41. Jahrgang
Heft 16
17. April 2020/S. 737

Zeitschrift für Wirtschaftsrecht ZIP

Aufsätze

Friedrich Graf von Westphalen[*)]

Disruptive Technology Creates Disrupted Law

Künstliche Intelligenz (KI) – Dateneigentum, Haftung, Bilanzierung

Ziel der nachfolgenden Darlegungen ist es, auf Basis des gegenwärtig gültigen politischen Konzepts der EU-Kommission, für Europa die Rahmenbedingungen für eine datengetriebene Wirtschaft zu schaffen, der Frage nachzugehen, inwieweit bereits für wesentliche Fragen der Digitalisierung eine zureichende Antwort auf europäischer Ebene bereitsteht. Es geht dabei um das Dateneigentum an maschinengenerierten Daten, weil der bisherige, am Sacheigentum ausgerichtete Eigentumsbegriff (§ 903 BGB) nicht mehr passt. Auch soll die daran anschließende Frage vertieft werden, ob denn ein besonderes Haftungsregime in der EU einzuführen ist, um die besonderen, durch den Einsatz von KI – selbstlernende KI, neuronale Netze und Roboter – erzeugten Risikolagen zugunsten des Gemeinwohls zu beherrschen. Schließlich ist ein Blick auf die bislang weitgehend ausgesparte Frage zu werfen, welche Regeln denn in Geltung gesetzt werden könnten, um die Bilanzierung von maschinengenerierten Daten in verlässlicher Weise zu erreichen. Über allem aber steht die Aussage, die auch als Fragezeichen zu verstehen ist, ob denn die disruptiven Merkmale der Digitalisierung nicht auch ein Recht hinter sich lassen, welches mit den rasanten technischen Fortschritten nicht mehr Schritt hält.

I. Konzept der EU-Kommission

Ausgangspunkt der hier anzustellenden Erwägungen ist das Grundsatzpapier der EU-Kommission „Building a European Data Economy“,[1)] weil dort die wesentlichen rechtspolitischen Grundsätze festgehalten sind, welche die nächsten Jahre beherrschen werden. Der erste der dort genannten Grundsätze ist der des „free flow of data“.[2)] Denn nur auf diese Weise, so die Kommission, können die vier Grundfreiheiten des Lissabon-Vertrags – Freizügigkeit, Dienstleistungsfreiheit, Kapital- und Warenverkehrsfreiheit – in einem immer weiter auszubauenden Binnenmarkt geschützt und ausgebaut werden. Dabei betont die Kommission auch, dass Gesichtspunkte der Datensicherheit und die entsprechenden gesetzlichen oder verwaltungsrechtlichen Maßnahmen und Vorkehrungen nicht dazu beitragen dürfen, dass die Ansicht sich durchsetzt, dass eine solche „Lokalisation“ des Datensicherheitsrechts dazu führt, dass nationale Regeln als sicherer angesehen werden als europarechtliche, also solche, die grenzüberschreitende Funktionen erfüllen.[3)]

Sodann trifft die Kommission die auch für unsere Erwägungen wichtige Unterscheidung bei der Behandlung der durch das „Internet of Everything“ hervorgerufenen Rechtsfragen zwischen „personal“ – also: personenbezogenen – Daten im Sinn der DSGVO und „non-personal“.[4)] Doch die Differenzierung zwischen diesen ist nicht als abschließend zu verstehen, weil ja maschinengenerierte Daten jedenfalls dann im Ergebnis als „personenbezogene“ Daten zu qualifizieren sind, wenn nämlich die betreffende Person, die hinter diesen Daten steht, identifiziert werden kann. Die Kommission ist sogar der Auffassung, dass dieser Mischtyp von Daten im Blick auf Datentransfer und Zugang zu den Daten im Vordergrund steht.[5)] Das anzumerken ist rechtspolitisch von hoher Bedeutung. Denn die Kommission stellt fest, dass Unternehmen, welche große Datenmengen herstellen und so ihr Eigen nennen, diese in aller Regel auch selbst auswerten. Es findet also – regelmäßig in der Praxis geschützt durch Geheimhaltungsvereinbarungen – eine Begrenzung der Weiterverwertung dieser Daten auf der nächsten Stufe des „downstream“ statt.[6)]

*) *Prof. Dr. iur., Rechtsanwalt, Köln*

1) COM(2017) 9 final.
2) COM(2017) 9 final – S. 5; seit dem 19. 2. 2020 liegt ein „White Paper on Artificial Intelligence“ vor – COM(2020) 65 final; dieses ist eingebettet in ein weiteres Papier der Kommission mit dem Titel „A European Strategy for Data“ – COM(2020) 66 final. Beide Stellungnahmen konnten aus Zeitgründen nicht mehr beachtet werden; sie setzen jedenfalls im Blick auf die Strategie der Kommission betreffend die „European Data Economy“ neue Akzente.
3) COM(2017) 9 final – S. 6 f.
4) COM(2017) 9 final – S. 9.
5) COM(2017) 9 final – S. 9.
6) COM(2017) 9 final – S. 9.

Darauf schon an dieser Stelle zu verweisen ist deswegen von Erheblichkeit, weil die Kommission mit Recht anmerkt, dass die von Maschinen erzeugten Rohdaten nach geltendem Urheberrecht nicht Schutzobjekte[7] im Rahmen des europäischen Rechts sein können.[8] Das gilt auch für die Frage nach einem Dateneigentum. Zur Folge hat diese Konstellation, dass die Frage des freien Datenhandels sich weitgehend in vertraglichen Regeln erschöpft,[9] was – wie ohne weitere Anfrage einzuräumen ist – vor allem das Recht des wirtschaftlich Stärkeren im Rahmen meistens einseitiger Vertragsgestaltung bevorzugt.

Die Kommission sucht daher nach neuen Rechtsregeln, die sich, um nur das Wichtigste zu nennen, auf folgende Fragen beziehen:

Erstens, Verbesserung des Zugangs zu anonymen maschinengenerierten Daten; dabei sind die Stichworte: „sharing, reuse and aggregation".[10]

Zweitens, gleichwohl sollen Investitionen und vor allem auch die „assets" des Unternehmens geschützt werden, das innovativ in der Sammlung und Auswertung von maschinengenerierten Daten tätig wird. Doch dabei soll – und das weiter im Detail im Lauf des Gesetzgebungsverfahrens zu verfolgen wird spannend – in der Wertschöpfungskette sichergestellt werden, dass ein „fair sharing of benefits between data holders, processors and application providers" vorgenommen werden soll.[11]

Drittens, auf der Ebene des B2B-Verkehrs will die Kommission „default contract rules"[12] einführen, um eine ausgewogene Vertragsgestaltung abzusichern.[13]

Viertens, öffentliche Behörden sollen Zugang zu Daten – auch zu personenbezogenen Daten, nicht nur maschinengenerierten – erhalten, soweit diese von öffentlichem Interesse sind oder für wissenschaftliche Zwecke eingesetzt werden können.[14] Das ist, wie auf den ersten Blick erkennbar, ein unglaublich komplexes Feld, wenn man an die statistischen Verkehrsdaten, aber vor allem an den Datentransfer in der Pharmaindustrie oder im Bereich des Sozialen denkt, was die Kommission ausdrücklich ins Visier nimmt.

Fünftens, schließlich soll auch ein Zugang zu Daten ermöglicht werden gegen eine Art bezahlter Zwangslizenz (FRAND)[15] – fair, reasonable and non discriminatory.[16]

II. Dateneigentum

1. Bisheriger Schutz

Um in etwa nachzuvollziehen, dass und in welchem Maß die „data economy", basierend auf einer „disruptive technology"[17] die bestehenden Rechtsregeln in Frage stellt oder sogar außer Funktion bringt, ist es hilfreich, zunächst einen kurzen Blick auf den insoweit für das Dateneigentum bestehenden Rechtsschutz zu werfen.

