welchen katastrophalen Folgen Halluzination führen können und wie mittels eines Filters der ein Embedded Law enthält dieses Risiko minimiert wird.

II. Praktisches Beispiel HR-Prozess

Es mag ein wenig ungewöhnlich klingen, aber bereits heute wird im Human-Resources-Recruiting-Prozess künstliche Intelligenz eingesetzt.[1093] So bietet die ständige Verfügbarkeit von Chatbots im Recruiting einen großen Anwendungsbereich, da Jobinteressierte sich meist außerhalb der Arbeitszeiten der HR-Abteilung bewerben.[1094] Da die ganzen Bewerbungen jedoch erst am darauffolgenden Werktag gesichtet werden können, staut sich einiges an Bewerbungen bei den Recruitern an. Der schleppende Prozess von der Sichtung hin bis zur Rückmeldung kann sich negativ auf das Unternehmen auswirken und es wichtige potenzielle Bewerbende kosten. Etwa die Hälfte aller Bewerbenden hat den Bewerbungsprozess schon einmal vorab beendet, trotz bestehenden Interesses an der Stelle, da ihnen die Wartezeit zu lange gedauert hat.[1095]

Der Einsatz von Chatbots kann dabei helfen, Prozesse schneller abzuwickeln und den Bewerbungsprozess attraktiver zu gestalten. Ein Chatbot (oder kurz Bot) ist ein auf Algorithmen und KI basierendes Computerprogramm, welches das Chatten mit einem technischen System erlaubt.[1096] Die Dialogsysteme des Chatbots nutzen Natural Language Processing (NLP), um geschriebene Sätze zu verstehen und im Nachgang auf diese reagieren zu können. Er ahmt hierbei natürlichsprachlichen geschriebenen Text oder natürlichsprachliche gesprochene Sprache nach, sodass eine intelligente, intuitive Mensch-Maschine-Kommunikation möglich ist.[1097]

So werden auf der Basis von intelligenten KI-Technologien die Fähigkeiten und Talente der Bewerber getestet. Gleichzeitig unterstützen solche Tools die Auswertung und Bewertung der einzelnen Bewerbenden. Die Leistungen solcher Tools gehen dabei weit über die Leistungen herkömmlicher Datenbanksysteme und Standard-Business-Intelligenz-Lösungen hinaus. Wie viele Innovationen beinhalten solche Entwicklungen Chancen und Risiken und müssen daher auch zum rechtlichen Rahmen

---

[1093] Siehe auch *Söbbing*, InTeR 2018, S. 64-67.

[1094] vgl. *Verhoeven*, 2020, S. 103.

[1095] Vgl. *Schnitzler*: Online-Kommunikation im Recruiting für KMU: Reifegrade von Employer Branding & Candidate Experience, Springer Gabler, 2020, S.24-25

[1096] vgl. *Hermeier* et al., 2018, S.10

[1097] vgl. Wilke, Gewndolin/Bendel, Oliver: KI-gestütztes Recruiting - technische Grundlagen, wirtschaftliche Chancen und Risiken sowie ethische und soziale Herausforderungen, in: HMD. Praxis Der Wirtschaftsinformatik, Bd.59, Nr.2, 2022, doi:10.1365/s40702-022-00849-w, S.653

passen, den der Gesetzgeber vorgegeben hat. Darum ist es wichtig, die rechtlichen Aspekte des Einsatzes von künstlicher Intelligenz im HR-Recruiting-Prozess zu untersuchen.

Die Anwendung von KI-Technologien im HR-Recruiting-Prozess ist noch nicht sehr verbreitet und es stellt sich auch die Frage nach der grundsätzlichen Akzeptanz bei Bewerbern, wenn sie zunächst mit einer Maschine kommunizieren müssen. Gerade in der Zeit von „Talent War", also dem Kampf um die talentiertesten Köpfe, klingt es doch für den Bewerber eher herabwürdigend, wenn er zunächst mit einem KI-System zu tun hat. Dabei ist durchaus die Frage berechtigt, ob der Bewerber überhaupt merkt, dass er mit einer Maschine kommuniziert. Mit den Chatbots wird angestrebt, dass der Mensch nicht merkt, dass sein Gegenüber kein Mensch ist.

Aktuelle Versuche mit Chatbots zeigen jedoch, dass die Reaktionen der Chatbots nicht immer vorhersehbar und planbar sind. Microsoft musste den Chatbot „Tay" deaktivieren, weil dieser nach wenigen Stunden angefangen hat, rassistische Aussagen zu treffen. Technisch sind Bots näher mit einer Volltextsuchmaschine verwandt als mit künstlicher oder gar natürlicher Intelligenz. Mit der steigenden Computerleistung können Chatbot-Systeme allerdings immer schneller auf immer umfangreichere Datenbestände zugreifen und daher auch intelligente Dialoge für den Nutzer bieten. Solche Systeme werden auch als virtuelle persönliche Assistenten bezeichnet.[1098] Wie unten dargestellt, können diese für das Unternehmen sehr schnell zu einer unangenehmen Haftung führen.[1099]

Fragt ein KI-System einen Bewerber nach personenbezogenen Daten, richtet sich auch dies nach den arbeitsrechtlichen Grundsätzen zum Fragerecht des Arbeitgebers. Das Bundesarbeitsgericht[1100] hat hier in jahrzehntelanger detaillierter Rechtsprechung festgelegt, welche Fragen im Bewerbungs- und Interviewprozess gestellt werden dürfen und welche nicht. Da es sich beim Bewerbungsprozess um ein sogenanntes „vorvertragliches Vertrauensverhältnis" handelt, ist eine Speicherung von Daten, welche

[1098] https://de.wikipedia.org/wiki/Chatbot, abgerufen am 11.10.2024.
[1099] *Zirn*, Chatbots – was Unternehmen wissen müssen, CIO Magazin, 17.10.2017.
[1100] *Schröder*, Datenschutzrecht für die Praxis, 2. Aufl. 2016, Kapitel 3: Datenschutz in der Personalabteilung/Arbeitnehmerdatenschutz.

mit zulässigen Fragen erhoben wurden, datenschutzrechtlich immer unproblematisch. Diese Daten genügen den Anforderungen des Art. 6 DSGVO und werden im Regelfall in entsprechenden Bewerbermanagementsystemen als Stammdaten erfasst. Unproblematisch ist daher die Erhebung von Daten, wie:

- Namen
- Anschrift
- Telefonnummer
- E-Mail-Adresse

Welche Daten darüber hinaus im Einzelfall im Rahmen der Bewerbung abgefragt werden können, richtet sich nach objektiven beruflichen Kriterien und dem vom Arbeitgeber festgelegten Anforderungsprofil. Nach der bisherigen Rechtsprechung des Bundesarbeitsgerichts wird ein Fragerecht des Arbeitgebers bei den Einstellungsverhandlungen nur insoweit anerkannt, als der Arbeitgeber ein berechtigtes, billigenswertes und zugleich schutzwürdiges Interesse an der Beantwortung seiner Fragen im Hinblick auf das Arbeitsverhältnis hat. Es kommt also immer auf die Stelle an, welche Fragen tatsächlich gestellt werden dürfen und damit verbunden auch, welche personenbezogenen Daten zulässigerweise gespeichert werden dürfen.[1101]

Die darüber hinausgehende Erhebung von sogenannten „schutzwürdigen Daten" ist datenschutzrechtlich nur eingeschränkt möglich. Hierunter fallen personenbezogene Daten über:

- rassische Herkunft
- ethnische Herkunft
- Religion oder Weltanschauung
- Behinderung
- sexuelle Identität
- Gesundheit
- Vermögensverhältnisse
- Vorstrafen
- laufende Ermittlungsverfahren

[1101] *Schröder*, Datenschutzrecht für die Praxis, 2. Aufl. 2016, Kapitel 3: Datenschutz in der Personalabteilung/Arbeitnehmerdatenschutz.

Die oben genannten Daten darf der Arbeitgeber auch datenschutzrechtlich nur unter den strengen Voraussetzungen des § 8 Abs. 1 AGG erheben. Maßgeblich für die Zulässigkeit der Erhebung sind daher die aus objektiver Sicht zu bestimmenden wesentlichen und entscheidenden beruflichen Anforderungen. Es kommt also sehr darauf an, was das Unternehmen macht und es hat immer eine Beurteilung des Einzelfalls zu erfolgen.[1102]

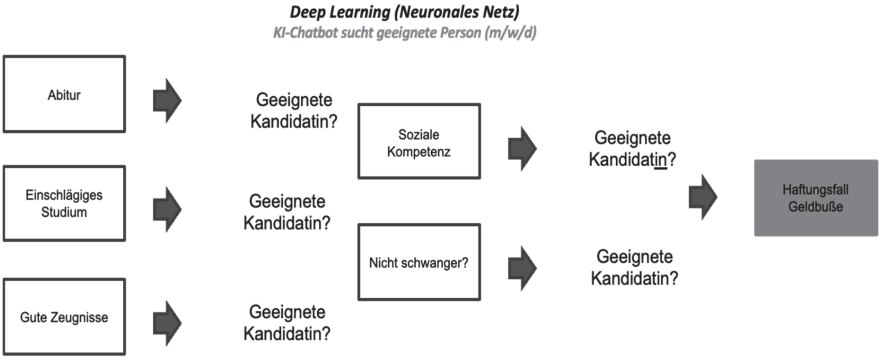


Abb. 1: KI-Chatbot im HR-Recruiting-Prozess

Hat Der Chatbot könnte beim Trainieren gelernt haben, dass sein Auftraggeber keine schwangeren Frauen mag, da diese nach der Einstellung sehr schnell wieder ausfallen. Dies wurde dem Chatbot zwar nicht ausdrücklich so mitgeteilt, aber er kommt auf der Basis seiner Deep-Learning-Routinen zu diesem Ergebnis. Im Bewerbungsprozess stellt der Chatbot eben diese Frage, die nach § 8 Abs. 1 AGG nicht zulässig ist (siehe Abb. 1), was man als „Halluzination" bezeichnen würde. Wenn in der Folge solcher Fragen auf Basis einer Halluzination ein Bewerber oder eine Bewerberin abgelehnt wird, sind Schadensersatzklagen auf Grundlage des AGG möglich. Aus Sicht des Unternehmens stellt sich dann die Frage, ob das Unternehmen beim Hersteller des KI-Systems Ersatz verlangen kann. Das Unternehmen kann das KI-System selbst nicht verklagen. Auch wenn KI-Systeme menschenähnlich wirken können und intelligent handeln, können sie nicht selbst für einen verursachten Schaden in Anspruch

