

Haftung für Trainingsdaten Künstlicher Intelligenz

Prof. Dr. Herbert Zech*

Daten werden zunehmend für das Training Künstlicher Intelligenz (KI) eingesetzt. Dies birgt ein neues Schädigungspotenzial: Trainingsdaten können über den Einsatz von KI Schäden an Rechtsgütern Dritter verursachen. Damit stellt sich die Frage nach der möglichen Haftung von Datenlieferanten. Während das Produkthaftungsgesetz (ProdHaftG) nicht eingreift (mangels Produkts und mangels Haftung für Informationsgehalt), kommt eine Haftung nach allgemeinem Deliktsrecht durchaus in Betracht. Rechtspolitisch ist zu überlegen, ob besondere Regelungen, sei es zur Verschärfung oder zur Erleichterung der Haftung, erforderlich sind.

I. Einleitung

1In der Diskussion um die Regulierung von KI einerseits und den Zugang zu Daten, um diese zu trainieren, andererseits, wurde ein Aspekt bislang vernachlässigt: die Haftung der Datenlieferanten.¹ KI-Trainingsdaten haben ein anderes Schädigungspotenzial als Daten, die nur im Wege einer „herkömmlichen“ Big-Data-Analyse verwendet werden. Dies legt die Frage nahe, wie es sich de lege lata mit einer möglichen Haftung von Datenlieferanten verhält und ob de lege ferenda etwas daran geändert werden sollte.

2Der Beitrag möchte erste Überlegungen zu diesen Fragen liefern. Dazu soll zunächst dargestellt werden, wie sich die Möglichkeit einer Schädigung durch Daten durch KI verändert hat, sodann ein Überblick über einschlägige Haftungsnormen de lege lata gegeben und abschließend sowohl eine mögliche Verschärfung als auch eine mögliche Be-

Zech: Haftung für Trainingsdaten Künstlicher Intelligenz(NJW 2022, 502)

503

schränkung der Haftung von Datenlieferanten diskutiert werden.

II. Datenwirtschaft und Schädigung durch Daten

3Grundüberlegung ist der Umstand, dass die Lieferung von Daten, insbesondere KI-Trainingsdaten (KI verstanden als lernfähige IT-Systeme²), eine Handlung darstellt, die kausal zu einer Beeinträchtigung geschützter Rechtsgüter wie Eigentum oder Gesundheit führen kann. Der Sonderfall einer Schädigung in der Privatheit durch Verletzung datenschutzrechtlicher Normen, der auch zu einer Haftung nach Art. 82 DS-GVO führen kann, soll dagegen nicht weiter betrachtet werden.

1. Von Big Data zu KI-Training

4Die Kausalketten, die einer Schädigung durch Daten bzw. deren Lieferung zugrunde liegen, haben sich verändert. Grundsätzlich stellen Daten maschinenlesbar codierte Informationen dar,³ das heißt etwas Unkörperliches, das nur mittelbar zu einer Beeinträchtigung körperlicher Rechtsgüter führen kann. Man kann hier von informationeller Kausalität sprechen.

5Allerdings unterscheiden sich die Wertschöpfungsketten, in denen Daten genutzt werden, und damit die resultierenden Kausalketten, wenn man herkömmliche Big-Data-Anwendungen und KI-Anwendungen vergleicht.

6Ursprünglich wurden Daten als „Rohstoff“ verstanden, der durch Big-Data-Analysen neue Erkenntnisse liefert (zunächst Korrelationen, die als Grundlage für die Erkenntnis bislang unbekannter Kausalbeziehungen dienen können).⁴ Aus diesen Erkenntnissen können sich dann Innovationen ergeben, deren Anwendung letztlich positive oder negative Effekte mit sich bringen. Entscheidend ist, dass dabei ein menschlicher Analyst als Zwischenglied auftritt. Deliktsrechtlich bedeutet dies einen typischen Fall mittelbarer Kausalität, wobei der Einteilung in mittelbare und unmittelbare Kausalität im Hinblick auf die Prüfung von Verkehrspflichten ohnehin richtigerweise nicht die entscheidende Bedeutung zukommt.⁵

7Werden Daten zum Training von KI eingesetzt, ändert sich das Bild. Trainingsdaten haben unmittelbare Auswirkung auf das Trainingsergebnis, also die trainierte KI. Deren Einsatz kann dann positive oder negative Effekte bewirken. Die Innovation, trainierte KI, wird also ohne geistiges Dazwischentreten eines Menschen generiert. Mögliche Schäden treten dann durch deren Anwendung ein. Zwar ist immer noch eine Reihe von Akteuren an der Kausalkette beteiligt (Programmierer, Datenlieferant, Trainer, Betreiber) und es bleibt bei mittelbarer Kausalität, die Risikokontrolle liegt aber zu einem höheren Teil beim Datenlieferanten als bei einer klassischen Datenanalyse durch Menschen.