1.1 § 202a StGB – § 303a StGB

An erster Stelle ist hier der strafrechtliche Schutz in den Blick zu nehmen, den § 202a StGB adressiert. Danach wird derjenige mit einer Freiheitsstrafe bis zu drei Jahren (oder Geldstrafe) bestraft, der sich oder einem anderen „unbefugt" den Zugang zu Daten „verschafft", „die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind", sofern er dies „unter Überwindung der Zugangssicherung" tut. Hier wird der Begriff „Daten" sehr weit verstanden; es unterfallen der Norm nicht nur personenbezogene Daten, sondern Informationen jeder Art, ohne dass ihnen ein Geheimnis zugrunde liegen muss.[18] Die kriminalpolitische Richtung von § 202a StGB liegt auf der Hand, weil der Schutz der Daten, die vor einem unberechtigten Zugriff besonders gesichert sein müssen, auf Hackerattacken gerichtet ist.[19]

Gleichrangig mit § 202a StGB gilt es, den Blick auf § 303a StGB zu richten. Danach wird mit Freiheitsstrafe bis zu zwei Jahren (oder Geldstrafe) bestraft, wer Daten „löscht, unterdrückt, unbrauchbar macht oder verändert". Schutzgut ist hier das Interesse des Berechtigten an der unversehrten Verwendbarkeit von Daten.[20] Das setzt – wie selbstverständlich – voraus, dass der so Geschützte ein unmittelbares Nutzungs- und Verfügungsrecht über die Daten in Händen halten muss.[21] Die Rechtsprechung spricht in diesem Kontext davon, dass der so durch die Norm Geschützte eine eigentümerähnliche Rechtsposition innehaben muss.[22]

1.2 § 17 UWG a. F. – § 4 GeschäftsgeheimnisG

Der früher geltende § 17 UWG schützte die unbefugte Weitergabe eines Geschäfts- oder Betriebsgeheimnisses durch einen Angestellten während seiner Dienstzeit. Der Zweck dieser mit einer Freiheitsstrafe bis zu drei Jahren (oder Geldstrafe) bewehrten Norm bestand darin, die Geheimhaltungsinteressen des Unternehmers, welche ja auch eine herausragende vermögensrechtliche Komponente aufweisen, zu schützen und damit auch – das war das zweite Ziel – die Interessen der Allgemeinheit am Bestehen eines redlichen und fairen Wettbewerbs zu schützen.[23]

Doch diese Vorschrift ist am 26. 4. 2019 aufgehoben worden, um die Umsetzung der bereits kurz gestreiften europarechtli-

7) Hierzu auch *Hugenholtz*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 75 ff.
8) COM(2017) 9 final – S. 10; ausgenommen ist das sui generis Schutzrecht der elektronischen und nicht elektronischen Datenbanken, welcher aber erhebliche Investitionen voraussetzt, hierzu *Gaster*, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 49. EL, 2019, Teil 7.6 Rz. 1 ff.; *Leistner*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 27 ff.; ausgenommen ist auch die RL 2016/943/EU betreffend die Wahrung von Geschäftsgeheimnissen, hierzu auch *Goldhammer*, NVwZ 2017, 1809 ff.; *Kalbfus*, GRUR-Prax 2017, 391 ff.; auch *Aplin*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 59 ff.
9) COM(2017) 9 final – S. 10.
10) COM(2017) 9 final – S. 11.
11) COM(2017) 9 final – S. 11.
12) Hierzu im Einzelnen, aber sehr skeptisch *Graf von Westphalen*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 245 ff.
13) COM(2017) 9 final – S. 12.
14) COM(2017) 9 final – S. 12.
15) COM(2017) 9 final – S. 13.
16) Hierzu auch *Kühnen*, GRUR 2019, 665 ff.; zur Frage der Bewertung, was denn FRAND ist, vgl. *Schaefer/Czychowski*, GRUR 2018, 532 ff.; im Übrigen *Weber*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 137 ff.
17) Hierzu *Twigg-Flessner*, in: De Franceschi, European Contract Law and the Digital Single Market, 2016, S. 1 ff.
18) Hierzu MünchKomm-*Graf*, StGB, 3. Aufl., 2017, § 202a Rz. 12.
19) *Weidemann*, in: BeckOK StGB, Stand: 1. 11. 2019, § 202a Rz. 12 ff.
20) MünchKomm-*Wieck-Noodt*, StGB, 3. Aufl., 2017, § 303a Rz. 2.
21) *Weidemann* (Fußn. 19), § 303a Rz. 5.
22) OLG Nürnberg BeckRS 2013, 3553, dazu EWiR 2013, 529 *(Floeth)*.
23) Hierzu *Rengier*, in: Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG, 3. Aufl., 2016, § 17 Rz. 4.

chen Geheimnisschutzrichtlinie 2016/943/EU[24] zu erreichen.[25] Dort heißt es dann in Art. 4 Abs. 1 des Gesetzes zum Schutz von Geschäftsgeheimnissen:[26] *„Ein Geschäftsgeheimnis darf nicht erlangt werden durch 1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt."*

Dabei wird – ausgehend von dem Begriff des Geschäftsgeheimnisses,[27] auch das Know-how,[28] also auch werthaltige Daten einer KI werden so erfasst – vorausgesetzt, dass die dem Geschäftsgeheimnis zugrunde liegende Information einen kommerziellen Wert für den Inhaber dieses Geheimnisses hat und nicht belanglos ist.[29] Das aber ist im Ergebnis kein rechtlicher Schutz, sondern einer, der ausschließlich auf dem Tatbestand des „geheimen Wissens" und letztlich auch auf vertraglichen Regelungen[30] aufruht.[31] Das wird auch in der Definition von Art. 4 Abs. 1 GeschäftsgeheimnisG deutlich. Dort ist das unbefugte Erlangen in Form des unbefugten Zugangs zu einem zu schützenden Geschäftsgeheimnis untersagt – ein Tatbestand, der am einfachsten mit „Betriebsspionage" gleichgesetzt werden kann.[32] Der gesetzliche verankerte Geheimnisschutz setzt jedoch voraus, dass der Inhaber der zu schützenden Daten nach § 2 Nr. 1 lit. b GeschäftsgeheimnisG „angemessene Geheimhaltungsmaßnahmen" trifft.[33]

Doch ist, von weiteren Details einmal abgesehen, deutlich zu machen: Der frühere Schutz des § 17 UWG zielte auf den strafrechtlichen Tatbestand. Dieser ist nunmehr stark in den Hintergrund getreten (vgl. § 23 GeschäftsgeheimnisG[34]); im Vordergrund der wettbewerbsrechtlichen Praxis stehen dabei die allgemeinen zivilrechtlichen Ansprüche, nämlich: der Anspruch auf Unterlassung, Beseitigung sowie der auf Ersatz des durch den Bruch des Geheimnisses entstandenen Schadens.[35] Der strafrechtliche Schutz ist jetzt in erster Linie eine Sache des Arbeitsrechts und hier vor allem beim Abwerben von Mitarbeitern.[36]

2. Zivilrechtliche Konsequenzen

2.1 Fragestellung

In Deutschland ist die rechtspolitische Debatte um die Begründung eines eigenständigen Eigentumstatbestands an maschinengenerierten Daten – also: ausgenommen personenbezogene Daten – nach wie vor im Gang. Im noch immer geltenden Koalitionsvertrag steht, dass diese Frage „zügig" anzugehen ist.[37] Im Mittelpunkt steht dabei die Antwort auf die Frage, ob denn ein so genannter sachenrechtlicher Eigentumsschutz an maschinengenerierten Daten (und einem Algorithmus) – außerhalb des bereits kurz angesprochenen Schutzes über das Geschäftsgeheimnis und den Schutz der vorgenommenen Investitionen im Rahmen der Datenbank-Richtlinie – anzuerkennen ist.

Das würde bedeuten, dass der Eigentümer der Daten, der im Zweifel auch der Besitzer ist (§ 1006 BGB), gegenüber jedermann geschützt ist und seinen Abwehranspruch daher auch gegen jeden, der einen Zugriff auf die Daten begehrt, erfolgreich abwehren kann. Dabei ist ein entscheidender Punkt hervorzuheben: Eigentumsrechte bestehen nämlich nur an Sachen, wie sich aus § 90 BGB ablesen lässt, was definitorisch einen „körperlichen Gegenstand" voraussetzt, was für Daten eben gerade nicht zutrifft. So besteht etwa ein Eigentumsrecht an einem Buch, nicht aber an den Informationen, die ein Dritter als Leser dieses (verliehenen) Buches sich aneignet.