[1102] § 8 AGG: Entschädigung und Schadensersatz. *Thüsing*, Münchener Kommentar zum BGB, 7. Aufl. 2015, Rn. 16-20.

genommen werden.[1103] Autonome Systeme sind nach derzeitiger Gesetzeslage keine Rechtssubjekte und besitzen keine eigene Rechtspersönlichkeit.[1104]

Grundsätzlich kann der Bewerber gegenüber dem Unternehmen bezüglich der unerlaubten Fragen des KI-Systems eine Entschädigung und Schadensersatz nach § 15 AGG verlangen. Bei einem Verstoß gegen das Benachteiligungsverbot ist der Arbeitgeber nach § 15 Abs. 1 S. 1 AGG verpflichtet, den hierdurch entstandenen Schaden zu ersetzen. Die Benachteiligung muss dabei unzulässig sein, darf also nicht nach §§ 5, 8 bis 10 AGG gerechtfertigt sein.[1105] Nach § 15 Abs. 1 S. 2 AGG gilt dies nicht, wenn der Arbeitgeber die Pflichtverletzung nicht zu vertreten hat. Die Schadensersatzverpflichtung trifft den Arbeitgeber sowie Personen, deren Verhalten ihm nach § 278 BGB zuzurechnen ist.[1106] Leider trifft der Gesetzgeber keine klare Regelung über die Zurechnung der Benachteiligung durch Dritte.[1107] Unter anderem wird angenommen, dass wegen des Bezugs auf das Vertretenmüssen in § 15 Abs. 1 AGG der § 278 BGB relevant ist.[1108]

Dagegen wird auch vertreten, dass § 278 BGB zur Anwendung kommt, soweit Führungskräfte handelten, denn wenn Arbeitnehmer ohne Personalverantwortung handelten und ein enger und qualifizierter Zusammenhang mit der arbeitsvertraglichen Aufgabenerfüllung bestehe, hafte der Arbeitgeber unter den Voraussetzungen des § 831 BGB. Natürlich wird nichts darüber ausgesagt, wie die Haftung auszusehen hat, wenn ein KI-System handelt.

Einfach ist der Sachverhalt, wenn dem Unternehmen grundsätzlich ein Verschulden i. S. v. § 278 BGB zuzurechnen ist, konkret, wenn das Unternehmen selbst vorsätzlich eine vom Hersteller eingesetzte Sperre zu unzulässigen Fragen entfernt hat oder fahrlässig die hierzu notwendige Sorgfalt außer Acht gelassen hat. Dieser Fall wird in der Praxis wohl recht selten vorkommen, aber wenn er vorkommt, ist ein Zurechnen i. S. v. § 15 Abs. 1 S. 2 AGG i. V. m. § 278 BGB zu bejahen.

[1103] *Günther/Böglmüller*, BB 2017, S. 53.
[1104] *Bräutigam/Klindt,* NJW 2015, S. 1137; *Cornelius*, MMR 2002, S. 353; *Horner/Kaulartz,* InTeR 2016, S. 22, 24.
[1105] BeckOK ArbR/*Roloff*, AGG § 15 Rn. 1–3.
[1106] BAG, 25.10.2007 = NZA 2008, S. 223, 227.
[1107] Vgl. grundsätzlich *Wobst*, NZA-RR 2016, S. 508. Abs. 5 ist jedenfalls nicht abschließend, BeckOK ArbR/*Roloff*, Rn. 33. §§ 31, 278 BGB finden Anwendung.
[1108] *Kamanabrou*, RdA 2006, S. 321, 338.

Mit einer sehr extensiven Gesetzesauslegung ließe sich ein KI-System möglicherweise noch als Erfüllungsgehilfe einordnen, jedoch stößt man beim Erfordernis des eigenen Verschuldens bei einer Maschine nach derzeitigem Gesetzeswortlaut an Auslegungsgrenzen.[1109] Verschulden setzt nach allgemeinem Verständnis eine willentliche Steuerung eigenen Handelns voraus.[1110] Intelligentes Handeln eines Roboters ist immer auf eine entsprechende Programmierung zurückzuführen. Das KI-System wird immer nur so autonom handeln können, wie es die Programmierung vorgegeben hat. Zwar mögen künstlich intelligente Systeme aus einem Fehlverhalten lernen und dadurch ihr Handeln für die Zukunft optimieren können („künstliche Einsichtsfähigkeit"). So autonom sich die Handlung des KI-Systems aber darstellt, sie ist nicht Ergebnis eines selbstbestimmten Entschlusses des KI-Systems. Dass das KI-System autonom handelt und die Fähigkeit besitzt, Entscheidungen zu treffen und zu vollziehen, beruht letztlich auf dem Willen des Entwicklers und/oder Anwenders.[1111]

Möglicherweise könnte über die Gefährdungshaftung eine Zurechnung des Handelns des KI-Systems i. S. v. § 15 Abs. 1 S. 2 AGG zum Unternehmen konstruiert werden. Gefährdungshaftung ist die Haftung für Schäden, die sich aus einer erlaubten Gefahr (z. B. Betrieb einer gefährlichen Einrichtung, Halten eines Haustieres) ergeben. Im Unterschied zur Haftpflicht wegen unerlaubter Handlung kommt es bei einer Gefährdungshaftung auf die Widerrechtlichkeit der Handlung oder ein Verschulden des Schädigers nicht an. Danach würde derjenige, der ein autonomes System (z. B. das KI-System zum Bewerbermanagement) einsetzt, prinzipiell unabhängig von einem eigenen Verschulden für Schäden haften, die durch den Einsatz entstehen. Fraglich ist, ob dies nicht eine Erweiterung der Haftung nach § 15 AGG ist, da für diesen Fall kein Verschulden mehr notwendig ist und ob dies wirklich vom Gesetzgeber so gewollt gewesen ist.

[1109] BeckOK ArbR/*Roloff*, AGG § 15 Rn. 1–3.
[1110] *Spindler* in: BeckOK BGB, 40. Ed., Stand: 01.05.2016, § 827 BGB Rn. 1.
[1111] *Günther/Böglmüller*, BB 2017, S. 53.

III. Praktisches Beispiel autonomes Fahren

In Talkshows wie auch in philosophischen Diskussionen wird oft die Utopie beschrieben, dass autonom fahrende Autos in der Zukunft entscheiden müssten, welche Menschen sie in einer ausweglosen Situation töten würde. Also müsste der Algorithmus des Fahrzeuges in dieser Situation bewerten, ob das Fahrzeug eher einen frauenunterdrückenden Taliban tötet oder ein unschuldiges kleines Mädchen. Der Algorithmus dürfte oder müsste also über den Wert eines Menschen für die Gesellschaft entscheiden. Oft wird es dann sogar als Dammbruch gesehen, dass zukünftig generell Algorithmen über den Wert eines Menschenlebens entscheiden dürften. Einmal davon abgesehen, dass eine solche Konstellation schon aus technischen Gründen sehr unwahrscheinlich ist, dürfte der Algorithmus nach dem neuen § 1e Abs. 2 Nr. 2 lit. c) StVG eine solche Entscheidung gar nicht vornehmen. Mit der Schaffung dieser Regelung wurde die leidige Diskussion bereits im Ansatz erstickt, aber lässt der neue § 1e Abs. 2 Nr. 2 lit. c) StVG dennoch eine Frage offen, weil an der Stelle nicht zu Ende gedacht worden ist.

Beim autonomen Fahren tritt anstelle des Menschen die künstliche Intelligenz oder ein Algorithmus i. V. m. Machine Learning (nachfolgend nur „KI"), um das Fahrzeug zu führen. Der KI müssen somit gewisse Wertungsmöglichkeiten zugestanden werden, denn auch gem. § 1 e Abs. 2 Nr. 1, Nr. 2 Alt. 1 StVG müssen Kraftfahrzeuge mit autonomer Fahrfunktion über eine technische Ausrüstung verfügen, die in der Lage ist,

- die Fahraufgabe innerhalb des jeweils festgelegten Betriebsbereichs selbstständig zu bewältigen, ohne dass eine fahrzeugführende Person in die Steuerung eingreift oder die Fahrt des Kraftfahrzeugs permanent von der technischen Aufsicht überwacht wird,
- selbstständig den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen

und die über ein System der Unfallvermeidung verfügt, das auf Schadensvermeidung und Schadensreduzierung ausgelegt ist. Fraglich ist indes, ob darüber hinausgehende Einschränkungen angängig sind.[1112] Zu denken ist etwa an Ad-hoc-Verkehrszeichen

[1112] *von Bodungen/Gatzke*, RDi 2022, S. 354.

oder Weisungen von Verkehrspolizisten, welche von autonomen Fahrfunktionen (noch) nicht erfasst werden können.[1113] Nach § 1 e Abs. 2 Nr. 3 StVG müssen Kraftfahrzeuge mit autonomer Fahrfunktion technisch so ausgerüstet sein, dass sie sich unter bestimmten Umständen (siehe § 1 e Abs. 2 Nr. 3, 5, 7, 8, 10 StVG) in einen risikominimalen Zustand versetzen können. Notwendig ist dies, wenn die Fortsetzung der Fahrt nur unter Verletzung des Straßenverkehrsrechts möglich ist – etwa, weil eine Ampel aufgrund eines technischen Defekts nicht auf grün umspringt.[1114] Dabei wird der Begriff des risikominimalen Zustands in § 1 d Abs. 4 StVG legaldefiniert und ist danach ein Zustand, in dem das Fahrzeug mit aktivierter Warnblinkanlage an geeigneter Stelle zum Stillstand kommt, um größtmögliche Sicherheit für die Fahrzeuginsassen, andere Verkehrsteilnehmende und Dritte zu gewährleisten.