2. KI-Trainingsdaten als Informationsgut

8Bereits in der Diskussion um Big Data ist klargeworden, dass Daten, auch sogenannte Rohdaten, Gütercharakter besitzen. Es handelt sich um Informationsgüter. Für KI-Trainingsdaten gibt es hier einige Besonderheiten.

a) Informationsgehalt von Trainingsdaten

9Ein wichtiger Unterschied ist derjenige zwischen faktischer und potenzieller Information.⁶ Von faktischer Information kann man nur sprechen, wenn diese bereits menschliche Erkenntnis geworden ist, wenn also ein Informationsgut Erkenntnis von einem Akteur an einen anderen vermittelt (kommuniziert). Bei Rohdaten ist dies häufig gerade nicht der Fall, vielmehr werden sie automatisiert erhoben und häufig erst im Rahmen der Analyse zum Gegenstand eines menschlichen Bewusstseins. Dies gilt grundsätzlich auch für KI-Trainingsdaten.

10Allerdings ist in diesem Zusammenhang auf den Unterschied zwischen überwachtem und nicht-überwachtem Lernen hinzuweisen.⁷ Beim überwachten Lernen weiß der Trainer, welche Information sich in den Trainingsdaten verbirgt und was die KI durch sie lernen soll. Mit anderen Worten liegt hier in den Trainingsdaten bereits faktische Information vor. Gewonnen wird diese insbesondere durch Annotation der Daten, was häufig durch den Datenlieferanten bzw. auf dessen Veranlassung geschieht. Die Lieferung annotierter für das Training bestimmter Daten stellt damit eine gänzlich andere Aufgabe dar, als die Lieferung schlichter Rohdaten.

11 Die Annotation von Daten stellt auch ein wichtiges Geschäftsmodell dar. Ein Beispiel sind Daten für das Training von KI in der Medizin. Die Annotation kann hier nur durch medizinische Experten vorgenommen werden. Gleichzeitig haben Trainingsdatensätze im medizinischen Bereich auch ein besonders Risikopotenzial. Dies alles wirkt sich auf die noch zu erörternde Frage der erforderlichen Sorgfalt beim Inverkehrbringen solcher Datensätze aus, die objektiv für das Training hochriskanter KI bestimmt sind.

12Ergänzend sei noch darauf hingewiesen, dass es auch eine dritte Quelle für Trainingsdaten gibt, nämlich die künstliche Erzeugung durch Simulation. Dass sich dabei eine besonders große Risikobeherrschung ergibt, liegt auf der Hand.

b) Datenmärkte

13Blickt man auf die möglichen Datenlieferanten, so ist zunächst zwischen Daten der öffentlichen Hand und privaten Datenlieferungen zu unterscheiden. Erstere sind unter

Zech: Haftung für Trainingsdaten Künstlicher Intelligenz(NJW 2022, 502)

504

anderem Gegenstand des von der Europäischen Kommission vorgeschlagenen Data Governance Act⁸ und der Open-Data-RL.⁹ Für Letztere wird ein Vorschlag der Europäischen Kommission in Form des sogenannten Data Act erwartet. Datenlieferungen durch staatliche Akteure sollen hier aber ausgeblendet bleiben.

14Datenlieferungen (Datenhandel¹⁰) durch private Akteure geschehen auf Datenmärkten.¹¹ Dabei können Primär- und Sekundärmärkte unterschieden werden.¹² Auf Primärmärkten bieten die unmittelbaren Datenerzeuger Daten an, auf Sekundärmärkten werden diese weiter gehandelt. Wegen der besonderen Bedeutung der Aufbereitung von Rohdaten für das Training von KI (Kuratierung) dürften hier Sekundärmärkte eine große Rolle spielen. Möglicherweise wird sich die Lieferung von KI-Trainingsdaten als eigenes typisches Geschäftsmodell herausbilden. Auch wird man unterscheiden können zwischen der Erzeugung von Daten für das Training von KI als Hauptzweck und der Erzeugung von Daten, die nur als Nebenzweck geschieht oder zumindest nicht zum Zwecke der Verwendung als KI-Trainingsdaten geschieht.

15Ökonomisch gesehen geht es wie bei allen Gütern um die optimale Produktion und Allokation, wobei Kosten und Nutzen gegeneinander abzuwägen sind. Diese können als Ziele rechtlicher Regelungen dienen, wobei neben der utilitaristischen Wohlfahrtsoptimierung im Recht dem deontologisch begründeten Schutz individueller Freiheitsrechte eigenständige Bedeutung zukommt (was auch zu einer Begrenzung des Ziels der Wohlfahrtsoptimierung führt).