Ähnlich ist es mit Urheberrechten. Um beispielhaft beim Buch als „Werk" zu bleiben, welches wegen seines geistigen Gehalts nach § 2 Abs. 2 UrhG[38] geschützt werden kann, bezieht sich dieser Schutz nur auf die „persönliche geistige Schöpfung", nicht aber auf die dem einzelnen Satz zugrunde liegenden Buchstaben oder Wörter. Von daher wird es verständlich,[39] dass auch maschinengenerierte Daten – auch und schon gar nicht der zugrunde liegende binäre Code – keinen urheberrechtlichen Schutz genießen.[40]

Das bedarf einer kurzen Erklärung. Daten sind nach der Definition der ISO[41] *„a reinterpretable representation of information … in a formalized manner suitable for communication, interpretation, or processing"*. Maschinengenerierte Daten, wie zum Beispiel von Sensoren erzeugte Daten, sind also allein deswegen nicht vom Urheberrechtsschutz erfasst, weil sie – in der Regel – automatisch generiert werden und damit keinen persönlichen geistigen Schöpfungsakt voraussetzen oder zum Gegenstand haben.[42]

Eine Ausnahme besteht allerdings nach §§ 87a und b UrhG für die Gesamtheit der Daten in einer Datenbank zugunsten ihres Herstellers.[43] Doch auch hier werden nicht die maschinengenerierten Daten als solche geschützt, sondern im Kern

24) ABl 2016 L 157, 3.
25) *Aplin* (Fußn. 8) S. 59, 62 ff.
26) Hierzu *Ohly*, GRUR 2019, 441 ff.; *Rosenkötter/Seeger*, NZBau 2019, 619 ff.; *Voigt/Grabenschröer*, BB 2019, 142 ff.
27) *„Geschäftsgeheimnis (ist) eine Information a) 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 b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht."*
28) *Nabert/Peukert/Seeger*, NZA 2019, 583 ff.
29) ErwG 14 der RL 2016/943/EU.
30) Hierzu eindrücklich *Mezger* zu den Mobilitätsdaten, GRUR 2019, 129 ff.
31) *Wiebe*, GRUR Int. 2016, 877, 880.
32) *Ohly*, GRUR 2019, 441, 446.
33) Zu Fragen der Compliance *Scholtyssek/Judis/Krause*, CCZ 2020, 23 ff.
34) *„Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,*
1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt."
35) *Ohly*, GRUR 2019, 441, 450.
36) *Nabert/Peukert/Seeger*, NZA 2019, 583, 587.
37) Koalitionsvertrag v. 12. 3. 2018 – Bundespresse- und Informationsamt – pdf.
38) *„Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen."*
39) *Wiebe*, GRUR 2017, 338 ff.
40) Statt aller *Determann*, ZD 2018, 503, 505; *Thalhofer*, GRUR-Prax 2017, 225, 226.
41) ISO/IEC 2382-1 (1993).
42) *Wiebe*, GRUR Int 2016, 877, 879.
43) Vgl. auch *Kraul*, GRUR-Prax 2019, 478.

die Investition des Herstellers in die Herstellung einer Datenbank,[44] was auch als sui generis-protection bezeichnet wird.

Zu ergänzen bleibt freilich, dass Computerprogramme nach § 2 Abs. 1 Nr. 1 UrhG zu den geschützten Werken zählen,[45] was sich auch in den Normen der §§ 69a ff. UrhG niederschlägt. Nach einer gängigen Definition des OLG Hamburg ist ein Computerprogramm *„ein Satz von Anweisungen an ein informationsverarbeitendes Gerät und an den mit diesem Gerät arbeitenden Menschen zur Erzielung eines Ergebnisses"*.[46] Nach § 69a Abs. 3 UrhG genießen Computerprogramme den gesetzlichen Urheberrechtsschutz, wenn sie als „individuelle Werke" „das Ergebnis der eigenen geistigen Schöpfung ihres Urhebers" sind. Insoweit kommt es auf die jeweilige Problemlösung an und eine „persönliche Schöpfung von hinreichend geistigem Gehalt".[47] So gesehen entscheidet daher auch die Individualität des geschaffenen Programms.[48]

2.2 Spannungsfelder: Ausschließlichkeit (Einzelner) v. Allgemeinheit

Immer, wenn ein so genanntes Ausschließlichkeitsrecht – wie Eigentum oder Urheberrechtsschutz – von einer Rechtsordnung dem Einzelnen gewährt wird, entstehen Kollisionen mit Rechten der Allgemeinheit, die im Sinn einer „praktischen Konkordanz" *(Hesse)* aufgelöst werden müssen. Die Allgemeinheit hat eben ein Recht auf Informationen und auch an den Ergebnissen der Verarbeitung der Daten, weil – um es verkürzt zu sagen – unberechtigt erteilte Ausschließlichkeitsrechte sehr nahe an einer unerwünschten Monopolbildung liegen, die ja – im Gegensatz zu einem funktionierenden Wettbewerb – bekanntlich eine Verschwendung volkswirtschaftlicher Ressourcen befördert.

Allerdings darf man nicht außer Acht lassen: Solange die Eigentumszuordnung von Daten nicht gesetzlich gelöst ist, herrscht allein die Zuordnung auf Basis von Geheimhaltungsverträgen, und zwar auch in den Fällen, in denen eine Auftragsverarbeitung von Daten durch ein drittes Unternehmen stattfindet. Der Ertrag steht dann regelmäßig auf Grund vertraglicher Absprachen dem Auftraggeber zu.[49] Anzumerken ist daher auch, dass der deutsche Gesetzgeber dieses Spannungsverhältnis für die Herstellung einer neuen körperlichen Sache in § 950 BGB zugunsten des Verarbeiters löst, indem er ihm in der Regel die durch die Verarbeitung entstehende neue Sache zu Eigentum zuweist.

3. Positionen

Wenn nunmehr kurz die einzelnen Positionen beleuchtet werden sollen, die in Deutschland zu den Fragen des Dateneigentums vertreten werden, so ist es am hilfreichsten, zwischen den offizielleren und den Positionen zu differenzieren, die in der Wissenschaft vertreten werden.

3.1 Quasi offizielle Stellungnahmen

In einer groben Unterscheidung der zu findenden Argumentationsansätze sei angemerkt: Die Referenten der Justizminister der Länder und des Bundes[50] haben sich in einer halboffiziellen Stellungnahme im Jahr 2017 gegen die Einführung eines Dateneigentums entsprechend der sachenrechtlichen Grundnorm des § 903 BGB entschieden.[51] Der Bundesminister für Verkehr und Infrastruktur – vornehmlich an Mobilitätsdaten interessiert – hat zu dieser Frage eine Studie veröffentlicht,[52] die aber wegen ihrer hohen Relevanz für den Schutz personenbezogener Daten auch im Licht des soeben publizierten Gutachtens der Datenethik-Kommission der Bundesregierung gesehen und bewertet werden muss.[53]

3.2 Literaturstimmen

Das ist hier schon aus Platzgründen nicht zu leisten, zumal der Eigentumsschutz maschinengenerierter Daten im Vordergrund der hier zu führenden Debatte steht. Festzuhalten bleibt also lediglich, dass die bisher ans Tageslicht gehobenen offiziellen oder halboffiziellen Publikationen sich jedenfalls nicht für einen an § 903 BGB ausgerichteten sachenrechtlichen Eigentumsschutz – trotz der bestehenden Schutzlücken der anwendbaren Gesetze – aussprechen. Stattdessen werden unterschiedliche Lösungsansätze vorgeschlagen.[54]

Im Vordergrund steht wohl nach wie vor die Meinung, dass ein eigentumsähnlicher Schutz für maschinengenerierte Daten[55] abzulehnen ist.[56] Diesen Standpunkt vertritt auch die Kommission, ohne dass sie diesen bislang auch schriftlich fixiert hat.