Bereits die Ethikkommission „Automatisiertes und Vernetztes Fahren" ist in ihrem Bericht vom Juni 2017 unter Ziffer 5 zu der Erkenntnis gekommen, dass automatisierte und vernetzte Technik Unfälle so gut wie praktisch möglich vermeiden sollte. Die Technik muss nach ihrem jeweiligen Stand so ausgelegt sein, dass kritische Situationen gar nicht erst entstehen, dazu gehören auch Dilemma-Situationen, also eine Lage, in der ein automatisiertes Fahrzeug vor der „Entscheidung" steht, eines von zwei nicht abwägungsfähigen Übeln notwendig verwirklichen zu müssen. Mit der Einführung des § 1e Abs. 2 Nr. 2 lit. c) StVG zum 28.07.2021 wurde dazu eine Neuerung ins Gesetz aufgenommen, dass Kraftfahrzeuge mit autonomer Fahrfunktion für den Fall einer unvermeidbaren alternativen Gefährdung von Menschenleben keine weitere Gewichtung anhand persönlicher Merkmale vornehmen dürfen.[1115]

Bereits auf den 30. Münchner Medientagen im Oktober 2016 hat die ehemalige Bundeskanzlerin Angela Merkel gefordert, dass Algorithmen, die Internetdienste für das Filtern von Informationen nutzen, transparent bleiben müssten. Die Mediennutzung werde immer stärker durch Algorithmen, Bots und intelligente Empfehlungssysteme beeinflusst. Algorithmen führten dazu, dass etwa Leser verstärkt im Netz nur noch

[1113] *Hilgendorf*, JZ 2021, S. 444 (447).
[1114] *von Bodungen/Gatzke*, RDi 2022, S. 354.
[1115] BT-Drucks. 19/27439 vom 09.03.2021, S. 1-2.

die Themen angeboten bekämen, die ihrem Suchverhalten entsprächen. Das könne ihre Fähigkeit verringern, sich mit anderen Meinungen auseinanderzusetzen.[1116] Dabei gibt es schon Regelungen, die zur Neutralität von Algorithmen führen sollen. Bereits im Erwägungsgrund. 71 S. 6 DSGVO findet sich eine Verpflichtung zur „Neutralität von Algorithmen". Ähnlich wie für das Scoring in § 28b Nr. 1 BDSG werden für das Profiling ein „geeignetes mathematisches oder statistisches Verfahren" und der Ausschluss diskriminierender Rechenverfahren verlangt.[1117] Im Falle von § 1e Abs. 2 Nr. 2 lit. c) StVG geht man sogar ein Schritt weiter und untersagt zu Recht einer KI, eine Wertung über Qualität von Menschenleben auszuüben.

Neben dem Verbot einer qualitativen Wertung von Menschenleben bleibt aber die Frage der quantitativen Wertung offen. Es wäre nach dem Gesetzeswortlaut durchaus erlaubt, bei Kraftfahrzeugen mit autonomer Fahrfunktion z. B. einen Algorithmus zu implementieren, der unterscheidet, ob bei einem unausweichlichen Unfall der Algorithmus eine Wahl trifft, ob eine Gruppe mit einer geringeren oder einer höheren Anzahl von Menschen getötet / geschädigt werden muss. An dieser Stelle sollte noch nachgebessert werden und auch hier sollte der Algorithmus ebenfalls keine Wertung vornehmen dürfen, sondern alle technischen Möglichkeiten ergreifen, damit es gar nicht erst zu einer solchen Entscheidung kommt.

IV. Embedded Law

In der Literatur[1118] wird darüber diskutiert, ob es Kontrollpflichten geben soll, die sogenannte „Kontrollalgorithmen" erschaffen sollen, um die Kontrolle über KI nicht zu verlieren. Auch über eine TÜV-Prüfung für Algorithmen wird diskutiert. Dies stellt natürlich einen erheblichen Eingriff in die Entwicklung von Algorithmen dar. Einen weitaus weniger dramatischen Weg geht das „Embedded Law". Wie aus Grafik zu entnehmen ist, stellt das Embedded Law einen Filter dar, der nicht zulässige Fragen und Aktionen herausfiltert. Abb. 2 zeigt dies am Beispiel des oben beschriebenen HR-Prozesses:

[1116] https://www.heise.de/newsticker/meldung/Algorithmen-und-Scoring-Maas-fordert-digitales-Anti-Diskriminierungsgesetz-3761722.html?seite=2, abgerufen am 11.10.2024.

[1117] *Härting*, ITRB 2016, S. 209-211.

[1118] *Martini,* JZ 2018, 1017 bis 1025.

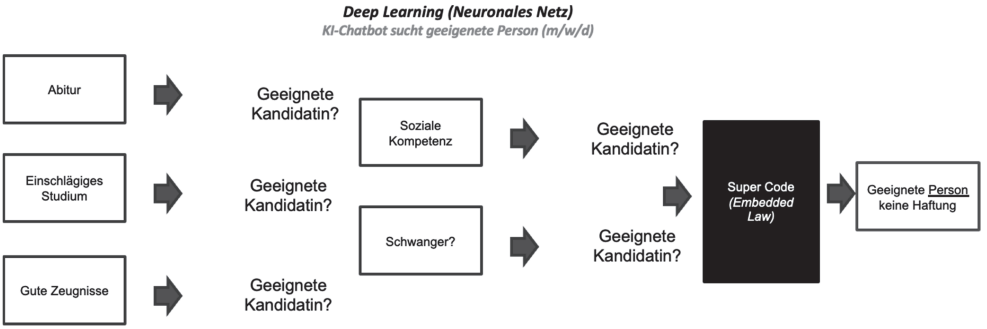


Abb. 2: KI-Chatbot im HR-Recruiting-Prozess mit Embedded Law

Beim Beispiel des autonomen Fahrens würde das bedeuten, dass die KI generell keine Entscheidung über die Qualität eines Menschenlebens treffen darf.

Das in der KI (z. B. im Machine Learning, Algorithmus, LLM etc.) implementierte Embedded Law verankert in einem sogenannten „Super Code" absolute Regeln (i.S. v. Geboten und Verboten) im System der KI,[1119] gegen die KI niemals verstoßen darf, insbesondere auch dann nicht, wenn das Gelernte und die daraus entwickelten Logiken zu einem anderen Ergebnis als die absoluten Regeln des Super Codes kommen. Der Super Code muss somit über der Logik der KI und den Ergebnissen der Algorithmen stehen. Dabei ist der Super Code als eine Art Selbstregulierung zu verstehen, der nicht von einer Behörde, wie die BaFin, vorgegeben wird, sondern die Hersteller oder Betreiber von KI-Systemen selbst dafür sorgen lässt, dass ihre Systeme gesetzestreu handeln. Gleichzeitig würde die Angst vor der Nichtbeherrschbarkeit der KI-Systeme[1120] erheblich eingeschränkt werden, da der Super Code dafür sorgen würde, dass die KI kontrollierbar bleibt. Anders als in dem Buch von Robert Harris[1121] würde die Kontrolle über die KI und damit über die Märkte nicht verloren gehen.

Durch ein sogenanntes „Rulemapping"[1122] werden Regeln des Super Codes und damit das Recht insbesondere in die KI-Tradersysteme integriert. Das Rulemapping soll

[1119] *Breidenbach* in: Rethinking: Law 2018, S. 38-41, 40.
[1120] *Moorstedt*, Intelligenz außer Kontrolle, SZ.de vom 11.10.2018, abgerufen am 24.10.2018.
[1121] *Harris*, „The Fear Index" (2011), deutsche Ausgabe unter dem Titel „Angst" erstmals 2011 bei Heyne erschienen.
[1122] Vgl. ausführlich *Breidenbach* in: Breidenbach/Glatz, Rechtshandbuch LegalTech 2018, S. 235 ff.

damit ausschließen, dass es durch die KI zu bedauerlichen Marktstörungen und Haftungsfällen kommt. Denn ohne den Super Code könnten KI-Systeme nicht vereinbar mit dem geltenden Recht sein.

V. Anwendung des Super Codes

Fraglich ist, wie ein solcher Super Code in der Praxis aussehen sollte. Im Gegensatz zu Asimovs Gesetzen enthält der Super Code keine drei oder vier Gesetze, deren richtige Interpretation der KI überlassen wird. Vielmehr müssten im Super Code grundsätzlich alle kodifizierten Gesetze Verbotsnormen enthalten sein. Auslegungen oder Ermessenspielräume der KI dürften dabei niemals gegen den Super Code verstoßen und der Super Code müsste weitestgehend keine Interpretation zulassen oder, wenn eine Interpretation notwendig wäre, eine menschliche Interaktion verlangen.

Denkbar wären aber durchaus Abstufungen bei der Transformation in den Super Code, wenn die KI auch nur partiell eingesetzt wird. Juristen würden den Super Code gestalten, welcher dann von Ingenieuren in die KI umgesetzt wird. Der Super Code der Maschine muss somit über der Logik der KI stehen. Durch das Rulemapping[1123] werden Regeln und damit insbesondere das Recht integriert und wesentlicher Bestandteil der KI. Anderenfalls käme es zu bedauerlichen Haftungsfällen und gesetzliche Anforderungen, z. B. die aus dem Produktsicherheitsgesetz (ProdSG), würden nicht eingehalten werden, was dazu führen würde, dass die KI niemals konform handeln könnte.