3. Regulierung von KI-Trainingsdaten

16Durch ihre große Bedeutung rücken KI-Trainingsdaten neben der eigentlichen KI als eigener Regulierungsgegenstand ins Blickfeld.¹³ Auch der von der Europäischen Kommission vorgeschlagene Artificial Intelligence Act enthält Vorschläge zur Regulierung von Trainingsdaten, die für das Training von Hochrisiko-KI-Systemen eingesetzt werden (Art. 10).¹⁴

17Eine umfassende Regulierung könnte sich verschiedener Instrumente bedienen, die entweder direkt oder indirekt Einfluss auf das Aktivitäts- und Sorgfaltsniveau von Datenlieferanten nehmen. Sie muss dabei nicht nur die Risiken, sondern auch die Chancen im Blick behalten und auf eine möglichst wohlfahrtsoptimale Datenverwendung (Erzeugung, Nutzung) zielen. Zu den möglichen Instrumenten gehören Ausschließlichkeitsrechte,¹⁵ Zugangsrechte, die sicherheitsrechtliche direkte Regulierung und nicht zuletzt auch das Haftungsrecht als indirekte Regulierung der Risiken.

18Auch die technische Standardisierung wird voraussichtlich eine große Rolle spielen, für das Recht etwa im Rahmen von Technikklauseln oder als Faktor bei der Bestimmung von

haftungsrechtlichen Sorgfaltspflichten. Dies alles ist aber, wie die Regulierung und Standardisierung von KI selbst, erst noch im Entstehen.

19Das Haftungsrecht stellt sich als wichtiges Instrument der indirekten Regulierung dar (ähnlich wie das Immaterialgüterrecht). Es sorgt durch die Internalisierung von Risiken für eine Anreizsetzung und beeinflusst so das Sorgfaltsniveau und – durch Gefährdungshaftungsregelungen – auch das Aktivitätsniveau.¹⁶

III. Haftung de lege lata

20Der Umstand, dass ein Lieferant von KI-Trainingsdaten einen höheren Einfluss auf das Risiko einer Schadensentstehung durch die Daten hat als der Lieferant von Daten, die nur für eine herkömmliche Datenanalyse bestimmt sind, gibt Anlass, über die mögliche Haftung nach geltendem Recht nachzudenken. Diese Frage stellt sich ergänzend zu den bereits intensiv diskutierten Fragen nach einer Haftung der Hersteller oder Betreiber von KI-Systemen. Zwar sind diese in der Kausalkette näher am letztlich auftretenden Schaden, unterbrechen aber dadurch nicht automatisch die Kausalkette. Eine rechtspolitische Frage ist, ob die mögliche Haftung der näherstehenden Akteure als Argument gegen eine Haftung der Datenlieferanten bzw. für deren Begrenzung herangezogen werden soll (dazu unter IV).

1. Vertragliche Haftung

21Wie in Fällen der Haftung für körperliche Produkte auch ist zunächst nach einer vertraglichen Haftung zu fragen. Hier bestehen einige Unterschiede zwischen körperlichen Produkten und Daten. Die Gemeinsamkeit besteht aber darin, dass es in der Regel zwischen dem ursprünglichen Lieferanten (Hersteller, Datenlieferant) und dem Geschädigten keine Vertragsbeziehung gibt.

a) Vertragsparteien

22Vertragsparteien der Datenlieferung sind einerseits der Datenlieferant, andererseits die KI-Trainer, die Daten für das Training einsetzen. In der Regel werden sowohl Datenlieferant als auch KI-Trainer unternehmerisch tätig. Datenlieferanten haben also eine gewisse Ähnlichkeit mit Zulieferern bei körperlichen Produkten (Hersteller eines Teilprodukts, §§ 1 III 1, 4 I 1 Alt. 3 ProdHaftG).

b) Vertragstypen

23Für Datenlieferungsverträge gibt es bislang keine gesetzliche oder durch die Rechtsprechung entwickelte Typisierung. Bislang wurde vor allem das Problem des „Bezahlens“ mit Daten durch Private („Dienste gegen Daten“¹⁷) thematisiert. Auch die Digitale-Inhalte-Richtlinie¹⁸ erfasst nach Art. 3 I zwar die Lieferung von Daten (als digitale Inhalte,

Zech: Haftung für Trainingsdaten Künstlicher Intelligenz(NJW 2022, 502)

505

Art. 2 Nr. 1), jedoch nur von Unternehmern an Verbraucher.

24Eine Typisierung könnte insbesondere im Hinblick auf die Pflichten des Lieferanten von KI-Trainingsdaten erfolgen. Diese würde sich, sofern keine entsprechende Leistungsbeschreibung vorgenommen wurde, nach dem vertraglich festgelegten Zweck (KI-Training, Art des KI-Trainings, Art der KI etc.) richten. Dabei kann eine Abstufung nach dem Grad der Kontrolle durch den Lieferanten vorgenommen werden.