Sieht man von allen rechtlichen Detailfragen einmal ab (die ihrerseits hochkomplex sind), dann sticht jedenfalls das rechtspolitische Argument heraus: Würde das deutsche Recht dem Inhaber der maschinengenerierten Daten (auf Grund eines Geheimhaltungsabkommens) das ausschließliche Recht zuweisen, mit diesen Daten nach seinem freien Belieben umzugehen, führte dies zwingend zu wirtschaftlichen und auch rechtlichen Folgeproblemen in den übrigen Mitgliedstaaten der EU, die keine gesetzliche Bestimmung aufweisen, welche dem Inhaber eine gegen jedermann wirkende, weil absolute und ausschließliche Rechtsposition zuweist.[57]

Hinzutritt das weitere Argument, dass eine durch das Dateneigentum begründete ausschließliche Rechtsposition an Daten notwendigerweise die Frage aufwirft, ob und wie denn für an-

---

44) *Wiebe*, GRUR Int. 2016, 877, 879.
45) Ausgangsentscheidung BGH NJW 1986, 192 – Inkasso-Programm.
46) OLG Hamburg CR 1998, 332, 333.
47) So *Kaboth/Spies*, in: BeckOK UrhG, Stand: 15. 10. 2019, § 69a Rz. 14.
48) *Dreier*, in: Dreier/Schulze, UrhG, 6. Aufl., 2018, § 69a Rz. 26.
49) Zu den politischen Fragen des „processor" oder auch „producer" vgl. auch Fußn. 1 S. 13.
50) Bericht der *Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder* v. 15. 5. 2017, abrufbar unter: https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf.
51) *Steinrötter*, MMR 2017, 731, 732.
52) *Bundesministerium für Verkehr und digitale Infrastruktur*, „Eigentumsordnung" für Mobilitätsdaten? – Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive", 2. 8. 2017 – BMVI – abrufbar – download.
53) Abrufbar unter https://www.bmjv.de → FokusThemen → Datenethikkommission_node.
54) Statt vieler *Fezer*, MMR 2017, 3 ff.; *Fezer*, ZD 2017, 99 ff. – Dateneigentum der Bürger; *Hoeren*, MMR 2019, 5 ff. – Datenbesitz statt Dateneigentum (analog § 303a StGB); im Prinzip für eine gesetzliche Regelung auch *Werner*, NJOZ 2019, 1041, 1044.
55) *Determann*, ZD 2018, 503 ff.; *Stender-Vorwachs/Steege*, NJOZ 2018, 1361, 1365 f.; *Zech*, GRUR 2015, 1151 ff.; *Wiebe*, GRUR Int 2016, 877, 884; *Czychowski/Siesmayer*, in: Kilian/Heussen, Computerrechts-Handbuch, 34. EL, 2018, Kap. 20.5 Rz. 19 ff.; *Fritzsche*, in: BeckOK BGB, Stand: 1. 8. 2019, § 903 Rz. 10; *Palandt/Ellenberger*, BGB, 78. Aufl., 2019, § 90 Rz. 2.
56) *Zimmer*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 101, 107.
57) Mit Recht auch *Stender-Vorwachs/Steege*, NJOZ 2018, 1361, 1365.

dere Marktteilnehmer – nicht zuletzt auch für Start-ups – der Zugang dann zur Nutzung dieser Daten eröffnet und gewährt werden kann.[58)]

4. Lösungsaufgaben

Doch dass die Antwort auf das Problem einer sachenrechtlichen Zuordnung der Daten als Dateneigentum (oder auch eines eigentumsähnlichen Rechts) rechtspolitisch bald im Kontext eines neu zu schaffenden europäischen Rechts befriedigend gelöst werden muss, um Rechtssicherheit zu erreichen, weil ja bekanntlich Rechtsunsicherheit Gift für das Florieren einer freiheitlichen Wirtschaft ist, soll durch folgende Gedankensplitter angedeutet und untermauert werden:

Erstens, es muss alsbald eine Entscheidung auf europarechtlicher Ebene getroffen werden, ob ein wie auch immer geartetes Institut – Dateneigentum – geschaffen wird und wer als Eigentümer in welchem Umfang legitimiert ist, nämlich: der Inhaber, der Producer oder die Allgemeinheit (vorbehaltlich personenbezogener Daten) und welche Zugangsrechte für Dritte bestehen und ihnen zwingend auch einzuräumen sind. Dass Daten bekanntlich rival sind, also mehrfach genutzt werden können, ohne an Wert zu verlieren, belegt den Hintergrund des Gemeinten.

Zweitens, fällt, wie zu erwarten, die Antwort negativ aus oder erweist sie sich aus Zeitgründen als im europäischen Rahmen zu komplex, dann müssen belastbare Regeln für die Frage entworfen werden (Modellverträge), wie etwa denn die Eigentumszuordnung an Daten im Bereich des immer weiter wachsenden Cloud-Computing[59)] zu bewältigen ist. Denn dort herrschen zahlreiche vertragliche (Eigentums-)Regeln zugunsten der Betreiber, die keineswegs immer den Nutzer, der seine Daten in der Cloud „ablegt", hinreichend schützen.[60)]

Drittens, herrschen für die rechtliche Einhegung der KI – wie bisher schon – im Wesentlichen vertragliche Absprachen über Geheimhaltung und Nutzungsrechten an Daten,[61)] dann bedarf es verlässlicher Grenzmarkierungen, welche Klauseln im Einzelnen als missbräuchlich und damit als unwirksam anzusehen sind.[62)] Denn das Recht des Stärkeren gibt keine belastbare Antwort auf diese entscheidende Gerechtigkeitsfrage.

III. Haftung für KI

Die rasant wachsende Bedeutung des Internet of Things für unseren Alltag, Künstliche Intelligenz (KI), miteinander kooperierende Maschinen (unabhängig von menschlicher Einwirkung), autonome Systeme einschließlich Drohnen im Cyberwar – diese fast jeden erdrückende Gemengelage hat den ehemaligen deutschen Verfassungsrichter *Wolfgang Hoffmann-Riem* in seinem Grundlagenwerk „Innovation und Recht – Recht der Innovation"[63)] zum Schluss seiner wegweisenden Erwägungen zu der resignierenden Feststellung verleitet: „Das Recht allein hat nicht die Kraft, das Notwendige (im Sinn des Schutz der Grundrechte) zu erreichen."[64)]

1. Grundaussage zur KI in haftungsrechtlicher Sicht

1.1 Definition

In ihrem ebenfalls unter dem 19. 2. 2020 herausgegebenen Bericht an das Europäische Parlament, den Rat und an den Ausschuss für Wirtschaft und Soziales[65)] „on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics" unterbreitet die Kommission eine sehr breit angelegte Definition der KI, in der bereits zentrale Rechtsfragen unmittelbar angesprochen werden. Sie lautet:

„Künstliche Intelligenz, Internet der Dinge und Robotik weisen viele gemeinsame Merkmale auf. Sie können Konnektivität, Autonomie und Datenabhängigkeit miteinander verknüpfen, um Aufgaben ohne oder nur mit geringer menschlicher Steuerung oder Aufsicht auszuführen. KI-gestützte Systeme können zudem ihre Leistung verbessern, indem sie aus Erfahrungen lernen. Ihre Komplexität spiegelt sich sowohl in der Vielfalt der an der Lieferkette beteiligten Wirtschaftsakteure als auch in der Vielzahl von Komponenten, Teilen, Software, Systemen oder Dienstleistungen wider, die zusammen die neuen technologischen Ökosysteme bilden. Hinzu kommt die Offenheit für Aktualisierungen und Verbesserungen nach der Markteinführung dieser Technologien. Die enormen beteiligten Datenmengen, der Rückgriff auf Algorithmen und die Opazität der KI- Entscheidungsfindung erschweren die Vorhersage des Verhaltens eines KI-gestützten Produkts und das Verständnis der potenziellen Schadensursachen. Schließlich können Konnektivität und Offenheit KI-Produkte und IoT-Produkte anfällig für Cyberbedrohungen machen."[66)]

Folgende, später noch einmal aufzugreifende Merkmale seien jetzt schon herausgegriffen: Der menschliche Einfluss auf das Funktionieren der KI ist vor allem wegen ihrer Autonomie begrenzt; die Komplexität der KI steht im Vordergrund, vor allem im Blick auf die mannigfachen Einwirkungen, welche innerhalb der „supply chain" vorgenommen werden können. Vor allem aber ist „Undurchsichtigkeit" der KI ein zentrales, rechtlich nur schwer zu bewältigendes Problemfeld, weil das Merkmal der Vorhersehbarkeit einer autonomen Entscheidung der KI fehlt und weil deshalb auch Merkmale der Kausalität im Schadensfall nicht einschlägig sind.

1.2 Bisherige Haftungssysteme

Gerade deswegen arbeitet die Kommission im Augenblick – dafür sind zwei Expertengruppen gebildet worden – an einer haftungsrechtlichen Erfassung der besonderen Risiken der KI sowie daran, ob die Produkthaftungsrichtlinie 85/374/EWG[67)] an die besonderen haftungsrechtlichen Risiken der KI angepasst werden soll.