Ausgehend von dem in Ziffer 1. beschriebenen Fall, wäre die konkrete Umsetzung folgende: Wenn der HR-Chatbot zu dem Ergebnis kommen würde, dass sein Auftraggeber keine schwangeren Frauen mag und er deshalb die Frage der Bewerberin stellen will, ob sie schwanger ist, sorgt der Super Code dafür, dass der Chatbot die Frage nicht stellt, auch wenn es den Algorithmen nach logisch wäre. Neben einer Schwangerschaft wären mit dem Super Code als Embedded Law weitere diskriminierende Fragen, z. B. hinsichtlich

- rassischer Herkunft,
- ethnischer Herkunft,

[1123] Vgl. ausführlich *Breitenbach* in: Breitenbach/Glatz, Rechtshandbuch LegalTech 2018, S. 235 ff.

- Religion oder Weltanschauung,
- Behinderung,
- sexueller Identität,
- Gesundheit,
- Vermögensverhältnissen,
- Vorstrafen,
- laufender Ermittlungsverfahren,

entsprechend dem Allgemeinen Gleichstellungsgesetz (AGG) ausgeschlossen.

VI. Gewissen

Wenn durch den Filter des Embedded Law, dem Super Code, die Maschine lernt, was sie tun darf und was nicht, dann könnte man dies philosophisch auch als ein Gewissen verstehen. Das Bundesverfassungsgericht hat dem Begriff „Gewissen" in einer Entscheidung aus dem Jahre 1961 Konturen verliehen. Als eine Gewissensentscheidung gilt danach „jede ernste sittliche, d. h. an den Kategorien von Gut und Böse orientierte Entscheidung […], die der Einzelne in einer bestimmten Lage als für sich bindend und unbedingt verpflichtend innerlich erfährt, so dass er gegen sie nicht ohne ernste Gewissensnot handeln könnte."[1124] Als Gewissen wird im Allgemeinen eine besondere Instanz im menschlichen Bewusstsein angesehen, die bestimmt, wie man urteilen soll und die anzeigt, ob eine Handlungsweise mit demjenigen übereinstimmt oder nicht übereinstimmt, was ein Mensch als für sich richtig und stimmig ansieht.[1125] Dies codifiziert eine Gesellschaft zu einem großen Teil durch Gesetze/Normen und sanktioniert auch ein Fehlverhalten durch eben die Gesetze/Normen.

Eben dies tut auch der Filter des Super Codes, indem er der KI Regeln gibt, gegen die KI nicht verstoßen darf. Dabei könnte man zu der Ansicht kommen, dies wäre das Gleiche wie der Prozess, bei dem Eltern ihren Kindern erklären, was man tun darf und was nicht, denn durch diese Erziehung bildet sich bei dem Kind ein

[1124] Vgl. BVerfGE 12, S. 45, 55.
[1125] https://de.wikipedia.org/wiki/Gewissen, abgerufen am 11.10.2024.

Gewissen heraus. Es stellt sich somit die Frage, ob die KI durch das Embedded Law/den Super Code ein Gewissen erhalten kann.

Wenn man diese Frage bejaht, wäre die nächste Frage, die man sich philosophisch stellen müsste, ob die KI ein Bewusstsein erhalten kann.

J. Literaturverzeichnis

2001 - Odyssee im Weltraum (1968).
Ahlberg BeckOK Urh, 32. Ed. 15.9.2021, UrhG § 2 Rn. 55
Ahlberg/Lauber-Rönsberg, BeckOK UrhR, 38. Ed. 01.05.2023, UrhG § 23, Rn. 10.
Albrecht, VD 06/2006, 143, 144.
Aldridge, High-Frequency Trading, 2nd ed 2013, Gresser, Praxishandbuch Hochfrequenzhandel, 2016, Jaskulla BKR 13, 221, Kobbach BKR 13, 233, Schultheiß WM 13, 596, Kasiske WM 14, 1933, Kindermann/Coridaß ZBB 14, 178.
Algorithmischer Handel und Hochfrequenzhandel. Mitteilung der BaFin, geändert am 13. Dezember 2017.
Alpert, CR 2000, 345, 347;
Amann/Brambring/Hertel, Die Schuldrechtsreform in der Vertragspraxis, 2002
Ambrosius, B. in: Däubler, W.; Bertzbach, M.: AGG, 2. Aufl. 2008, § 20 Rn. 40
Andrees/Bitter/Buchmüller/Uecker, in: Hoeren, S. 104,
Antoine, L. in: CR 2019, S. 1–8.
Armbrüster, C. in: Begemann, M.; Bruns, A. (Hrsg.): Die Versicherung des Alterns, 2008,
Armbrüster, C.: Benachteiligungsverbot und Rechtfertigungsgründe beim Abschuss privatrechtlicher Versicherung, Expertise erstellt im Auftrag der Antidiskriminierungsstelle des Bundes, Mai 2010, S. 6.
Asimov, Der Zweihundertjährige, 1978, (The Bicentennial Man And Other Stories, 1976).
Auer-Reinsdorff, ITRB 2006, 181.

Bachmann, R.; Kemper, G.; Gerzer, T.: Big Data – Fluch oder Segen? Unternehmen im Spiegel gesellschaftlichen Wandels, 2014, S. 2.
Bartl, Produkthaftung nach dem neuen EG-Recht ProdHaftG, Landsberg 1989, 142
Bartsch, CR 2000, 721, 722 ff.
Basedow, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 5/1: Schuldrecht Besonderer Teil III/1, 7. Auflage 2017, § 309 Nr. 5 Rn. 8.
BASt, Rechtsfolgen zunehmender Fahrzeugautomatisierung, 2012
Baumann/Wirtz, RDi 2024, S. 27.
Beck, JR 2009, 225, 229 f.
Beck: Japanisch-Deutsches Zentrum, Mensch-Roboter-Interaktionen aus interkultureller Perspektive, 2011, S. 124, 126
Becker/Feuerstack, MMR 2024, S. 22.
Beckmann, R. M. in: Staudinger, BGB, 2014, § 453 BGB, Rn. 37
Berger, C.: Jauernig, BGB, 14. Aufl. 2011, § 453, Rn. 11
Berger/Stemper, WM 2010, 2289, 2294
Berz/Dedy/Granich, DAR 2002, 545.
Bettinger/Scheffelt, CR 2001, 729, 734.;
Beuth, Zeitonline vom 24.03.2016, Microsoft Twitter-Nutzer machen Chatbot zur Rassistin.
BGBl. I, S. 1693.
BGBl. II, 1977, S. 811 ff.
Bisges, MMR 2012, 574 (577 f.)
Bodungen/Gatzke, RDi 2022, S. 354.
Bodungen/Hoffmann, NZV 2015, 521, 524 ff.
Boerner, ZIP 2001, 2264, 2272.
Bomhard/Siglmüller, RDi 2024, 45, Rn. 1.
Bonnmann/Erberich, in: Luther/Knot/Palm, Die Schuldrechtsreform, 2001, S. 106.
Borges, NJW 2018, 977.
Borges/Sesing, in: Matusche-Beckmann, Saar-Tage 2016: Rechtsprobleme der Informationsgesellschaft, 2018 (iErsch.), 177, 187.

Bown, Liability for Defective Software in the United Kingdom, in: Software Protection 1/1986, 1, 12
Bräutigam/Klindt, NJW 2015, 1137
Bräutigam/Rücker, E-Commerce, 2016, 14 B III Rn. 64.
Bräutigam/Thalhofer in Bräutigam, Teil 14, Rn. 120
Brehm, FS Niederländer, 1991, 233
Brehmer, Wille und Erklärung, 1992, S. 29, 80 f.
Breidenbach in: Breidenbach/Glatz, Rechtshandbuch LegalTech 2018, S. 235 ff.
Breidenbach in: Rethinking: Law 2018, S. 38–41, 40.
Britisches Urheberrecht: Designs and Patents Act 1988
Brox, Allgemeiner Teil des BGB, 41. Aufl. 2017, Rn. 83.
Brox/Walker, Schuldrecht AT, 36. Aufl. 2012,
Bruderer, H.: Erfindung des Computers, Elektronenrechner, Entwicklungen in Deutschland, England und der Schweiz. In: Meilensteine der Rechentechnik. 2., völlig neu bearbeitete und stark erweiterte Auflage. Band 2. De Gruyter, 2018, ISBN 978-3-11-060261-6; Wörterverzeichnis zur Technikgeschichte, S. 408 (eingeschränkte Vorschau in der Google-Buchsuche, abgerufen am 23.11.2019).
Brüggemeier, DeliktsR Rn. 565 ff.
Brüggemeier, RabelsZ 66, 2002, 193 ff.
Brüggemeier, ZHR 152, 1988, 511, 525 f.
Brunotte, CR 2017, 583, 585 f.
Buchberger, ITRB 2014, 116, 117.
Büchting/Heussen, Beck'sches Rechtsanwalthandbuch, 10. Aufl. 2011, C.13 deliktische Haftung Rn.15 bis 18.
Bydlinski, Grundzüge der juristischen Methodenlehre, 2. Aufl. 2011, S. 23.

C-26/22 und C-64/22, EU:C:2023:XXX „Restschuldbefreiung"
Clemens, NJW 1985, 1998
COM/2022/496 final
Copyright and Related Rights Act 2000
Cornelius, MMR 2002, 353, 354
Craig S. Smith: AI Hallucinations Could Blunt ChatGPT's Success. In: IEEE Spectrum, 24. März 2023. Abgerufen am 24. September 2023 (englisch)

Dallmann/Busse ZD 2019, 394 (395)
Dauner-Lieb, in: Dauner-Lieb/Langen, BGB Schuldrecht Band 2/1, 2. Aufl. 2012, § 276 Rn. 10.
Deselby, Journal of dyslexic programming 13 (2017), 131 ff.;
Deutsch, NJW 1978, 1998, 2000.
Deutsch/Ahrens, Deliktsrecht, 6. Aufl. 2014, Rn. 7
Dieker ZD 2024, 132, 135, beck-online
Dietrich, Produktbeobachtungspflicht und Schadenverhütungspflichtig der Produzenten, 1994
Dietrich, ZUM 2010, 567 ff.
Dreier, T. / Schulze, G. a.a.O., Rz. 20
Dreier, T. / Schulze, G.: Urheberrechtsgesetz, 2. Auflage, § 69a Rz. 12.
Dreier, T.: Urheberrecht, 2. Auflage, § 69a, Rz. 14.
Dreier/Schulze/Dreier, 7. Aufl. 2022, UrhG § 44b, Rn. 7.
Dreier/Schulze/Dreier, UrhG § 69c, Rn. 27.

