Ministerium der Justiz
des Landes Nordrhein-Westfalen

Arbeitsgruppe „Digitaler Neustart“

der Konferenz der Justizministerinnen und Justizminister der Länder

Berichte vom 1. Oktober 2018 und 15. April 2019

Baden-Württemberg | Bayern | Berlin | Hamburg | Hessen

Niedersachsen | Nordrhein-Westfalen | Saarland | Sachsen | Schleswig-Holstein

www.justiz.nrw

Bericht vom 1. Oktober 2018

Big Data

Algorithmentransparenz

Gesundheitsdaten

Bericht vom 15. April 2019

Robotic Law

Blockchain

Leistungsschutzrecht an Daten

Inhaltsverzeichnis

Bericht vom 1. Oktober 2018 (S. 3 ff.)
Bericht vom 15. April 2019 (S. 129 ff.)

Bericht vom 1. Oktober 2018 3

Zusammenfassung und Ergebnisse 3

Vorgehensweise der Arbeitsgruppe 4

A. Beschlusslage 4
B. Arbeitsauftrag 5
C. Tätigkeit der Arbeitsgruppe 6

Kapitel 1: Big Data 8

A. Vorbemerkung 8
B. Algorithmen 9
   I. Begriff des Algorithmus 9
   II. Anwendungsgebiete von Algorithmen im Kontext des Arbeitsauftrages 17
C. Bestehender Rechtsrahmen für Big Data-Anwendungen 27
   I. Verfassungsrecht 27
   II. Datenschutzrecht 33
   III. Allgemeines Gleichbehandlungsgesetz 51
   IV. Kartellrecht 60
D. Abstrakte Betrachtung der rechtspolitischen Handlungsoptionen 61
   I. Erkenntnisse aus anderen Rechtsgebieten: Finanzmarktrecht 61
   II. Untersuchung rechtspolitischer Handlungsoptionen 65
E. Konkrete Betrachtung rechtspolitischer Handlungsoptionen für personalisierte Newsfeeds, personalisierte Werbung und personalisierte Preise 71
   I. Personalisierte Newsfeeds 71

II. Personalisierte Werbung 75
III. Personalisierte Preise 93
F. Ergebnis 102

Kapitel 2: Gesundheitsdatenschutz 103

A. Vorbemerkung 103
B. Begriffsbestimmungen 104
I. Definition „Fitness-Tracker“ 104
II. Definition „Gesundheitsdaten“ 106
C. Stand der Diskussion in Literatur und Rechtsprechung 107
I. Diskussionsstand im Hinblick auf private Versicherungen 107
II. Diskussionsstand/ übertragbare Argumentationen im Hinblick auf gesetzliche Krankenversicherungen 111
III. Zu berücksichtigende bzw. übertragbare Rechtsprechung des Bundesverfassungsgerichts 114
IV. Europarechtliche Zulässigkeit einschränkender Regelungen im Hinblick auf die Datenschutz-Grundverordnung 117
D. Stellungnahme 118
E. Regelungsvorschlag 123
F. Ergebnis 124

Literaturverzeichnis 125

Bericht vom 1. Oktober 2018

Zusammenfassung und Ergebnisse

Die Überlegungen der Arbeitsgruppe sind nach wie vor von dem Grundsatz getragen, dass kein gesetzgeberischer Handlungsbedarf besteht, soweit und solange das geltende („analoge“) Recht tragfähige Normen für die Folgen der Digitalisierung bereithält und es den Gerichten überantwortet werden kann, die neuen Sachverhalte durch Subsumtion unter vorhandene Normen sachgerechten Lösungen zuzuführen. Zudem ist eine Etablierung unterschiedlicher Regelungsregime für analoge und digitale Sachverhalte und damit eine weitere Fragmentierung des Rechts zu vermeiden. Etwaigem gesetzgeberischen Handlungsbedarf ist daher primär dadurch Rechnung zu tragen, dass die bereits vorhandenen Regelungsregime gegebenenfalls durch gezielte Sondervorschriften ergänzt werden.