Diese Richtlinie ist im Bereich des Haftungsrechts – neben unzähligen, dem öffentlichen Recht angehörenden Verordnun-

58) Hierzu auch *Kerber*, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, S. 109, 113.
59) Hierzu *Wicker*, MMR 2012, 783 ff.; vgl. auch *Splittgerber/Rockstroh*, BB 2011, 2179 ff.
60) Hierzu im Einzelnen *Boehm*, ZEuP 2016, 358, 380 ff.
61) Im Einzelnen auch *Jakl*, MMR 2019, 711, 713, 715.
62) Hierzu im Einzelnen mit Verweis auf die entsprechenden Regeln des Common European Sales Law (CESL) als Leitlinien für default rules *Graf von Westphalen* (Fußn. 12).
63) *Hoffmann-Riem*, Innovation und Recht – Recht der Innovation, 2016.
64) *Hoffmann-Riem* (Fußn. 63), S. 693.
65) Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final.
66) COM(2020) 64 final, S. 2.
67) ABl v. 7. 8. 1985 L 210, 29 ff.; hierzu im Einzelnen *Graf von Westphalen*, in: Foerste/Graf von Westphalen, Produkthaftungs-Handbuch, 3. Aufl., 2012, §§ 44 ff.

gen zum Produktsicherheitsrecht[68] – der einzige europarechtlich vereinheitliche Sektor. Er ist allerdings auf den Verbraucherschutz bezogen, gilt also nicht in dem Bereich, der in diesem Rahmen nicht minder interessiert, nämlich: die Bewältigung der Haftungsrisiken im gewerblichen Bereich, welche durch ein Versagen der KI verursacht werden. Ob sich aus den Ergebnissen der Expertengruppe zur Haftung für KI[69] ein eigener Gesetzesansatz der Kommission ergeben wird, der auch den B2B-Bereich erfasst, ist gegenwärtig noch nicht absehbar.

Daneben gelten – und das ist die Quintessenz – nur einzelne mitgliedstaatliche Haftungsregime, die keineswegs harmonisiert sind. Harmonisiert ist insoweit nur die Rom II-VO;[70] sie regelt die Frage, welches Recht denn dann anwendbar ist, wenn der eingetretene Schadensfall grenzüberschreitenden Charakter aufweist, also bezogen auf den Handlungsort – zum Beispiel bei Vorliegen eines Fabrikationsfehlers – und auf den Erfolgsort – der Ort, an dem der Schaden eingetreten ist – unterschiedlichen nationalen Haftungsregeln folgt.

Ausgehend vom deutschen Haftungsrecht gilt hier der sich aus § 823 BGB ergebende Grundsatz einer vom Verschulden abhängigen Haftung, die das Element der Kausalität zwischen dem haftungsauslösenden Ereignis und dem Schaden voraussetzt. Demgegenüber ist die Haftung nach dem Produkthaftungsgesetz, welches die RL 865/374/EWG ins deutsche Recht umgesetzt hat, vom Vorwurf des Verschuldens (also: mindestens dem Vorwurf einfacher Fahrlässigkeit) losgelöst; es ist eine Gefährdungshaftung[71] für Schäden an Leib, Leben und Gesundheit sowie an privat genutzten körperlichen Sachen für fehlerhafte Produkte, die ein Verbraucher erleidet.

2. Neue Lösungsansätze

2.1 Ausgangspunkt

KI – zusammenfassend verstanden als selbstlernendes System[72] und künstliche neuronale Netze[73] – stiftet deshalb neue Herausforderungen – den Roboter nicht zu vergessen[74] – für die bisherigen haftungsrechtlichen Regime, weil sie – wie in der oben zitierten Definition der KI auch nachzulesen – aus den verschiedensten Gründen äußerst komplex ist und demzufolge unvorhersehbare Risiken auf Grund eines Fehlverhaltens nach sich zieht.[75] Mit anderen Worten: Das Risiko der Unvorhersehbarkeit folgt aus der Komplexität,[76] die eine nur eingeschränkte Aufklärbarkeit und eine ebenfalls nur eingeschränkte Erklärbarkeit nach sich zieht.[77] Ein weiteres Phänomen der KI folgt aus ihrer „Verwundbarkeit" („vulnerability" dieser Systeme) durch Cyberangriffe.[78] Das Problem mangelnder Aufklärbarkeit wird durch das Phänomen der Intransparenz (selbstständiges „bottom up", nicht vom Menschen veranlasstes „bottom down") verstärkt. Gegenüber den bisher bekannten und auch bewährten Haftungsregimen liegt in alledem der „game changer"[79] und damit auch die neue rechtspolitische und legislatorische Herausforderung bei der Einführung einer Haftung für Fehlverhalten der KI.

2.2 Herausforderungen

2.2.1 Ausgangspunkte

Wegen der nicht vorhersehbaren und auch technisch nicht beherrschbaren „Fehler" der KI und der so geschaffenen Risikolagen und dann eben auch eingetretener Rechtsgutverletzungen folgt zunächst ein doppelter Ansatz: Man kann diese – neuartigen – Risiken gesellschaftlich und damit auch rechtlich in Kauf nehmen, soweit sich die Nützlichkeit dieser Systeme auf Basis einer „Kosten-Nutzen"-Analyse als vertretbar erweist.[80] Dann trifft das Risiko den mehr oder weniger zufällig Geschädigten. Er bleibt mit seinem Schaden allein. Man kann allerdings auch die grundsätzlichere Frage stellen, ob es denn verfassungsrechtlich unter der Perspektive der Schutzpflicht des Staates vertretbar ist, unbekannte und nicht vorhersehbare Risiken eines Fehlverhaltens der KI sanktionslos zu akzeptieren. Denn das Verfassungsgericht hat in seiner bekannten Kalkar-Entscheidung[81] die Grenze der „praktischen Vernunft" zugunsten der vom Staat zu schützenden Grundrechte der Bürger gezogen.

Es heißt dort in dem entscheidenden 6. Leitsatz dieses Urteils:[82] *„Vom Gesetzgeber im Hinblick auf seine Schutzpflicht eine Regelung zu fordern, die mit absoluter Sicherheit Grundrechtsgefährdungen ausschließt, die aus der Zulassung technischer Anlagen und ihrem Betrieb möglicherweise entstehen können, hieße die Grenzen menschlichen Erkenntnisvermögens verkennen und würde weithin jede staatliche Zulassung der Nutzung von Technik verbannen. Für die Gestaltung der Sozialordnung muss es insoweit bei Abschätzungen anhand praktischer Vernunft bewenden. Ungewissheiten jenseits dieser Schwelle praktischer Vernunft sind unentrinnbar und insofern als sozialadäquate Lasten von allen Bürgern zu tragen."*

Bezogen auf das geltende Recht ist die Klammer zwischen diesen beiden Denkansätzen die Frage, ob denn der „Hersteller" – und die Lieferkette – die geltenden Regeln der Technik und den – jeweiligen (internationalen)[83] – Stand von Wissenschaft und Technik beachtet hat,[84] um das von ihm gefertigte/konzipierte Produkt sicher – das heißt: ohne einen vermeidbaren Fehler – in den Verkehr zu bringen. Ein solcher Fehler wird dann in § 3 ProdHaftG dahin definiert, dass das Produkt nicht die Sicherheit bietet, die „man" zu erwarten berechtigt war.[85] So gesehen lässt sich sagen, dass der jeweilige Stand von Wissenschaft und Technik zum Garanten für die Sicherheit des Produktbenutzers wird.