25 Auch ist es denkbar, dass entweder der Lieferant bestimmte Garantien übernimmt oder umgekehrt, soweit zulässig, Haftungsausschlüsse vereinbart werden. Eine Besonderheit würden unentgeltliche Verträge (etwa im Rahmen des von der Kommission vorgeschlagenen „Datenaltruismus“¹⁹) darstellen, bei denen in Analogie zum Schenkungsrecht, § 521 BGB,²⁰ und zum Recht der Leihe, § 599 BGB, eine Haftungsreduktion in Betracht kommt („Datenschenkung“).

26 De lege lata dürfte die entgeltliche dauerhafte Überlassung von KI-Trainingsdaten als Kaufvertrag nach §§ 433, 453 I Alt. 2 BGB einzuordnen sein.²¹ Die Mangelhaftigkeit ergibt sich dann nach § 434 I BGB (vereinbarte Beschaffenheit, vertraglich vorausgesetzte Verwendung, gewöhnliche Verwendung), was den eben angestellten Überlegungen zu einer zukünftigen Vertragstypologie entspricht. Bei einer unentgeltlichen dauerhaften Überlassung dürfte ein Schenkungsvertrag vorliegen (als Zuwendung genügt nach § 516 I BGB, dass jemand aus seinem Vermögen einen anderen bereichert, womit auch unkörperliche Schenkungsgegenstände erfasst sind;²² allerdings muss beim Schenker Entreicherung eintreten²³), wodurch § 521 BGB auch direkt anwendbar sein kann. Bei Überlassungen auf Zeit bestehen jedoch die aus dem Immaterialgüterrecht hinlänglich bekannten Probleme mit der Qualifikation von Lizenzverträgen, die zwar Elemente der Miete und Pacht bzw. der Leihe enthalten, jedoch Verträge eigener Art darstellen.²⁴

c) Vertragsketten

27 Das Hauptproblem dürfte jedoch darin liegen, dass in der Regel keine Vertragsbeziehung zwischen Datenlieferant und Geschädigtem besteht. Wie bei typischen Produkthaftungsfällen scheiden daher auch bei „Informationsprodukthaftungsfällen“ vertragliche Ansprüche meistens aus.

2. Produkthaftung

28 Damit stellt sich die Frage, ob das ProdHaftG und die ihm zugrundeliegende Produkthaftungs-RL (RL 85/374/EWG) Anwendung finden können. Eine solche „Informationsprodukthaftung“ de lege lata begegnet zwei Schwierigkeiten: zum einen dem Produktbegriff, zum anderen der Fehlerhaftigkeit durch einen bestimmten Informationsgehalt.

a) Produktbegriff (Körperlichkeit)

29 Ein altes Problem ist die Frage, ob unter Produkt iSd § 2 ProdHaftG bzw. des Art. 2 ProdHaftRL auch unkörperliche Gegenstände außer der ausdrücklich genannten Elektrizität subsumiert werden können. Der Wortlaut (bewegliche Sache, movables) sowie der Umkehrschluss zur ausdrücklich genannten Elektrizität sprechen dagegen. Für Software, zu der es auch entsprechende Überlegungen de lege ferenda gibt, wird aber zutreffend eine Anwendung bejaht.²⁵ Der Grund dafür liegt in der Funktion der Produkthaftung, gerade vor technisch-körperlichen Schädigungen (Materie, Energie) zu schützen. Es geht um „das unserem Zeitalter fortschreitender Technisierung eigene Problem einer gerechten Zuweisung der mit der modernen technischen Produktion verbundenen Risiken“, wie der zweite Erwägungsgrund der Produkthaftungs-RL von 1985 formuliert. Nach Andreas Günther ist das „Leitbild“ der Produkthaftung die „direkte, physikalische Schädigung [...] durch industrielle Waren“²⁶. Dies rechtfertigt es, nicht nur klassische Software, sondern auch trainierte KI als Produkte zu qualifizieren, nicht aber sonstige Informationsgüter.²⁷ Datensätze sollten damit gerade nicht als Produkt eingeordnet werden.

b) Informationsvermittelte Schädigung (Haftung für Informationsgehalt)

30 Das korrespondierende Problem liegt in der informationsvermittelten Schädigung, die aktuell auch dem EuGH im Fall KRONE²⁸ zur Entscheidung vorliegt. Die Frage ist, ob ein Informationsgehalt ein Produkt fehlerhaft machen kann. Generalanwalt Hogan lehnt es in seinen Schlussanträgen ab, dass der „Anwendungsbereich [der Produkthaftungsrichtlinie] auf in einem beweglichen Produkt enthaltene Informationen erstreckt“²⁹ wird. Er zieht insbesondere einen Vergleich zu einer Fehlinformation über unkörperliche Kanäle wie Radio. Daher kommt er zutreffend zu dem

Zech: Haftung für Trainingsdaten Künstlicher Intelligenz(NJW 2022, 502)