Unter Berücksichtigung dessen sieht die Arbeitsgruppe gesetzgeberischen Handlungsbedarf hinsichtlich folgender Punkte:

- Bei der Erstellung personalisierter Trefferlisten im Internet sollten die wesentlichen Kriterien des Sortieralgorithmus offengelegt werden.
- Der Einsatz algorithmischer Entscheidungsfindung darf nicht zu Erleichterungen im Rahmen des Entlastungsbeweises nach § 21 Abs. 2 S. 2 AGG führen.
- Bei der Verwendung personalisierter Preise im Rahmen von Vertragsbeziehungen im Internet sollten die Unternehmen verpflichtet werden, dem Verbraucher gegenüber die Tatsache des Einsatzes algorithmischer Entscheidungssysteme zur personalisierten Preisbildung offenzulegen, ohne weitere Details der Preisfindung preisgeben zu müssen („transparentes Preisschild“).
- Die laufende Erhebung personenbezogener Gesundheitsdaten zu Zwecken der Tarifgestaltung in der privaten Krankenversicherung sollte für unzulässig erklärt werden.

Vorgehensweise der Arbeitsgruppe

A. Beschlusslage

Mit Beschluss zu TOP I.2 „Bericht der Länderarbeitsgruppe Digitaler Neustart“ der Frühjahrskonferenz vom 21. und 22. Juni 2017 in Deidesheim billigten und würdigten die Justizministerinnen und Justizminister den Bericht ihrer mit Beschluss vom 17. und 18. Juni 2015 eingesetzten Länderarbeitsgruppe „Digitaler Neustart“ und erteilten dieser folgenden Arbeitsauftrag:

„Die Justizministerinnen und Justizminister sind sich darin einig, dass die Arbeitsgruppe die Diskussion um die zivilrechtlichen Folgen der Digitalisierung, sowohl auf nationaler als auch europäischer Ebene, weiter begleiten soll. Unter diesem Aspekt beauftragen sie die Arbeitsgruppe, ihre Arbeit fortzusetzen und

a) sich vertieft mit bisher ausgeklammerten Themen, insbesondere den zivilrechtlichen Aspekten im Zusammenhang mit „Big Data“, zu befassen, sowie gegebenenfalls auch Fragestellungen, die sich aus der Dynamik der digitalen Entwicklung perspektivisch ergeben, aufzugreifen,

b) die bereits behandelten Themen im Blick zu halten und auf der Grundlage des Berichts den Austausch mit der Fachöffentlichkeit zu suchen und

c) bei Bedarf einzelne Themen wieder aufzugreifen und nochmals einer speziellen Prüfung zu unterziehen.“

Unter TOP I. 9 „Marktmacht und Datenhoheit im Recht – Algorithmentransparenz bei Vertragsbeziehungen im Internet schaffen“ erteilten die Justizministerinnen und Justizminister der Länderarbeitsgruppe im Rahmen ihrer Konferenz vom 21.und 22. Juni 2017 verbunden mit einer Positionierung in der Sache folgenden weiteren Arbeitsauftrag:

„1. Die Justizministerinnen und Justizminister stellen fest, dass durch den Einsatz von Algorithmen immer mehr Daten über Internetnutzerinnen und -nutzer gesammelt und diese bei der Erstellung von Angeboten (auch beim Preis) eingesetzt werden. Für die Nutzerinnen und Nutzer ist dabei oft nicht erkennbar, auf welchen Kriterien mittels Algorithmen entstandene Werbe- oder Vertragsangebote beruhen. Dies deutet auf ein Missverhältnis zwischen Nutzer- und Anbieterseite hin. Um informierte und selbstbestimmte Entscheidungen zu ermöglichen, halten die Justizministerinnen und Justizminister eine Prüfung für erforderlich, wie die wesentlichen Kriterien, aufgrund derer Algorithmen entscheiden, überprüfbar und für die Nutzerinnen und Nutzer besser erkennbar gemacht werden können.