---

68) Hierzu *Klindt*, Produktsicherheitsgesetz, 3. Aufl., 2015; diese Fragen werden auch tendenziell in dem Bericht der Kommission COM(2020) 64 final angesprochen (S. 3 ff.).
69) Hierzu Report from the Expert-Group on Liability an New Technologies – New Technologies Formation, abrufbar im Internet.
70) VO 864/2007 – ABl 2007 L 199, S. 40 ff.
71) Zum Diskussionsstand und der dogmatischen Einordnung dieser Haftungsfigur vgl. *Graf von Westphalen* (Fußn. 67), § 45 Rz. 1 ff.
72) Hierzu *Zech*, ZfPW 2019, 198, 200.
73) *Zech*, ZfPW 2019, 198, 201.
74) *Zech*, ZfPW 2019, 198, 199, 203 f.
75) Statt aller *Spindler*, in: Lohsse/Schulze/Staudenmayer, Liability for Artificial Intelligence and the Internet of Things, 2019, S. 125, 126 f.; vgl. auch im Einzelnen *Wagner*, AcP 2017, 708; *Graf von Westphalen*, ZIP 2019, 889 ff.
76) *Meyer*, ZRP 2019, 233, 235.
77) Im Einzelnen *Zech*, ZfPW 2019, 198, 199, 205.
78) Report from the Experts (Fußn. 69), S. 3.
79) So mit Recht *Comandé*, in: Lohsse/Schulze/Staudenmayer, Liability for Artificial Intelligence and the Internet of Things, 2019, S. 165, 169.
80) Hierzu *Wagner*, AcP 2017, 708, 731 ff.
81) BVerfG NJW 1979, 359.
82) So *Graf von Westphalen*, ZIP 2019, 889 f.
83) BGH NJW 1981, 1603, 1604 – Desoral.
84) Grundlegend BGH NJW 2009, 2952 – Airbag.
85) Hierzu im Einzelnen *Graf von Westphalen* (Fußn. 67), § 48 Rz. 1 ff.

2.2.2 Konsequenzen betreffend KI

Im Blick auf die fehlende Vorhersehbarkeit eines Fehlverhaltens der KI leuchtet es unmittelbar sein, dass das Konzept des Standes von Wissenschaft und Technik in diesen Fällen als Verteidigungslinie des Verursachers eines Schadens nicht mehr uneingeschränkt tragfähig ist. In gleicher Weise muss dann auch gelten, dass das Anknüpfen an eben diesen Tatbestand in der Definition eines Fehlers nicht mehr haltbar ist, weil nach geltendem Verständnis – Stichwort: unvermeidbares Entwicklungsrisiko – der Verbraucher berechtigterweise nur die Sicherheit erwarten kann, die ihm nach dem Stand von Wissenschaft und Technik verbürgt ist.

Das löst die rechtspolitische Frage aus, ob denn der von einem Fehlverhalten der KI – beispielsweise der Fehlfunktion eines Roboters in seiner Gesundheit geschädigt oder gar getötet worden ist – mit diesem Ergebnis als „Schicksalsschlag" allein gelassen wird, oder ob sein Schaden ausgeglichen wird (Stichwort: Contergan vor Gründung der Stiftung). Entscheidet man sich für eine Haftung, so kann dies in ihrem Grundansatz nur eine reine Gefährdungshaftung sein. Diese kann wohl nur an dem Schadensfall als haftungsbegründend anknüpfen, und nur insoweit am Vorliegen eines Fehlers, als der Verbraucher stets bei der bestimmungsgemäßen Nutzung eines Produkts – auch im Rahmen des Internet of Things – davon ausgehen kann und darf, dass er in seinen Rechtsgütern nicht geschädigt wird.[86)]

Wegen der hohen Komplexität der KI und ihrer mangelnden Erklärbarkeit und Aufklärbarkeit im Fall eines Versagens wird man hier aber – außerhalb des Produktnutzers/Geschädigten – alle Unternehmen, die möglicherweise am Entstehen des Risikos[87)] und damit auch des eingetretenen Schadens eine technische Verantwortung tragen,[88)] gesamtschuldnerisch in die Haftung nehmen müssen.

Diese weit gespannte Haftung beruht letztlich auch auf einem weiteren Gesichtspunkt, der eine eigene Antwort einfordert: Wenn neben der hohen, nicht vorhersehbaren Komplexität im potentiellen Fehlverhalten der KI auch der Aspekt ihrer Intransparenz eine Rolle spielt,[89)] dann fällt auch das Tatbestandselement der Kausalität – also die ursächliche Verknüpfung zwischen Handlung und Schaden – in sich zusammen. Dieser Nachweis kann jedenfalls nicht vom Geschädigten sinnvollerweise geführt werden. Man denke nur an einen selbstlernenden Algorithmus (update), der von zahlreichen maschinengenerierten und ihm dann zur Verarbeitung zugeführten (fehlerhaften) Daten gefüttert wurde, der dann einen Schaden verursacht.[90)] Das führt zum Stichwort der Multikausalität[91)] sowie einer alternativen Kausalität.

Die Antwort der mitgliedstaatlichen Rechte für diese Fälle von Beweisschwierigkeiten ist: Entweder ist keiner haftbar oder alle im Wege der Gesamtschuld.[92)] Letzteres erscheint vorzugswürdig. Auch ist an eine Proportionalhaftung aller Beteiligten zu denken, die aber in ihrer Ausprägung schwierig zu begründen ist.[93)]

Ob darüber hinaus zur Beseitigung von Beweisschwierigkeiten verschiedenster Art auf eine Umkehr der Beweislast zum Nachteil des oder der Anspruchsgegner in Bezug auf die Schadenskausalität rekurriert wird,[94)] ist offen,[95)] aber wohl abzulehnen. In der Debatte ist möglicherweise auch die Erwägung, stattdessen nur auf Korrelationen abzustellen. Doch das kann und muss im gegenwärtigen Zeitpunkt der rechtspolitischen Debatte noch offenbleiben.

Entscheidend ist, dass wichtige Stimmen,[96)] auch die Expert-Group on Liability for Artifical Intelligence, vorgeschlagen haben,[97)] die besonderen von einer KI geschaffenen – besonderen – Schadensrisiken – vor allem im Blick auf die nicht befriedigend lösbaren Kausalitätsprobleme – im Rahmen einer Pflichtversicherung abzudecken,[98)] was allerdings die europäische Versicherungswirtschaft bislang kaum entzückt.[99)]

2.3 Abschließende Bemerkung

Während sich die Arbeit der Expertengruppe für die Novellierung der Produkthaftungsrichtlinie auf den zu verbessernden Verbraucherschutz konzentriert, ist der Report der AI-Gruppe auch auf den Schutz des B2B-Verkehrs bezogen. In Konsequenz dieses Ansatzes sind dann auch Schäden als Vermögensschäden – Zerstörung der Daten („corrupted data") unter gewissen Voraussetzungen von der neu zu schaffenden Haftungsfigur für das Versagen der KI erfasst.

Bis wir hier eine oder zwei neue Richtlinien sehen werden, werden noch einige Jahre ins Land gehen. Es ist leider bis dahin ungewiss, ob das in Deutschland geltende Haftungsregime der verschuldensabhängigen Haftung nach § 823 BGB hier die Lücke zugunsten des Geschädigten immer schließen kann. Und im Blick auf das ProdHaftG ist in Erinnerung zu rufen: Es stammt aus dem Jahr 1985; es war schon juristisch schwierig

86) So BGH ZIP 1990, 516 – Pferdebox, dazu EWiR 1989, 1191 *(Cahn)*.
87) *Spindler* (Fußn. 75), S. 125, 130 f.
88) Im Einzelnen auch *Comandé* (Fußn. 79), S. 165 ff.
89) „The Union product safety legislation does not explicitly address the increasing risks derived from the opacity of systems based on algorithms. It is therefore necessary to consider requirements for transparency of algorithms, as well as for robustness, accountability and when relevant, human oversight and unbiased outcomes, particularly important for the ex-post mechanism of enforcement and to build trust in the use of those technologies. One way of tackling this challenge would be imposing obligations on developers of the algorithms to disclose the design parameters and metadata of datasets in case accidents occur" – COM(2020) 64 final S. 9.
90) Report (Fußn. 69), S. 20.
91) *Zech*, ZfPW 2019, 198, 199, 207 f.
92) Report (Fußn. 69), S. 21 f.
93) Hierzu auch *Zech*, ZfPW 2019, 198, 199, 208.
94) So *Spindler* (Fußn. 75), S. 125, 139 f. – Gesichtspunkt auch der Beweissicherungspflichten im Blick auf Konzeption und Funktionstüchtigkeit der KI.
95) Umfassend auch *Martin-Casals*, in: Lohsse/Schulze/Staudenmayer, Liability for Artificial Intelligence and the Internet of Things, 2019, S. 201 ff., „The Commission is seeking views whether and to what extent it may be needed to mitigate the consequences of complexity by alleviating/reversing the burden of proof required by national liability rules for damage caused by the operation of AI applications, through an appropriate EU initiative. As regards Union legislation, according to the Product Liability Directive, a product that does not meet mandatory safety rules would be considered defective, regardless of the producers' fault. There may, however, also be reasons to contemplate ways on how to facilitate the burden of proof for victims under the Directive: the Directive relies on national rules on the evidence and the establishment of causation" – COM(2020) 64 final S. 14.
96) *Borges*, in: Lohsse/Schulze/Staudenmayer, Liability for Artificial Intelligence and the Internet of Things, 2019, S. 145 ff.
97) Report (Fußn. 69), S. 4; vgl. auch *Graf von Westphalen*, ZIP 2019, 889 ff.
98) So auch *Zech*, ZfPW 2019, 198, 199, 218; „For the operation of AI applications with a specific risk profile, the Commission is seeking views on whether and to what extent strict liability, as it exists in national laws for similar risks to which the public is exposed (for instance for operating motor vehicles, airplanes or nuclear power plants), may be needed in order to achieve effective compensation of possible victims. The Commission is also seeking views on coupling strict liability with a possible obligation to conclude available insurance, following the example of the Motor Insurance Directive, in order to ensure compensation irrespective of the liable person's solvency and to help reducing the costs of damage" – COM(2020) 64 final, S. 16.
99) Stellungnahme von Insurance Europe v. 29. 11. 2019.