506

Schluss, dass die Schadensverursachung durch fehlerhafte in einem Produkt verkörperte Information „keinen Schaden betrifft, der sich aus einem dem Produkt innewohnenden körperlichen Fehler ergibt“³⁰. Mit anderen Worten: Aus der Körperlichkeit des Produkts schließt er auf die notwendige Körperlichkeit des Fehlers, ein bloßer Informationsfehler (Produkt enthält fehlerhafte Information) genügt nicht. Vielmehr geht es dabei im Kern um eine Dienstleistung („Klage, die mit der Erbringung einer Dienstleistung – einer Verbraucherempfehlung in einer Zeitungskolumne – in Zusammenhang steht, die nicht die Zeitung als körperliches Produkt betrifft“).³¹ Der EuGH hat sich nunmehr der Einschätzung des Generalanwalts angeschlossen und – eng am Sachverhalt – entschieden, dass „ein Exemplar einer gedruckten Zeitung, die im Zuge der Behandlung eines Themas aus dem Umfeld der Medizin einen unrichtigen Gesundheitstipp zur Verwendung einer Pflanze erteilt, durch dessen Befolgung eine Leserin dieser Zeitung an der Gesundheit geschädigt wurde, kein ‚fehlerhaftes Produkt‘ im Sinne dieser Bestimmungen ist“.

c) Zugrundeliegendes Problem: Virtualisierung der Technik

31 Das Problem, das bereits der Diskussion um Software zugrunde liegt, ist die zunehmende Informatisierung bzw. Virtualisierung der Technik. Während zum Entstehungszeitpunkt der Produkthaftungs-RL Technik ganz überwiegend physikalisch-körperlicher Natur war (Einsatz von Materie und Energie), gewann die maschinelle Informationsverarbeitung immer mehr an Bedeutung und mit ihr die Möglichkeit einer unmittelbaren physischen Schädigung durch Information. Dies trifft für Software als maschinensteuernde Information zu und möglicherweise auch für trainierte KI (Modelle). Selbst wenn die Information, wie etwa bei trainierten künstlichen neuronalen Netzen, nicht symbolisch explizit vorliegt, kann sie doch unmittelbar maschinensteuernde Funktion haben und damit körperliche Rechtsgüter ohne Dazwischentreten eines Menschen schädigen.

32 Anders ist es bei einem Informationsgehalt, der seine Wirkung erst durch Dazwischentreten eines menschlichen Rezipienten entfalten kann. Hier steht aus produkthaftungsrechtlicher Sicht das Dienstleistungselement im Vordergrund. Es handelt sich nicht mehr um eine technisch, sondern um eine geistig vermittelte Schädigung. Sie entspricht gerade nicht dem Leitbild der Produkthaftung.

33 KI-Trainingsdaten stehen genau zwischen klassischen Datensätzen (die durch Menschen analysiert werden müssen) und Software (die unmittelbar Maschinen steuert). Sie entfalten ihre Wirkung ohne Dazwischentreten menschlicher Erkenntnis (wohl aber eines Trainingsvorgangs), steuern aber Maschinen nicht unmittelbar (das tut erst die trainierte KI). Bei annotierten Daten tritt der Informationsgehalt noch mehr in den Vordergrund. Insgesamt dürfte es richtig sein, die Schädigung durch einen semantischen Informationsgehalt

unabhängig von ihrer automatisierten Verwirklichung dem Produkthaftungsrecht zu entziehen.

3. Deliktische Verschuldenshaftung

34 Als Grundnorm bleibt die Haftung nach § 823 I BGB. Daneben ist auch eine Haftung nach § 823 II BGB denkbar, sofern entsprechende Schutzgesetze bestehen. Dabei ist vor allem an die direkte Regulierung von KI-Trainingsdaten zu denken, wie sie etwa von der Kommission in Art. 10 des Entwurfs für einen Artificial Intelligence Act³² vorgeschlagen wird. Solange aber keine entsprechenden Schutzgesetze bestehen, stellt § 823 I BGB das zentrale Haftungsrisiko für Datenlieferanten dar.

a) Pflichtwidrigkeit als entscheidende Stellschraube

35 Entscheidende Stellschraube für die Haftung nach § 823 I BGB ist die Verletzung einer Sorgfaltspflicht bzw. Verkehrspflicht, die bei unmittelbaren Schädigungen ohne Weiteres gegeben, bei mittelbaren Schädigungen eigens zu prüfen ist. Die Schädigung durch Daten ist ein typischer Fall der mittelbaren Schädigung. Das gilt nicht nur für Daten, die durch Menschen analysiert werden, sondern auch für KI-Trainingsdaten, da diese erst durch Training und Anwendung der KI zu einer Schädigung führen (s. oben II 1).