2. *Die Justizministerinnen und Justizminister bitten daher die Arbeitsgruppe „Digitaler Neustart“ um Prüfung, ob und gegebenenfalls welche rechtlichen Anpassungen geboten sind. Die Arbeitsgruppe wird gebeten, einen Zwischenbericht bis zur Justizministerkonferenz im Frühjahr 2018 vorzulegen.“*

Schließlich beschlossen die Justizministerinnen und Justizminister im Rahmen der vorbezeichneten Frühjahrskonferenz in Deidesheim unter TOP I.10 „Marktmacht und Datenhoheit im Recht – vertragliche Vereinbarungen über höchstpersönliche Gesundheitsdaten regeln“:

„*1. Die Justizministerinnen und Justizminister nehmen zur Kenntnis, dass sensible private Gesundheitsdaten zum Gegenstand von vertraglichen Vereinbarungen über die Tarifhöhe bei privaten Versicherungen werden. Sollten sich derartige Geschäftsmodelle künftig durchsetzen, droht ein mittelbarer Zwang zur Ermittlung und zur Preisgabe derartiger hochsensibler Daten.*

2. *Die Justizministerinnen und Justizminister bitten daher die Arbeitsgruppe „Digitaler Neustart“ um Prüfung, ob und gegebenenfalls durch welche Maßnahmen sensible Gesundheitsdaten wirksam gegen die Kommerzialisierung geschützt werden sollten.“*

B. Arbeitsauftrag

Der aus den vorstehend aufgeführten Beschlüssen folgende Arbeitsauftrag an die Arbeitsgruppe lässt sich in die Themen „Big Data“, mit dem Unterthema „Algorithmen“, sowie „Gesundheitsdatenschutz“ aufgliedern.

Im Bereich „Algorithmen“ ist das Zivilrecht in den Blick zu nehmen und hier insbesondere das Vertragsrecht, für das unter dem Gesichtspunkt des Schutzes der Privatautonomie die Erforderlichkeit und bei deren Bejahung die mögliche Ausgestaltung rechtlicher Anpassungen in Bezug auf algorithmenbasierte Werbe- und Vertragsangebote geprüft werden soll, die darauf abzielen, die Kriterien, aufgrund derer Algorithmen entscheiden, transparenter zu machen. Hinsichtlich der algorithmischen Entscheidungsfindung als solcher geht es insbesondere um das Phänomen, dass personenbezogene Daten der Nutzer erhoben werden und bei der algorithmischen Entscheidungsfindung Verwendung finden („Personalisierung“).

Ferner bezieht sich der Arbeitsauftrag auf das private Versicherungsrecht, für das vor dem Hintergrund vertraglicher Gestaltungen, die die Überlassung sensibler Gesundheitsdaten zum Gegenstand von Vereinbarungen über die Tarifhöhe

machen, geprüft werden soll, ob und gegebenenfalls auf welche Weise Gesundheitsdaten wirksam gegen Kommerzialisierung geschützt werden können.

Demgegenüber werden mit Blick auf die thematische Begrenzung des Arbeitsauftrags andere Anwendungsbereiche algorithmenbasierter Entscheidungsfindung im vorliegenden Bericht nicht näher untersucht. Zu diesen nachfolgend nicht ausdrücklich behandelten Anwendungen gehört beispielsweise der Einsatz von Algorithmen bei der Personalauswahl im Rahmen der Mitarbeitergewinnung und der Vergabe von Führungspositionen in Unternehmen[1] oder bei der Bonitätsprüfung im Vorfeld einer Kreditvergabeentscheidung (sogenanntes „Kreditscoring“).[2]
Schließlich soll seitens der Arbeitsgruppe der mit den zu untersuchenden Fragestellungen verbundene rechtspolitische Handlungsbedarf in Bezug auf den digitalen „Ist – Zustand“ abgeklärt werden.

C. Tätigkeit der Arbeitsgruppe

Die Auftaktsitzung der Länderarbeitsgruppe unter Federführung Nordrhein-Westfalens fand am 26. September 2017 in der Landesvertretung Nordrhein-Westfalens beim Bund unter Beteiligung der Länder Baden-Württemberg, Bayern, Berlin, Freie und Hansestadt Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein sowie des Bundesministeriums der Justiz und für Verbraucherschutz statt.