genug, aus dem erwähnten Begriff einer Haftung für Schäden wegen eines Fehlers der Elektrizität zu folgern, dass damit im Wege einer Analogie auch die Haftung für Softwarefehler erfasst war;[100] für die neue Haftungsfigur bei einem Versagen der KI ist insoweit wirklich kein Platz.

IV. Bilanzierung von KI

1. Ausgangspunkt

Klar ist, dass die Digitalisierung auch auf Fragen der Bilanzierung – schon wegen der teils völlig neuen Geschäftsmodelle – im Sinn des Themas einen disruptiven Einfluss ausübt.[101] Immaterielle Ressourcen stehen im Vordergrund; Daten sind mittlerweile ein wesentlicher Teil der Wertschöpfung des Unternehmens. Es herrschen mehr und mehr Dauerschuldverhältnisse, und angelehnt an die aus dem Know-how-Recht bekannten Beispiele herrscht der Nutzungs- oder Lizenzvertrag (mit der zwangsläufig gekoppelten Geheimhaltungspflicht). Dabei ist wenig klar, ausgenommen der Grundtatbestand: Daten sind nach IAS 38 ein immaterieller Vermögenswert.

2. Zweifelsfragen

Mangels verfügbarer und in der Praxis bewährter Richt- oder auch Leitlinien für die Bilanzierung von KI – vor allem im Blick auf den jeweiligen „fair value" – verbleiben einige bedeutsame Zweifelsfragen, die aber beantwortet werden müssten:

2.1 Parallele zum Know-how

Bei den hier zu bewältigenden Bilanzierungsfragen für maschinengenerierte Daten (KI), ist von einer gewissen Parallele zu der Bilanzierung von Know-how auszugehen. Denn in beiden Fällen handelt es sich um geheimhaltungsbedürftiges Wissen. Beim Know-how erfolgt die Zuordnung als immaterieller Vermögensgegenstand im Anlagevermögen (also weder den Sach- noch den Finanzanlagen)[102], wenn Nutzungs- und Funktionszusammenhang im Unternehmen das Interesse an der unkörperlichen Substanz, etwa auch bei der Übertragung von Lizenzrechten, beherrscht.[103] Ein gewisser Haltepunkt ist die Regel des § 248 Abs. 2 HGB. Danach können selbstgeschaffene immaterielle Vermögensgegenstände des Anlagevermögens in der Bilanz im Rahmen eines Wahlrechts aktiviert werden. Dabei zählen hierzu auch unentgeltlich erworbene immaterielle Vermögensgegenstände.[104] Für den Bereich des Steuerrechts kommt es nach § 5 Abs. 2 EStG darauf an, dass es sich um einen entgeltlichen Erwerb handelt, so dass dann ein Aktivierungsgebot besteht.[105]

Nach dem Grundsatzurteil des BFH vom 3. 7. 1987 ist dies auch für die Bilanzierung von Software anerkannt.[106] Auch hier handelt es sich um einen selbstständigen immateriellen Vermögensgegenstand.[107]

2.2 Zweifelsfragen

Erstens, wenn an Daten – KI – kein privatrechtlicher Eigentumstitel besteht, kann dann auf den Ausnahmetatbestand des wirtschaftlichen Eigentums nach § 39 Abs. 2 Nr. 1 AO zurückgegriffen werden und dieser Vermögenswert im Anlagevermögen bilanziert werden? Gilt dies auch dann, wenn in der Norm bestimmt ist, dass der wirtschaftliche Eigentümer die tatsächliche Sachherrschaft über das Wirtschaftsgut ausübt und so in der Lage ist, den wirklichen Eigentümer für die Dauer der Nutzung von eben dieser auf Dauer auszuschließen? Denn einen wahren Eigentümer, der von der Nutzung der Daten auszuschließen ist, gibt es nicht.

Zweitens, mehr noch: Wenn bei einer KI auch weitere Daten Dritter aggregiert wurden, etwa auch auf Grund eines Lizenzvertrags, wie sind dann die Wertverhältnisse zu ermitteln?

Drittens, sind selbst erstellte Daten der KI Teil und Ergebnis eines FE-Prozesses nach IAS 38,52?[108]

Viertens, wie ist der Vermögenswert der KI anzusetzen und ggfs. abzuschreiben, wenn man bedenkt, dass Daten – vor allem auch personenbezogene Daten – keiner Abnutzung unterliegen? Natürlich ist hier die Erstbewertung nach den Herstellkosten vorzunehmen, wie sich dies aus § 255 Abs. 2 Satz 2 HGB ablesen lässt (Einzelkosten und variable Gemeinkosten). Aber die hiermit verknüpften personenbezogenen Daten könnten ja unentgeltlich erworben worden sein. Wenn aber diese Daten keiner Abnutzung unterliegen, passt dann noch die für die Folgebewertung heranzuziehende Vorschrift des § 255 Abs. 3 HGB? Diese schreibt ja für selbstgeschaffene immaterielle Vermögensgegenstände einen Abschreibungszeitraum von 10 Jahren vor.[109]

Es mag jedoch sein, dass man den hier angedeuteten Problemlagen mit den Grundsätzen der Rechnungslegung nach IAS 38 etwas auf die Spur kommen kann. Die maschinengenerierten Daten, vor allem die jeweiligen Algorithmen, wären dann eben ein Asset – verstanden als immaterieller Vermögenswert (ohne physische Substanz) –, weil erwartet werden kann, dass bei ihrer Nutzung dem Unternehmen künftig ein wirtschaftlicher Wert zufließt. Eine Abschreibung ist hier nicht zwingend vorgesehen, weil keine zeitlich begrenzte Nutzungsdauer anzunehmen ist, so dass nur eine konkrete Wertminderung nach IAS 36 in Betracht zu ziehen ist.[110] Wird allerdings Know-how im Rahmen einer Lizenz erworben, dann ist dieses Wirtschaftsgut innerhalb eines Zeitraumes von 15 Jahren abzuschreiben – ein Zeitraum, der für die (wirtschaftliche) Nutzung maschinengenerierter Daten nicht unbedingt als richtig anzusehen ist.[111] Doch ist das Nutzungsrecht für den Lizenznehmer – es handelt sich dann um ein schwebendes Geschäft – nicht zu aktivieren; wohl aber sind die Lizenzentgelte als Aufwand zu verbuchen.[112]

Fünftens, wie sind die Bilanzierungsgrundsätze, wenn das Unternehmen auch personenbezogene Daten – etwa für Werbezwecke – einsetzt? Wie wirkt es sich dann aus, dass Art. 3 RL 2019/770 die Hergabe der personenbezogenen Daten als

100) Im Einzelnen *Graf von Westphalen* (Fußn. 67), § 47 Rz. 40 ff. zum Meinungsstand.
101) *Beyhs/Poymanov*, IRZ 2019, 19, 24 ff.
102) *Pfaff/Nagel/Wittkowski*, in: Pfaff/Osterrieth, Lizenzverträge, 4. Aufl., 2018, Kap. A V Rz. 428.
103) *Schubert/Huber*, in: Beck Bil-Komm, 12. Aufl., 2020, § 247 HGB Rz. 384.
104) *Schmidt/Usinger*, in: Beck Bil-Komm, 12. Aufl., 2020, § 248 HGB Rz. 13.
105) *Schmidt/Usinger* (Fußn. 104), § 248 HGB Rz. 35.
106) BeckRS 1987, 5473.
107) Vgl. *Müller-Hengstenberg*, NJW 1994, 3128.
108) *Beyhs/Poymanov*, IRZ 2019, 19, 25.
109) *Schmidt/Usinger* (Fußn. 104), § 248 HGB Rz. 439.
110) *Pfaff/Nagel/Wittkowski* (Fußn. 102), Rz. 448.
111) *Pfaff/Nagel/Wittkowski* (Fußn. 102), Rz. 483.
112) *Pfaff/Nagel/Wittkowski* (Fußn. 102), Rz. 469.