36 Bei der Bestimmung ist nicht auf die vertraglichen Pflichten im Rahmen der Datenlieferung abzustellen, sondern es geht um die objektiv gegenüber jedermann bei Inverkehrgabe von Daten bestehenden Pflichten. Werden sie nicht beachtet, kann man von fehlerhaften Daten bzw. von einem Datenfehler sprechen.

b) Verkehrspflichten beim Inverkehrbringen von Daten

37 Die konkreten Verkehrspflichten ergeben sich aus einer Abwägung des potenziellen gesellschaftlichen Nutzens und der damit verbundenen Risiken. Die in den Verkehr gegebenen Daten stellen eine Gefahrenquelle dar, deren Verwirklichung aber nur dann dem Datenlieferanten zugerechnet wird, wenn er im Rahmen der Abwägung zumutbare Maßnahmen zur Risikoverringerung unterlassen hat.

38 Zu den möglichen Pflichten gehört nicht nur Gewährleistung inhaltlicher Richtigkeit, sondern auch eine entsprechende Kennzeichnung der Trainingsdatensätze. Die inhaltlichen Anforderungen richten sich nach der objektiven Zweckbestimmung. Trainingsdaten für hoch-riskante KI-Systeme („Hochrisikodaten“) unterliegen damit höheren Sorgfaltsanforderungen als sonstige Daten.

39 Sorgfaltspflichten können sich auch aus dem regulatorischen Recht ergeben (hier wäre insbes. an Kennzeichnungspflichten de lege ferenda zu denken). Regulatorische Vorgaben sind zwar nicht allein bestimmend, spielen aber insbesondere als regelmäßige Mindestanforderung eine wichtige Rolle.³³ Gegenwärtig gibt es zwar noch keine entsprechende Regulierung, im von der Europäischen Kommission vorgeschlagenen Artificial Intelligence Act gibt es

Zech: Haftung für Trainingsdaten Künstlicher Intelligenz (NJW 2022, 502)

507

jedoch einen ersten Vorschlag. Eine beispielhafte Umschreibung möglicher Sorgfaltspflichten findet sich daher in Art. 10 des Vorschlags für einen Artificial Intelligence Act, der aus regulatorischer Sicht unter anderem fordert, dass Datensätze „subject to appropriate data

governance and management practices" (Abs. 2 S. 1) sowie „relevant, representative, free of errors and complete" (Abs. 3 S. 1) sein sollen.

c) Beweisprobleme

40Praktisch wird eine Haftung von Datenlieferanten häufig Beweisproblemen begegnen.³⁴ Dies mag zwar zunächst als gute Nachricht für Datenlieferanten erscheinen, bedeutet aber vor allem Rechtsunsicherheit.

41Hinzu kommt, dass durch Vernetzung multikausale Verursachungen auftreten können (so bei Datenlieferungen durch vernetzte IT-Systeme untereinander, etwa im Straßenverkehr).³⁵ Indra Spiecker gen. Döhmnn³⁶ spricht anschaulich von der „Teilnahme einer unüberschaubar großen Zahl an weiteren Teilnehmern mit unterschiedlicher bis höchst geringer Einflussnahme auf die Ausgestaltung und Durchführung". Hier ist rechtspolitisch zu fragen, ob und wie Haftungsregeln noch eine sinnvolle Steuerungswirkung entfalten können.

IV. Überlegungen zu möglichen Gesetzesänderungen

42Rechtspolitische Optionen können sowohl auf eine Verschärfung als auch auf eine Erleichterung der Haftung von Datenlieferanten zielen. Denkbar wäre als dritte Option auch eine Haftungsersetzung durch Unfallversicherung (etwa im Rahmen einer KI-Unfallversicherung).³⁷

1. Gefährdungshaftung für Hochrisikodaten

43Eine Haftungsverschärfung würde die Einführung einer Gefährdungshaftung, etwa für Hochrisikodaten, darstellen. Eine Gefährdungshaftung sollte jedoch bei demjenigen liegen, der ein Risiko – hier das Risiko von KI – am besten kontrollieren kann. Daher stellt sich die Frage, ob nicht eine Haftung des Programmierers oder des Trainers vorzugswürdig ist (Gefährdungshaftung der Herstellerseite).³⁸ Selbst wenn in bestimmten Fällen der Datenlieferant einen großen Einfluss auf das Risiko hat, werden die Anreize der Herstellerhaftung durch das vertragliche Verhältnis zwischen Trainer und Datenlieferant und die damit verbundene Regressmöglichkeit weitergegeben.

44De lege lata ist auch die richterrechtliche Entwicklung entsprechender Verkehrspflichten möglich, die für Hochrisikodaten ein entsprechend höheres Haftungsrisiko schaffen. Allerdings besteht dabei das Problem der Rechtssicherheit.

2. Haftungsbeschränkungen

45Insbesondere beim „altruistischen"³⁹ data sharing stellt sich die Frage nach möglichen Haftungsbeschränkungen. Für die vertragliche Haftung bestehen zwar bereits de lege lata die unter III 1 dargestellten Haftungsbeschränkungen. Diese entfalten aber keine Wirkung gegenüber Dritten.