E. „Cyborg" u. a. § 14 MPG i. V. m. Medizinprodukte-Betreiberverordnung.
Ehinger/Grünberg K&R 2019, 232 (236)
Ensthaler, J. in: NJW 2016, S. 3473–3552, (3473).
Entwurf der EU-Richtlinie über KI-Haftung (COM/2022/496 final)
Epping, V.: Grundrechte, 7. Auflage 2017, Rn. 770.
Erdmann FS v. Gamm, 1990, 389 (399 f.))
Erman, in: Hefermehl/Werner, BGB, 9. Aufl. 1993, § 11 Nr. 10 AGBG Rn. 36.
Ernst, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021
Ertel, W.: Grundkurs Künstliche Intelligenz, 4. Auflage 2016, S. 132, 258, 300, 331, 333.
Erwägungsgrund 12 KI-VO.

Erwägungsgrund 14 RL (EU) 2016/943.
Erwägungsgrund 18 UAbs. 1 Satz 4 DSM-RL; BT-Drs. 19/27426, 87.
Erwägungsgrund 47 ber. ABl. 2018 L 127 S. 2.
Erwägungsgrund 49 KI-VO.
Erwägungsgrund 51.
Erwägungsgrund 52 KI-VO.
Erwägungsgrund 70 KI-VO.
Erwägungsgrund 71 DSGVO.
Erwägungsgrund 71 KI-VO.
Erwägungsgrund 72 KI-VO.
Erwägungsgrund 9 der Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April 2019
Esser, JZ 1953, 129.
Etteldorf, MMR-Aktuell 2023, 456626.
Euklid, Die Elemente, herausgegeben von Thaer, C., 1. Auflage 2011, § 2
Eurex-Rundschreiben 213/13 vom 27. September 2013.

Faust, BGB AT, 6. Aufl. 2018, § 2 Rn. 4
Finke, Die Auswirkungen der europäischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, 2001, S. 9 ff.
Fleck/Thomas, NJOZ 2015, 1393, 1397
Foerste, DB 1999, 2199, 2200
Foerste, in: Foerste./v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24 Rn. 37
Foerste, in: Foerste/Graf v. Westphalen, HdB Produkthaftung, § 24
Foerste, in: Foerste/v. Westphalen, Produkthaftungshandbuch, 3. Aufl. 2012, § 24
Frenz/van den Broek, NZV 2009, 530
Frisse, F./ Glaßl, R./ Baranowski, A./ Duwald, L. in: BKR 2018, S. 177.
Fritzemeyer, in: Lehmann/Meents, Handbuch des Fachanwalts Informationstechnologie, 2. Aufl. 2011, Kapitel 2 Rn. 70.
Fukushima, Bio.Cybernetics 36, 193–202 (1980)
Funk/Wenn, CR 2004

G.J. Leasing Co. v. Union Elec. Co. (1995) 54 F. 3d 379, 386 (7th Cir. 1995).
Gasser, VKU 2009, 224.
Geminn, ZD 2021, S. 354.
Generative AI: a game-changer society needs to be ready for. In: World Economic Forum.
Giedke, Cloud Computing: Eine wirtschaftliche Analyse mit besonderer Berücksichtigung des Urheberrechts, München 2013, 402 ff.
Giedke, S. 382 ff.
Gigerenzer, G./ Todd, P. M.; ABC Research Group: Simple heuristics that make us smart. Oxford University Press, New York 1999.
Gleß/Weigend, ZStW 126, 2014, 561, 585 f.
Gola in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Aufl. 2022, Art. 4 Rz. 35.
Gola/Heckmann/Schulz, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 152 mit Hinweis auf die Stellungnahme der EU-Kommission.
Gola/Schomerus, BDSG,11. Aufl. 2012, § 3 Rz. 21, 26.
Görgülü et al., BKR 2024, S. 175.
Grätz, Künstliche Intelligenz im Urheberrecht, 2021, S. 10
Greger, NZV 2018, 1 ff.
Grigoleit/Herresthal, BGB AT, 3. Aufl. 2015, Rn. 6
Groß, InTeR 2018,
Groß, Kapitalmarktrecht: Kommentar zum Börsengesetz, 6. Auflage 2016, § 26d Rn. 1. – 4.
Groß/Gressel, NZA 2016

Grosskopf, L. : IPRB 2011, S. 259 (259);
Gruber, in Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 123, 156, 198
Grundmann, in: Münchener Kommentar BGB Bd. 2: Schuldrecht Allgemeiner Teil (§§ 241 - 432), 7. Aufl. 2015, § 276 Rn. 150 bis 163.
Grunsky, NJW 1983, 2465.
Grünvogel, MDR 2017, 973, 974.
Grützmacher in Wandtke/Bullinger, UrhG, 6. Auflage 2022, § 69 c
Grützmacher, CR 2011
Grützmacher, CR 2015
Grützmacher, CR 2015, 779-787
Grützmacher, CR 2016
Grützmacher, M. in: Wandtke, A. / Bullinger, W.: UrhG, 4. Aufl. 2014, § 69a,
Günther/Böglmüller, BB 2017, 53 bis 58.

Haberstumpf in Lehmann, Kap. II, Rz. 15, 30
Hägele/Schäfer, in: Gevatter/Grünhaupt (Hrsg.), Handbuch der Mess- und Automatisierungstechnik in der Produktion, 2006.
Hagemeier, BeckOK UrhR, 38. Ed. 01.02.2023, UrhG § 44b Rn. 1.
Hager, in: Staudinger, BGB, 2009, § 823 Rn. 26, je m. w. N.
Hanisch, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014
Harris, „The Fear Index" 2011
Härting, ITRB 2016, S. 209–211.
Hartung, J. in: Kühling, J.; Buchner, B.: DS-GVO/BDSG, 2. Aufl. 2018, Art. 28, Rn. 22.
Hauck, R.: NJW 2014, S. 3616 (3616)
Heckmann, D. in: Heckmann, D.: jurisPK-Internetrecht, 5. Aufl. 2017, Kap. 9 1. Überarbeitung Rn. 214.
Heine/Frank, NZA 2023, S. 1281.
Heinz, Deep Learning – Teil 1: Einführung, Fn. 11.
Herbst in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, zu den einzelnen Vorgängen.
Herfurth ZD 2018, 514 (517)
Hermeier et al., 2018, S.10
Hessel/Dillschneider, Datenschutzrechtliche Herausforderungen beim Einsatz von KI, RDI 2023, 459, 461
Hessel/Dillschneider, RDI 2023, 458, 460.
Hetmank, S. / Lauber-Rönsberg, A. in: GRUR 2018, S. 574.
Heun, W.: Art. 3, Rn. 70–71. In: Dreier, H. (Hrsg.): Grundgesetz Kommentar: GG. 3. Auflage. Band I: Präambel, Artikel 1–19. Tübingen, Mohr Siebeck 2013
Heydn, MMR 2020, 435
Heymann, GRUR 2012, 814 (815 Rz. 39, 42 f.)
Heymann, in: CR 2016, S. 650–657 (650).
Hieke, R. in: InTeR 2017, S. 10, 11 f.; zu §§ 377, 381 Abs. 2 HGB
Hiéramente, BeckOK GeschGehG § 2
Hilber/Paul/Niemann, Teil 3, Rn. 94
Hilgendorf, in: Beck (Hrsg.), Jenseits von Mensch und Maschine, 2012, S. 119, 125 ff.
Hilgendorf, JZ 2021, S. 444 (447)
Hoeren, IT Rechtskript, Stand Okt. 2018,
Hoeren, IT Vertragsrecht 2018,
Hoeren, IT-Recht Stand Okt. 2018, S. 184.
Hoeren, MMR 2016, 8, 10
Hoeren, RdV 1988, 115, 119
Hoeren, Softwarehaftung innerhalb der Europäischen Gemeinschaft, in: Handbuch der modernen Datenverarbeitung, Heft 146/1989, 22, 30 f.
Hoeren, T. in: CR 2004, 721–724.
Hoeren, T.; Völkel, J. in: Hoeren, T.: Big Data und Recht, 2014, S. 22.
Hoeren, T.; Wehkamp, N. in: CR 2018, S. 1–7.
Hoeren/Sieber/Holznagel MMR-HdB, Teil 29 Rn. 17, beck-online
Hoeren/Wehkamp, CR 2018, 1-7.