„Gegenleistung" für eine kostenlos gewährte digitale Dienstleistung oder für digitale Inhalte – gesetzlich gleichgewichtig neben einem in Euro ausgewiesenen Preis – qualifiziert? Ergibt dies dann etwa eine bei der Umsatzteuer zu beachtende Größe?

V. Summe

Fasst man nunmehr zusammen, so zeigt sich, dass die disruptiven Elemente der in der KI verkörperten Digitalisierung von Schritt zu Schritt im Rahmen der behandelten Themen zugenommen haben. Es wird auch sicherlich noch einige Zeit dauern, bis hier abschließende Lösungen – wenn denn überhaupt – gefunden werden. Bis dahin gilt wohl der nur salopp formulierte Grundsatz, dass man im Nebel nur auf Sicht fahren sollte – keine unbedingt überzeugende Perspektive angesichts des ohnedies vorhandenen technischen Vorsprungs von Amerika und China.

Carsten Herresthal[*)]

Die Rechtsfolgen einer Richtlinienwidrigkeit der Musterwiderrufsbelehrung bei Verbraucherdarlehen

Zugleich Besprechung EuGH v. 26. 3. 2020 – Rs C-66/19, ZIP 2020, 663 – Kreissparkasse Saarlouis

Am 26. 3. 2020 ist der EuGH in einer bemerkenswerten Entscheidung zu dem Ergebnis gelangt, dass den Anforderungen der Verbraucherkreditrichtlinie 2008 an eine klare und prägnante Belehrung des Verbraucherdarlehensnehmers dann nicht genügt ist, wenn der Darlehensvertrag hinsichtlich der Pflichtangaben zum Beginn der Widerrufsfrist auf eine nationale Vorschrift verweist, die wiederum auf weitere Normen in anderen Gesetzeswerken Bezug nimmt. Damit stellt sich der EuGH gerade auch gegen den Inhalt der Musterwiderrufsbelehrung nach Anlage 7 zum EGBGB, die eine solche sog. „Kaskadenverweisung" vorsieht und bei deren Verwendung die Widerrufsbelehrung nach der Gesetzlichkeitsfiktion in Art. 247 § 6 Abs. 2 Satz 3 EGBGB den gesetzlichen Bestimmungen genügt. Die Folgen dieser EuGH-Entscheidung für das deutsche Recht sind allerdings überaus begrenzt; geboten ist aber ein zeitnahes Tätigwerden des deutschen Privatrechtsgesetzgebers.

I. Einleitung

Die Entwicklung der vergangenen Jahre hat eindrucksvoll gezeigt, dass die Qualifikation des Widerrufsrechts als prozedurales Instrument der Vertragsgerechtigkeit[1)] in der Rechtspraxis u. a. bei Verbraucherdarlehen in den Hintergrund getreten ist. Der Schutz der tatsächlichen Entscheidungsfreiheit durch die Möglichkeit des Verbrauchers, seine Vertragsentscheidung angesichts der wirtschaftlichen Bedeutung und Tragweite von Krediten zu prüfen und nochmals befristet abzuwägen, wurde vom Gesetzgeber als legitimer Zweck eines befristeten, einseitigen Rechts des Verbrauchers anerkannt, sich vom Verbraucherkreditvertrag zu lösen.[2)] In der Praxis hat sich dieses Widerrufsrecht allerdings als Mittel zur rechtsgrundlosen Lösung von zwischenzeitlich unliebsamen Verträgen unabhängig von diesem gesetzgeberischen Zweck entwickelt. Erheblich dazu beigetragen hat der unionsrechtsinduzierte Webfehler der Anknüpfung der Widerrufsfrist an eine ordnungsgemäße Widerrufsbelehrung ohne Ausschlussfrist.[3)] Hierdurch wird dem Darlehensnehmer beim Verbraucherdarlehen ermöglicht, sich nach Jahr und Tag von dem mittlerweile unliebsamen Vertrag gestützt auf mehr oder (häufig) weniger bedeutende Defizite in der Widerrufsbelehrung zu lösen.[4)] Nur auf den ersten Blick scheint die Entscheidung des EuGH vom 26. 3. 2020,[5)] die auf eine Vorabentscheidungsvorlage des LG Saarbrücken[6)] ergangen ist, den Grundstein für eine neue „Welle" von entsprechenden Widerrufen von Verbraucherdarlehen zu legen. Bei näherer Analyse zeigt sich indes sehr deutlich, dass diese Befürchtung unbegründet ist. Aus Gründen der Rechtssicherheit ist aber der deutsche Privatrechtsgesetzgeber gefordert, die Musterwiderrufsbelehrung mit Gesetzlichkeitsfiktion umgehend an die vom EuGH nunmehr weiter konkretisierten Vorgaben der Verbraucherkreditrichtlinie[7)] anzupassen. Darüber hinaus gibt die EuGH-Entscheidung Anlass, in Zukunft den Fokus im Unionsrecht wie auch im nationalen Recht verstärkt auf die Kernfrage zu richten, ob jedes, gegebenenfalls auch marginales Defizit der Widerrufsbelehrung das Anlaufen der Widerrufsfrist hindern und eine fundamentale Verschiebung des Vertragsgefüges einschließlich der grundsätzlichen Verteilung der Vertragsrisiken rechtfertigen kann.[8)]

II. Die Entscheidung des EuGH vom 26. 3. 2020

Die Entscheidung des EuGH vom 26. 3. 2020, die ohne Schlussanträge über die Rechtssache erging, beantwortet die Vorlagefragen der Vorabentscheidungsvorlage nach Art. 267 AEUV

*) *Prof. Dr. iur, LL.M. (Duke), ist Inhaber des Lehrstuhls für Bürgerliches Recht, Handels- und Gesellschaftsrecht, Europarecht und Rechtstheorie an der Universität Regensburg.*

1) Vgl. *Canaris*, AcP 200 (2000), 273, 344.

2) So Begr RegE BT-Drucks. 11/5462, S. 21 zu § 7 VerbrKrG.

3) Dieser Webfehler besteht auch nach der Einfügung von § 356b Abs. 2 Satz 4 bei Allgemein-Verbraucherdarlehensverträgen fort; s. a. zur Schaffung von Rechtssicherheit durch die Vermeidung eines vermeintlich „ewigen" Widerrufsrechts bei Immobiliar-Verbraucherdarlehensverträgen, Begr RegE, BT-Drucks. 18/5922, S. 74; BT-Drucks. 18/7584, S. 155 f.

4) Vgl. zur Kritik am sog. „Widerrufsjoker" schon *Herresthal*, ZIP 2018, 753 f.

5) EuGH v. 26. 3. 2020 – Rs C-66/19, ECLI:EU:C:2020:242 = ZIP 2020, 663.

6) LG Saarbrücken v. 17. 1. 2019 – 1 O 164/18, ZIP 2019, 1952, dazu EWiR 2019, 677 *(Koch/Biggen)*.

7) RL 2008/48/EG des Europäischen Parlaments und des Rates vom 23. 4. 2008 über Verbraucherkreditverträge und zur Aufhebung der RL 87/102/EWG des Rates, ABl EG Nr. L 133, S. 66; vgl. dazu Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdienste Richtlinie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht, BGBl I 2009, 2355 ff.

8) Neben dem Institut der Verwirkung, zusammenfassend BGH v. 18. 2. 2020 – XI ZR 25/19, BeckRS 2020, 3950, und dem Rechtsmissbrauch, vgl. *Herresthal*, NJW 2019, 13, ist insbesondere das Verhältnismäßigkeitsprinzip im Unionsrecht selbst hinsichtlich der Wirkung geringfügiger Belehrungsdefizite für den Lauf der Widerrufsfrist und die Möglichkeit, sich nach Jahr und Tag von einem geschlossenen Vertrag zu lösen, noch näher in Blick zu nehmen.