46Es bleibt zudem der Umstand, dass in einer Reihe von Fällen der Datenlieferant die beste Möglichkeit der Risikokontrolle hat, das heißt den größten Einfluss auf das Risiko und auch den geringsten Aufwand der Risikovermeidung. Daher ist es zumindest diskussionswürdig, ob und in welchen Fällen Datenlieferanten vor einer Haftung geschützt werden sollen.

3. Haftungsersetzung

47Als dritte Option bliebe, Datenlieferanten vor einer Haftung zu schützen, ohne Geschädigten einen Ersatz abzuschneiden. Eine Haftungsersetzung könnte insbesondere

durch haftungsetzende Unfallversicherung geschehen (etwa im Rahmen einer KI-Unfallversicherung).⁴⁰ Dies schafft einerseits Rechtssicherheit und Anreize für das Teilen von Daten, andererseits muss darauf geachtet werden, dass nicht Anreize zu unnötig riskantem Verhalten geschaffen werden (moralisches Risiko).

V. Zusammenfassung

48 Im Rahmen der Regulierung von KI-Trainingsdaten kommt dem Haftungsrecht eine erhebliche Bedeutung zu. De lege lata besteht neben vertraglichen Ansprüchen vor allem die Möglichkeit einer Haftung nach § 823 I BGB. De lege ferenda ist zu entscheiden, welche Haftungsregelung – insbesondere auch im Zusammenspiel mit der Haftung von Herstellern und Anwendern der trainierten KI – rechtspolitisch sinnvoll ist.

* Der Autor ist Inhaber des Lehrstuhls für Bürgerliches Recht, Technik- und IT-Recht an der Humboldt-Universität zu Berlin und Direktor am Weizenbaum-Institut für die vernetzte Gesellschaft.

¹ S. aber Hacker ZGE 12 (2020), 239 (268).

² Zum Begriff der KI Zech Risiken digitaler Systeme: Robotik, Lernfähigkeit und Vernetzung als aktuelle Herausforderungen für das Recht, Weizenbaum Series #2, 2020, <https://doi.org/10.34669/wi.ws/2 mwN>; alle zitierten Internetseiten zuletzt abgerufen am 1.2.2022; für einen anwendungsorientierten KI-Begriff als Algorithmisches Entscheidungssysteme s. Kuschel/Asmussen/Golla/Müller/Kirchner/Schüßler Intelligente Systeme – Intelligentes Recht, 2021, S. 85, 86 ff.

³ Zum Datenbegriff Zech Information als Schutzgegenstand, 2012, S. 32 f.; ders. CR 2015, 137 (138); Specht CR 2016, 288 (290); Becker GRUR 2017, 346 (347); Steinrötter MMR 2017, 731 (732); ders. FS Jürgen Taeger, 2020, S. 491 (492 f.); Pertot/Hofmann Rechte an Daten, 2020, S. 9, 10 f.; Oster JZ 2021, 167 (168 ff.).

⁴ Zu Daten als „Rohstoff“ und zu Big Data Zech CR 2015, 137 (138).

⁵ Zur Unterscheidung von mittelbarer und unmittelbarer Kausalität bzw. dazu, dass es immer um die Verletzung von Verkehrspflichten geht, MüKoBGB/Wagner, 8. Aufl. 2020, BGB § 823 Rn. 6, 21, 26; Kötz/Wagner Deliktsrecht, 14. Aufl. 2021, 5. Kap. Rn. 17 f. und 29 ff.; Looschelders Schuldrecht BT, 16. Aufl. 2021, § 59 Rn. 4; Zech in Jahrbuch SGHVR 2016, 17 (25).

⁶ Dazu Zech Information als Schutzgegenstand, 2012, S. 15.

⁷ Zur Unterscheidung von überwachtem und nicht-überwachtem Lernen Zech Risiken digitaler Systeme S. 35 (o. Fn. 2).

⁸ Europäische Kommission, 25.11.2020, COM (2020) 767 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz). In Art. 15 ff. des Vorschlags sind aber Regelungen zum sog. Datenaltruismus enthalten, die auch private Akteure betreffen.

⁹ RL (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20.6.2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Neufassung).

¹⁰ Pertot/Sattler Rechte an Daten, 2020, S. 49, 51 ff.

¹¹ Zech GRUR 2015, 1151 (1153).

¹² Schweitzer/Peitz NJW 2018, 275 (275 f.).

¹³ Dazu Hacker ZGE 12 (2020), 239; ders. NJW 2020, 2142 (2144 f.).

¹⁴ European Commission, 21.4.2021, COM(2021) 206 final, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Art. 10 I.

15 Hacker GRUR 2020, 1025.

16 Grdl. dazu Wagner VersR 1999, 1441.

17 Metzger AcP 216 (2016), 817.

18 RL (EU) 2019/770 des Europäischen Parlaments und des Rates v. 20.5.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen.