Honsell, in: Staudinger, BGB 13. Bearb. § 463 (a. F.) Rn. 48 ff
Hoppen, P. in: CR 2015, S. 802 (803)
Horner/Kaulartz, CR 2016, 7.
Horner/Kaulartz, InTeR 2016, 22, 24.
https://www.zeit.de/news/2021-10/09/von-ki-vollendete-10-sinfonie-von-beethoven-uraufge-fuehrt?utm_referrer=https%3A%2F%2Fwww.google.com%2F
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2,
https://www.bafin.de/SharedDocs/Downloads/DE/dl_bdai_studie.html, abgerufen am 17. Dezember 2018.
https://www.kaggle.com/c/titanic (zuletzt abgerufen am 03.03.2020)
http://www.patentochmarknadsoverdomstolen.se/Domstolar/pmod/2018/Svea%20HR%20PMT%2022-17%20Ej%20slutligt%20beslut%202018-04-03.pdf (letzter Abruf jeweils 10.12.2018), s. Rz. 19.
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_DE.pdf.
https://www.heise.de/hintergrund/Was-darf-KI-Stockfotograf-und-KI-Verein-streiten-um-das-Copyright-8984836.html (abgerufen am 06.07.2023).
https://www.schufa.de/ueber-uns/presse/pressemitteilungen/schufa-loescht-restschuldbefreiung-sechs-monaten/ (abgerufen am 07.07.2023).
https://www.bearingpoint.com/files/BEDE13_0887_FC_DE_Hochfrequenzhandel_final_web.pdf, abgerufen am 24. Oktober 2018.
http://blog.audi.de/2015/05/26/per-autopilot-durch-die-megacity-shanghai/ (zuletzt abgerufen am 24.01.2016).
http://de.wikipedia.org/wiki/Software_as_a_Service (abgerufen am 28.10.2022).
https://de.serlo.org/informatik/baustelle/algorithmen-ist-algorithmus, abgerufen am 03.03.2020.
https://de.wikipedia.org/wiki/Chatbot, abgerufen am 11.10.2024.
https://de.wikipedia.org/wiki/Gewissen, abgerufen am 11.10.2024.
https://de.wikipedia.org/wiki/Maschinelles_Lernen
https://developers.google.com/search/docs/crawling-indexing/robots/intro?hl=de (abgerufen am 06.07.2023).
https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A31996L0009 (abgerufen am 06.07.2023).
https://laion.ai/about/ (abgerufen am 06.07.2023).
https://saasoptics.com/saaspedia/saas-subscription-models/ (abgerufen am 28.10.2022).
https://www.alamy.com/enterprise/ (abgerufen am 06.07.2023).
https://www.alltageinesfotoproduzenten.de (abgerufen am 06.07.2023).
https://www.bdzv.de/service/presse/branchennachrichten/2023/wiener-erklaerung-deutschsprachige-verlegerverbaende-verabschieden-gemeinsamen-forderungskatalog?sword_list%5B0%5D=Lizenz&no_cache=1 (abgerufen am 06.07.2023).
https://www.gettyimages.com/photos/holding (abgerufen am 06.07.2023).
https://www.heise.de/newsticker/meldung/Algorithmen-und-Scoring-Maas-fordert-digitales-Anti-Diskriminierungsgesetz-3761722.html?seite=2, abgerufen am 11.10.2024.
https://www.mind-verse.de (abgerufen am 06.07.2023).
https://www.mvfp.de/nachricht/artikel/tagesspiegel-verlage-fordern-lizenzgebuehren-wegen-chatbot-suchmaschinen (abgerufen am 06.07.2023).
https://www.profifoto.de/szene/notizen/2023/02/21/laion-droht-kneschke/ (abgerufen am 06.07.2023).
https://www.europarl.europa.eu/committees/de/juri/subject-files.html?id=20150504CDT00301, zuletzt abgerufen am 27.07.2018.
htpps://www.openai.com (abgerufen am 06.07.2023); www.businessinsider.com (abgerufen am 06.07.2023)
http://www.unece.org/trans/conventn/legalinst_08_RTRSS_RT1968.html abrufbar (zuletzt abgerufen am 24.01.2016).
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2,
https://www.archives.gov/milestone-documents/14th-amendment]
https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/

https://gemini.google.com/app
https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/
https://noyb.eu/de/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai
https://treaties.un.org/doc/Publication/CN/2015/CN.529.2015.Reissued.06102015-Eng.pdf (Stand: 05.02.2016).
https://www.bast.de/DE/BASt/BASt_node.html;jsessionid=905ABC3FD1F06FA5F8CD8E1F99925695.live2051 (zuletzt abgerufen am 24.01.2016).
https://haerting.de/wissen/ki-und-haftung-in-der-praxis-ein-ueberblick/
https://www.unece.org/leginstr/cover.html (zuletzt abgerufen am 29.12.2015).
http://t3n.de/news/facebook-ki-bilderkennung-chrome-781194/, abgerufen am 11.05.2020.
https://www.heise.de/ct/ausgabe/2017-11-Kuenstliche-Intelligenz-macht-Bildbearbeitung-intuitiv-3705914.html, abgerufen am 11.05.2020.
http://www.grur.org/de/stellungnahmen.html; a. A. *Redeker*, *S. S.*; *Pres*, *S.*; *Gittinger*, *C.*: WRP 2015, S. 681, Rn. 7.
https://www.golem.de/news/google-brain-algorithmus-macht-ge-sichter-auf-schlechten-bildern-erkennbar-1702-126066.html, abgerufen am 11.05.2020; https://netzpolitik.org/2016/verpixelung-macht-unsichtbar-oder-doch-nicht, abgerufen am 11.05.2020
https://www.heise.de/newsticker/meldung/eBay-Produkte-mithilfe-von-Fotos-suchen-und-kaufen-3784371.html, abgerufen am 11.05.2020.

ISO 10218-1 „Robots and robotic devices – Safety requirements for industrial robots – Part 1: Robots"
ISO 10218-2 „Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration".
ISO/DIS 13482 „Robots and robotic devices – Safety requirements for non-industrial robots – Non-medical personal care robot"
ISO/TS 15066 „Robots and robotic devices – Safety requirements for industrial robots – Industrial collaborative workspace"
Israel, JW 1902, 238, 240

Jaeger, CR 2002, 309 (311)
Jänich/Schrader/Reck, NZV 2015
Jarass, H.: Art. 3, Rn. 1b. In: Jarass, H.; Pieroth, B.: Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 28. Auflage, C. H. Beck, München 2014.
Jaskulla, BKR 2013, S. 221
Jauernig, Kommentar zum BGB, 7. Aufl. 2010
Junker, Computerrecht, 3. Aufl. 2003
Junker, WM 1988, 1217 ff., 1249 ff.

Käde, Kreative Maschinen und Urheberrecht, 2021, S. 183
Kalbfus, B.: GRUR 2016, S. 1009.
Kamanabrou, RdA 2006, S. 321, 338.
Karl, C.: Der urheberrechtliche Schutzbereich von Computerprogrammen, 2009, S. 191 f.
Kasiske, WM 14, 1933, Kindermann/Coridaß ZBB 14, 178.
Katharina Miklis: Aus Bielefeld? Das gibt's doch nicht! In: der Freitag. 7. April 2010.
Katharina Zweig: Die KI war's!: Von absurd bis tödlich: Die Tücken der künstlichen Intelligenz
Kersten, JZ 2015
Kindermann, Coridass, ZBB 2014, S. 178
Kirchner, InTeR 2018,
Kirsch, CT Magazin für Computertechnik Nr. 22, 2011, 43.
Kischel, U.: Art. 3, Rn. 91. In: Beck'scher Online-Kommentar GG, 34. Auflage 2017
Kitz, in: Hoeren/Sieber/Holznagel, Teil 13.1 Rn. 37.
KI-VO S.14 21.04.2021.
Klein, DSRITB 2015, 429, 438.
Klindt, BB 2009, 792, 793
Koch, AcP 203, 2003, 603, 624 ff., 631 f.
Koch, Computer-Vertragsrecht, 6. Aufl. 2002, Rn. 1346.

Koch, CR 2001, 574.
Koch, NJW 2004, 801, 802
Koch, Versicherbarkeit von IT-Risiken, 2005, Rn. 185 ff., 355 ff., 632 ff.
Köhler, AcP 182, 1982, 126
Köhler, AcP 182, 1982, 126, 135.
Koziol, ÖBA 1987, 3
Kriesel, A Brief Introduction to Neural Networks. (1.7.2024).
Krystal Hu, ChatGPT sets record for fastest-growing user base - analyst note. In: Reuters. 2. Februar 2023 (reuters.com [abgerufen am 12. Juli 2023]).
Kühling, NJW 2017, S. 1985, 1988.
Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 441.
Kuhnert, in: Haus/Krumm/Quarch, Gesamtes Verkehrsrecht, 2. Aufl. 2017, § 7 StVG Rn.
Kuschel/Asmussen/Golla/Hacker, Intelligente Systeme – Intelligentes Recht, 2021, S. 227 ff.

Lange, NZV 2017, 345.
Larenz, Allgemeiner Teil des deutschen Bürgerlichen Rechts, 1960, § 19 I.
Larenz, Methodenlehre der Rechtswissenschaft, 6. Aufl. 1991, S. 5
Laurin Meyer: ChatGPT erreicht die nächste Entwicklungsstufe. Die Welt, 17. März 2023. Seite 10.
LeCun et al, Gradient-Based Learning Applied to Document Recognition, Proc. of the IEEE, November 1998.
Leipold, BGB I, Einführung und AT, 9. Aufl. 2017, § 10 Rn. 17.
Leistner, FS Dreier 2022, 87 (90 f.)).
Lesshafft, K. / Ulmer, D. in: CR 1993, S. 607 (608)
Lewke, InTeR 2017, 207 bis 216.
Liebing, BB 1983, 667
Lippert, in: Deutsch/Lippert/Ratzel/Tag, MPG, 2. Aufl. 2010, § 2 MPBetreibV Rn. 1 ff.
Loewenheim in Schricker/Loewenheim, UrhR, 6. Aufl. 2020, § 69a, Rz. 2
Loewenheim, U. / Spindler, G. in: Schricker, G. / Loewenheim, U.: UrhG, 5. Aufl. 2017, § 69a, Rz. 5.
Lohmann, ZRP 2017, 168, 169.
Luhui Hu: Generative AI and Future. In: Medium. 15. November 2022.
Lutz, DAR 8/2014, 446, 448.
Lutz, NJW 2015
Lutz, Softwarelizenzen und die Natur der Sache, München 2009, 164 f.
Lutz/Tang/Lienkamp, NZV 2013, 57, 61.