19 Art. 2 Nr. 10, Art. 15 ff. des vorgeschlagenen Data Governance Act (Europäische Kommission, 25.11.2020, COM(2020) 767 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance). Art. 2 Nr. 10 definiert „Datenaltruismus“ als die Einwilligung betroffener Personen zur Verarbeitung der sie betreffenden personenbezogenen Daten oder die Erlaubnis anderer Dateninhaber zur unentgeltlichen Nutzung ihrer nicht personenbezogenen Daten für Zwecke von allgemeinem Interesse wie die wissenschaftliche Forschung oder die Verbesserung öffentlicher Dienstleistungen.

20 Die Analogiefähigkeit des § 521 BGB wird jedoch bezweifelt, MüKoBGB/Koch, 8. Aufl. 2019, BGB § 521 Rn. 8; Staudinger/Chiusi BGB, 2021, BGB § 521 Rn. 13.

21 Vgl. Metzger JZ 2019, 577 (578, 580).

22 Allerdings scheiden ideelle Güter aus, MüKoBGB/Koch BGB § 516 Rn. 5; Staudinger/Chiusi BGB § 516 Rn. 10. Datensätze dürften unabhängig von der Frage, ob an ihnen Ausschließlichkeitsrechte bestehen, als reelle Güter einzuordnen sein. Dafür spricht auch die Parallele zur kaufrechtlichen Einordnung sonstiger Gegenstände. Zur Unterscheidung von Ideal- und Realgütern Becker Absolute Herrschaftsrechte, iErsch.

23 MüKoBGB/Koch BGB § 516 Rn. 6; Staudinger/Chiusi BGB § 516 Rn. 15 ff. Die Daten müssten also beim Lieferanten gelöscht werden, was häufig nicht der Fall sein wird.

24 Vgl. zum parallelen Problem der Einordnung von Verträgen über die Bereitstellung digitaler Dienstleistungen nach der Digitale-Inhalte-Richtlinie Sattler CR 2020, 145 (147).

25 Wagner AcP 217 (2017), 707 (716 ff.); ders. VersR 2020, 717 (726); Zech Information als Schutzgegenstand, 2012, S. 342.

26 Günther Produkthaftung für Informationsgüter, Verlagserzeugnisse, Software und Multimedia im deutschen und US-amerikanischen Produkthaftungsrecht, 2001, S. 647. Er lehnt daher eine Haftung für semantischen Informationsgehalt ab (S. 646 ff.), befürwortet aber die Anwendung der Produkthaftung auf Software (S. 668 ff.).

27 Zech Gutachten A zum 73. Deutschen Juristentag, 2020, S. A 68 mwN. Auf die Dienstleistungselemente vieler KI-Applikationen als Hinderungsgrund für eine Einordnung als Produkt de lege lata weist Hacker ZGE 12 (2020), 239 (250) hin.

28 EuGH ECLI:EU:C:2021:471 = NJW 2021, 2015 mAnm Finkelmeier NJW 2021, 2017 – KRONE.

29 Schlussanträge des Generalanwalts Gerard Hogan v. 15.4.2021 ECLI:EU:C:2021:298 = BeckRS 2021, 7667 Rn. 30 – KRONE.

30 Schlussanträge des Generalanwalts Hogan Rn. 31.

31 Schlussanträge des Generalanwalts Hogan Rn. 42. Günther Produkthaftung für Informationsgüter, Verlagserzeugnisse, Software und Multimedia im deutschen und US-amerikanischen Produkthaftungsrecht, S. 19 ff., 646, spricht von kommunikativen Informationsgütern, die der Kommunikation (also der Übermittlung von Information zwischen Menschen) dienen und nicht als Produkt zu qualifizieren sind.

32 European Commission, 21.4.2021, COM(2021) 206 final, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Art. 10 I: „High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5.“ Dazu Grützmaker CR 2021, 433 (439 f.).

33 Hacker ZGE 12 (2020), 239 (268).

34 Zech Gutachten A zum 73. Deutschen Juristentag, 2020, S. A 58.

35 Zech ZfPW 2019, 198 (207); ders. Gutachten A zum 73. Deutschen Juristentag, 2020, S. A 57 f.

36 Spiecker gen. Döhmann CR 2016, 689 (701). Vgl. Teubner AcP 218 (2018), 155 (201 f.).

37 Dazu Zech Gutachten A zum 73. Deutschen Juristentag, 2020, S. A 107 ff.

38 Zu einer solchen Haftung de lege ferenda Wagner VersR 2020, 717 (734 f.); Zech Gutachten A zum 73. Deutschen Juristentag, 2020, S. A 87 ff., 98 ff. mwN.

39 Zum Konzept des Datenaltruismus Art. 2 Nr. 10, Art. 15 ff. des vorgeschlagenen Data Governance Act (Europäische Kommission, 25.11.2020, COM(2020) 767 final, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance) s. Fn. 19.

40 Dazu Zech Gutachten A zum 73. Deutschen Juristentag, 2020, S. A 107 ff.

□Verlag C.H.BECK oHG 2024