Mansel, in: Jauernig, § 611 BGB Rn. 13
Markets in Financial Instruments Directive II – MiFID II
Marly, GRUR 2012,
Marly, in: GRUR 2011
Marly, J.: Praxishandbuch Softwarerecht, 5. Aufl. 2009, Rn. 398.
Marly, Praxishandbuch Softwarerecht, 6. Aufl. 2014, Rn. 1861
Marly, Praxishandbuch Softwarerecht, 7. Aufl. 2018, Rz. 1087
Marly, Softwareüberlassungsverträge, 7. Aufl. 2018,
Martin, Sachversicherungsrecht, 4. Aufl. 2022, Abschnitt B III Rn. 4.
Martini in: Paal/Pauly, DS-GVO BDSG, Art. 22, Rn. 15
Martini, JZ 2018, 1017 bis 1025.
Mattig, WM 2014, S. 1940.
Matusche-Beckmann, in: Staudinger, 15. Aufl. 2014, § 434 Rn. 73
Mayiner, Die künstliche Person, 2017,
Medicus, Bürgerliches Recht. 30. Aufl. 2025, Rn. 45.
Mehlhorn, K. / Sanders, P.: Algorithms and Data Structures, 2008, S. 26.
Meier/Wehlau, CR 1990, 95, 97
Mestmäcker/Schulze/Haberstumpf § 69a Rz. 3; auf DIN 44300

Milstein/Lippold, NVwZ 2013, 182, 184 f.
MMR, „Künstliche neuronale Netze: Wie KI-Lernstrukturen rechtlich zu betrachten sind“ 2021, 111
MMR-Aktuell 2023, 456626.
Möhring, P. / Nicolini, K.: Urheberrechtsgesetz, 2. Aufl. § 69a, Rz. 9.
Molitoris, NJW 2009, 1049, 1050 f.
Moorstedt, Intelligenz außer Kontrolle, SZ.de vom 11.10.2018, abgerufen am 24.10.2018.
Mortenson v. Timberline Software Corporation, Supreme Court of Washington (140 Wash. 2.d. 568, 998 P.2d 305).
Möschel, AcP 186, 1986, 187, 197 ff.
MüKo/Wendehorst, BGB, 9. Aufl. 2022,
Müller-Glöge, in: MüKo-BGB, 6. Aufl. 2012, § 611 BGB Rn. 23
Müller-Hengstenberg/Kirn, MMR 2014, 307, 311
Müller-Hengstenberg/Kirn, NJW 2014, 307, 311.
MünchKomm-BGB/Thüsing, 5. Aufl. 2007, § 20 AGG Rn. 55

Nägele/Jacobs, ZUM 2010, 281 (286)
Nielsen, M.: Neural Networks and Deep Learning. Determination Press, http://michaelnielsen.org, abgerufen am 11.05.2020.
Niemann, CR 2009, 661 (662 f.)
Niemann, in Hilber, Handbuch Cloud Computing, Köln 2014, S. 290 und 293
Niemann/Paul, K&R 2009, 444 (448)
NJW 2018, 2956 = MDR 2018, 1116
NZI 2023, S. 399.

Obergfell FS Windbichler, 2020, S. 1397 (1403 f.)
Oellinger, in: Achleitner/Everling (Hrsg.), Rechtsfragen im Rating, 2005, S. 360.
Oetker, in: MüKo/BGB, 4. Aufl., § 249
Oetker, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 2: Schuldrecht Allgemeiner Teil, 7. Auflage 2015, § 249 Rn. 96.
Olbrich/Bongers/Pampel GRUR 2022, 870
Osborne Clarke: Analyse der neuen EU-Haftungsrichtlinien

Paal, JuS 2010, 953, 954 f.
Paal, ZfDR 2024, 129, beck-online.
Paal/Pauly/Martini, 3. Aufl. 2021, DS-GVO Art. 26 Rn. 19
Pahlow, L. in: JA 2006, S. 385 (385)
Palandt/Grüneberg, BGB, 72. Aufl. 2013
Palandt/Grüneberg, BGB, 83. Aufl. 2024
Palandt/Heinrichs, 67. Aufl. 2008
Palandt/Heinrichs, 72. Aufl. 2013
Palandt/Heinrichs, 77. Aufl. 2017
Palandt/Putzo, 77. Aufl. 2017, § 439 Rn. 3.
Palandt/Thomas, 77. Aufl. 2017, § 823 Rn. 4.
Patzak, A./ Beyerlein, T. in: MMR 2007, S.687 (688)
Paul/Niemann in Hilber, Handbuch Cloud-Computing, 1. Aufl. 2014, Teil 3
Peschel, C.; Rockstroh, S. in: MMR 2015, S. 571 ff. (572).
Peschel/Rockstroh, MMR 2014, 571, 576.
Peters, in: Staudinger, BGB 13. Bearb. § 635 (a. F.) Rn. 55.
Pick-a-Pic: An Open Dataset of User Preferences for Text-to-Image Generation – Stability AI.
Pieper, BB 1991, 985, 988
Pieper, InTeR 2018,
Pohle/Ammann, CR 2009, 273 (276)
Pohle/Ammann, K&R 2009, 625 (626).
ProdHaftG vom 15.12.1989, BGBl. I, S. 2198.
Pröless, in: Pröless/Martin, Versicherungsvertragsgesetz, 28. Aufl. 2010, § 1 AHB Rn. 15.

Prütting, H./Wegen, G./Weinreich, G.: BGB Kommentar, AGG § 19 AGG – Zivilrechtliches Benachteiligungsverbot, Rn. 7.
Pukas, GRUR 2023, 614
Puppe, Kleine Schule des juristischen Denkens, 2 . Aufl. 2011, S. 4.

Quelle: ChatGPT.
Quelle: LAION e. V.

Rashid, T.: Neuronale Netz selbst programmiert, 1. Auflage 2017
Raue/Hegemann, MAH UrhR, § 3 Urheberrechtliche Schranken, Rn. 40.
Rauer/Bibi BeckOK Urheberrecht, Götting/Lauber-Rönsberg/Rauer 41. Edition Stand: 15.02.2024 § 2
Rauer/Bibi, BeckOK UrhR UrhG § 2 Rn. 61.
Redaktion beck-aktuell, becklink 2026476.
Redeker, Handbuch der IT Verträge, 1.5 Rn. 27
Redeker, IT-Recht, 5. Aufl. 2012, Rn. 830
Reed, Product Liability for Software, in: Computer Law & Practice 4 (1988), 149 ff.
Reiter/Methner, in: Taeger (Hrsg.), Smart World - Smart Law?, 2016, S. 453, 458
Resuch/Weidner, Future Law, 2018
Richtlinie (EU) 2019/790, 96/9/EG und 2001/29/EG.
Richtlinie 2000/43/EG,
Richtlinie 2001/29/EG
Richtlinie 2004/112/EG
Richtlinie 2004/39/EG
Richtlinie 85/374/EWG
Riehm, ITRB 2014, 113.
Rimscha, M.: Algorithmen kompakt und verständlich – Lösungsstrategien am Computer, 4. Auflage 2017, S. 3.
RL 91/250/EWG v. 14.05.1991, ersetzt durch konsolidierte Fassung als RL 2009/24/EG
Rödl, F. in: Rust, U. Falke, J.: AGG, 2007, § 20 Rn. 26 f
Rohe, AcP 201, 2001, 118, 134 ff.
Roloff. BeckOK ArbR, AGG § 15 Rn. 1–3.
Roßnagel, NJW 2017, 10
Rüthers, Rechtstheorie, 4. Aufl. 2010, S. 25.
Rüthers/Fuscher/Birk, Rechtstheorie mit Juristischer Methodenlehre, 10. Aufl. 2018.

S. Beck, in: Spranger (Hrsg.), Aktuelle Herausforderungen der Life Sciences, 2010, S. 95, 102 ff.
S. Beck, JR 2009, 225, 229 f.
Saenger, in HK-BGB, 9. Aufl. 2017, § 434 Rn. 11.
Schack, GRUR 2021, 904, 907
Schade, ZD 2014, S. 306, 309,
Schaub, JZ 2017, 342, 348
Scheja, K. in: CR 2018, S. 485.
Schellhammer, Schuldrecht nach Anspruchsgrundlagen, 11. Aufl. 2021
Schellhammer, Schuldrecht nach Anspruchsgrundlagen, 8. Aufl. 2011
Schermaier, JZ 98, 857.
Schiek, D. in: Schiek, D.: AGG, 2007, § 20 Rn. 8;
Schiemann, in: Staudinger, BGB 13. Bearb., Vorbemerkung zu §§ 249 ff
Schild in BeckOK Datenschutzrecht, 48. Ed. 1.5.2024, Art. 4 DSGVO Rz. 36.
Schmidt, B./ Freund, B. in: ZD 2017, S. 14 (16)
Schneider, J. in: Schneider, J.: Handbuch EDV-Recht, 5. Aufl. 2017, G. Rz. 79
Schneider/Günther, CR 1997, 389 ff.
Schnitzler: Online-Kommunikation im Recruiting für KMU: Reifegrade von Employer Branding & Candidate Experience, Springer Gabler, 2020, S.24-25

Schreiben der BaFin vom 21. Mai 2013.
Schreiber, S. B.: Natürliche Intelligenz. Neuronen und Synapsen – alles nur ein organischer Computer? (Teil 1), c't – Magazin für Computertechnik, 1987 (4), S. 98 ff.
Schricker/Loewenheim, Urheberrecht, 6. Aufl. 2020, § 16, Rn. 21.
Schricker/Loewenheim/Loewenheim/Leistner Rn. 40
Schröder, Datenschutzrecht für die Praxis, 2. Aufl. 2016, Kapitel 3: Datenschutz in der Personalabteilung/Arbeitnehmerdatenschutz.
Schuhr, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 13, 17.
Schulte, NJW 2014, 1238, 1238
Schulte-Nölke, Karlsruher Forum 2015, 3 ff. m. w. N.
Schultheiß, WM 2013, S. 596
Schulz in Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz 3. Auflage 2022 Art. 6
Schulz, Verantwortlichkeit bei autonom agierenden Systemen, S. 104
Schuster/Reichl, CR 2010, 38 (40 f.)
Schweighofer, in: Schweighofer/Menzel/Kreuzbauer, Auf dem Weg zur ePerson, 2001, S. 45, 49 ff.
Siedersleben, J. (Hrsg.): Softwaretechnik, Hanser, 2003, S. 44 ff.
Sieg, BB 983,1187.
Silke Hahn: OpenAI stellt GPT-4 vor: Sprachmodell versteht jetzt auch Bilder. In: heise online (heise.de). 14. März 2023, abgerufen am 15. März 2023.
Simitis: BDSG, 8. Aufl. 2014, § 3 Rz. 102.
Söbbing, „Das Märchen vom bösen Algorithmus oder rechtliche Fragen zur Diskriminierung durch künstliche Intelligenz (KI)" RTLaw 2020, 62–69.
Söbbing, Fundamentale Rechtsfragen künstlicher Intelligenz, 1. Auflage 2019, S. 11-14.
Söbbing, Fundamentale Rechtsfragen Künstlicher IntelligeSöbbing, in: CR 2020, S. 223–228.
Söbbing, InTeR 2018, S. 64-67.
Söbbing, ITRB 2018, 161 bis 163.
Söbbing, ITRB 2021, 168–171.
Söbbing, ITRB 2024, 184.
Söbbing, Möglicher Rechtsschutz von KI-Output nach dem UrhG oder GeschGehG - Genießt der Output von Generativen Chatbots wie ChatGPT einen rechtlichen Schutz? ITRB 2024, 184 - 188
Söbbing, Rechtliche Grenzen für KI-Entscheidungen im Rahmen des autonomen Fahrens, RDi 2023, 239
Söbbing, Verabschiedung der europäischen KI-Verordnung – Darstellung wesentlicher Punkte der KI-VO und Kritik ITRB 2024, 108 – 111.
Söbbing/Schwarz, in Recht der Datenverarbeitung Beck-Verlag, ZD 2023, 579.
Söbbing/Schwarz, Urheberrechtliche Grenzen für lernende Künstliche Intelligenz" zu den Fragen des Text und Data Mining (§ 44b UrhG) RDi 5/ 2023, 415
Söbbing/Schwarz, Verstößt das Maschine Learning beim Auslesen des Internets gegen die DSGVO? ITRB 2024, 212 – 217.
Söbbing/Schwarz, ZD 2024, 160.
Sodtalbers, Softwarehaftung im Internet, 2006, Rn. 513, 518.
Soergel, in: Münchener Kommentar zum Bürgerlichen Gesetzbuch Bd. 5/1: Schuldrecht Besonderer Teil III/1, 7. Auflage 2017, § 635 (a. F.) Rn. 39 m. w. N.
Sosnitza, CR 2016, 764, 772
Späte, Kommentar zu den Allgemeinen Versicherungsbedingungen für die Haftpflichtversicherung, 1993, § 1 AHB Rn. 49.
Specht-Riemenschneider FS Taeger, S. 711 (717 f.)).
Spindler FS Schack 2022, S. 340 (343)
Spindler in Schricker/Loewenheim, UrhG, 6. Auflage 2020, § 69c, Rn. 41–41c.
Spindler in: BeckOK BGB, 40. Ed., Stand: 01.05.2016, § 827 BGB Rn. 1.
Spindler, CR 2015, 766 bis 776.
Spindler, GRUR 2016, 1112, beck-online.
Spindler, in: BeckOGK/BGB, § 823
Spindler, in: BeckOK BGB, 40. Ed., Stand: 01.05.2016, § 827 BGB Rn. 1.
Spindler, in: Hilgendorf (Hrsg.), Robotik im Kontext von Recht und Moral, 2014, S. 63, 66 f.
Spindler, in: Kullmann/Pfister, Produzentenhaftung, Produkthaftung im IT-Bereich, erscheint demnächst

Spindler, in: Lorenz, Karlsruher Forum 2010: Haftung und Versicherung im IT-Bereich, 2011, S. 26 ff.
Spindler, Roboter, CR 2015, 766 bis 776.
Spindler/Schuster/Spindler/Dalby, 4. Aufl. 2019, DS-GVO
Spindler: BeckOGK/BGB, § 823 Rn. 607.
Spiro, Die Haftung für Erfüllungsgehilfen, 1984, S. 209 ff.
Spoerr, BeckOK DatenschutzR 46. Ed. 1.5.2022, DS-GVO Art. 26 Rn. 17
Spoerr, W. in: Wolff/Brink, Beck'scher Onlinekommentar, Stand 01.11.2017, Art. 28 DSGVO, Rn. 30 f.
Sprau, in: Palandt – Kommentar zum BGB, 77. Aufl. 2017, § 1 ProdHaftG Rn. 17.
Staudenmayer, NJW 2023, S. 894, Rn. 8.
Staudinger/Coester/Waltjen, BGB, § 11 Nr. 6 AGBG Rn. 27
Steiner in C't 7/2023 16–17 (16).
Stiemerling, O. in: CR 2015, S. 762.
Stoffels, AGB-Recht, 5. Aufl. 2024
Stuurman, Product liability for software in Europe. A discussion of the EC-directive of 25 July 1985, in: Vandenberghe (Hrsg.), Advanced Topics of Law and Information Technology, Deventer 1989, 110, 112 ff.

T 1814/07, ABl. 2003, S. 352.
T 208/84, ABl. 1987, S. 14.
T 258/03
T 641/00
Taeger (Hrsg.), Internet der Dinge - Digitalisierung von Wirtschaft und Gesellschaft, 2015, S. 429, 436
Taeger, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 259 f.
Taschner, Produkthaftung, 1986, 84
Taschner/Frietsch, ProdHaftG, 2. Aufl. 1990, Einführung Rn. 89
Thomale, P.-C. in: Auernhammer, DS-GVO/BDSG, 5. Aufl. 2017, Art. 28, Rn. 8.
Thüsing, in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke, 41. EL April 2018, Rn. 18.
Tiedtke, in: FS Gernhuber, 1993, S. 471, 480 f.

Ulmer, ZHR 152, 564, 579
Ulmer/Brandner/Hensen, 4. Aufl. 1999, § 11

v. Bar, in: v. Bar, Produktverantwortung und Risikoakzeptanz, 1998, S. 29, 36.
v. Pentz, AfP 2017, 102, 115.
v. Welser GRUR-Prax 2023, 2023, 57 (58))
v. Westphalen, DB 1999, 1369, 1370
v. Westphalen, DB 2001, 799, 802.
Verhoeven, 2020, S. 103.
Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828
VkBl 1970, 797, 798 f.
Vogt, NZV 2003, 153
Voigt, P.: Sonstige branchenspezifische Vorschriften zur IT-Sicherheit. In: Voigt, P.: IT-Sicherheitsrecht, 1. Auflage 2018.
Volhard/Jang in W/B/A | KAGB § 36 Rn. 20-24 | 3. Auflage 2021

Wagner, in: MünchKomm/BGB, 6. Aufl. 2013, § 823
Walter, SVR 2006, 41, 69.
Wandtke/Bullinger/Bullinger Rn. 16a; Schmoll/Graf Ballestrem/Hellenbrand/Soppe GRUR 2015, 1041 (1042)).
Wandtke/Bullinger/Grützmacher, § 69c
Weichert, ZRP 2014, 168

Weidenkaff, in: Palandt, § 611 BGB Rn. 15 f.
Weise, P./ Brandes, W./ Eger, T./ Kraft, M.: Neue Mikroökonomie, Physica, Heidelberg 2005, S. 22.
Weisser/Färber, MMR 2015, 506, 511.
Wendehorst, Christiane: „Regulatorische Herausforderungen für KI-Produkte", MüKo-Digitalrecht, 2022.
Wendehorst, NJW 2016, 2609.
Wendehorst/Gritsch in: Omlor/Link, Kryptowährungen und Token, II. Datenschutzrechtlicher Befund, 2., aktualisierte und erweiterte Auflage 2023, Rn. 57.
Wendtland, BeckOK BGB47. Ed. 01.08.2018, BGB § 119 Rn. 28, 29.
Wendtland, in: Bamberger/Roth (Hrsg.), BeckOK BGB, 42. Edition Stand: 01.02.2017, § 130 Rn. 10.
Westermann, BGB, 7. Aufl. 2016, § 434 Rn. 18 f.
Wettig/Zehendner, AI Law 12, 2004, 111, 127 ff.
Whittaker, European Product Liability and Intellectual Products, in: LQR 105 (1989), 125, 138 ff.
Wiebe, CR 2013, 1; Grützmacher, Urheber-, Leistungs- und Sui-generis-Schutz von Datenbanken, 1999, 340 f.
Wiebe, Die elektronische Willenserklärung, 2002, S. 214 ff.
Wilke, Gewndolin/Bendel, Oliver: KI-gestütztes Recruiting - technische Grundlagen, wirtschaftliche Chancen und Risiken sowie ethische und soziale Herausforderungen, in: HMD. Praxis Der Wirtschaftsinformatik, Bd.59, Nr.2, 2022, doi:10.1365/s40702-022-00849-w, S.653
Wobst, NZA-RR 2016, S. 508. Abs. 5, BeckOK ArbR/Roloff, Rn. 33. §§ 31, 278 BGB
Wolf/Horn/Lindacher, AGB-Gesetz: Gesetz zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen, 4. Aufl. 1999, § 11 Nr. 6 AGBG
Wolff/Brink/v. Ungern-Sternberg in BeckOK Datenschutzrecht, 46. Ed. 1.11.2023, Norm
World Intellectual Property Organization, Weltorganisation für geistiges Eigentum
Wulf/Burgenmeister, CR 2015, 404

Yoav Goldberg, Reducing Hallucination in Language Models, veröffentlicht auf arXiv.org.

Zimmermann, The Law of Obligations, 1996, P. 1105 ff.
Zimmermann/Leenen/Mansell/Ernst, JZ 2001, 684, 690 f.
Zirn, Chatbots – was Unternehmen wissen müssen, CIO Magazin, 17.10.2017.
Ziwie Ji et al.: Survey of hallucination in natural language generation. In: ACM Computing Surveys, 55(12), S. 1–38, 2023 (englisch)
Zweig, K.: Ein Algorithmus kennt kein Taktgefühl, 1. Auflage 2019, S. 140 ff.

K. Stichwörterverzeichnis