Zur weiteren Bearbeitung wurde die Einrichtung zweier Arbeitsgruppen zu den Themenbereichen „Big Data, Algorithmentransparenz und Gesundheitsdaten“ unter Federführung Hessens (Arbeitsgruppe 1) und „Robotic Law (einschließlich Haftungsfragen und selbstlernende Algorithmen), Blockchain und Leistungsschutzrecht an Daten“ (Arbeitsgruppe 2) unter der Gesamtfederführung Nordrhein-Westfalens eingerichtet, die sich ihrerseits in drei Unterarbeitsgruppen untergliedert.

An der Arbeitsgruppe 1 unter Federführung Hessens wirkten die Länder Baden-Württemberg, Freie und Hansestadt Hamburg, Saarland und Schleswig-Holstein mit. Die Arbeitsgruppe 1 traf sich nach einer ersten vorbereitenden Besprechung im Anschluss an die Sitzung der Bund-Länder-Arbeitsgruppe am 26. September 2017 zu einer Sachverständigenanhörung am 24. November 2017 in Saarbrücken.

---

[1] Vgl. *Werle*, Der Bierfaktor im Bewerbungsgespräch, Karriere-Spiegel vom 14.2.2017, abrufbar unter: http://www.spiegel.de/karriere/recruiting-unternehmen-setzen-verstaerkt-auf-algorithmen-a-1132633.html (letzter Abruf: 25.8.2018).
[2] *Lobe*, Wenn Algorithmen über die Bonität entscheiden, Der Standard vom 6.2.2015, abrufbar unter: https://derstandard.at/2000011340593/Wenn-Algorithmen-ueber-die-Bonitaet-entscheiden (letzter Abruf: 25.8.2018).

Im Rahmen der ganztätigen Veranstaltung vermittelten Prof. Dr. Mehlhorn (Direktor am Max-Planck Institut für Informatik, Saarbrücken) und Dr. Andreas Karrenbauer (Senior Researcher am Max-Planck Institut für Informatik, Saarbrücken) sowie Prof. Dr. Katharina Zweig (Professorin an der TU Kaiserslautern, Mitbegründerin der Initiative „Algorithm Watch“) in Form von Vorträgen und Workshops den Mitgliedern der Arbeitsgruppe zunächst ein technisches Verständnis der Materie. Die gewonnenen Erkenntnisse wurden in den folgenden Sitzungen rechtlich bewertet.

Kapitel 1: Big Data

A. Vorbemerkung

Unter dem Begriff Big Data ist ein Bündel neu entwickelter Methoden und Technologien zu verstehen, das die Erfassung, Speicherung und Analyse eines großen und beliebig erweiterbaren Volumens unterschiedlich strukturierter Daten ermöglicht. Charakteristisch für Big Data ist die Datenmenge (Volume), die Geschwindigkeit (Velocity) und die unterschiedliche Beschaffenheit (Variety) der komplex und vielfältig strukturierten Quellen wie zum Beispiel soziale Netzwerke, Fotos, Videos, Blogs, MP3-Dateien, E-Mails, Tweeds, Sensoren intelligenter Geräte.[3]

Mittlerweile generieren technische Geräte, Internetseiten und Software-Anwendungen massenhaft personen- oder nichtpersonenbezogene Daten, die in „Datenraffinerien“[4] aufbereitet, gespeichert und für die weitere Nutzung bereitgestellt werden. Die Aufbereitung verschiedener Sammlungen bestimmter Datentypen durch die Datenraffinerien führt dazu, dass die so geschaffenen „Datencontainer“ von Abnehmern maschinenlesbar neu miteinander kombiniert und so völlig neue, bisher unbekannte Korrelationen aufgedeckt werden können. So können Daten für neue Zwecke nutzbar gemacht werden und betroffene Personen mittels eines auf der Auswertung basierenden Profilings beispielsweise zum Ziel eines feinabgestimmten Direktmarketings werden. Letztendlich trifft man durch Big Data-Anwendungen Aussagen über statistische Korrelationen.

Es gibt kaum einen Bereich gesellschaftlichen Lebens, in dem keine Anwendungsgebiete von Big Data denkbar sind. Besonderes Potenzial erhofft man sich auf dem Gebiet der Früherkennung und Behandlung von Krankheiten, der Entwicklung neuer Therapien mittels personalisierter Medizin und Präzisionsmedizin, der Verhütung und Bewältigung großer Naturkatastrophen, der Verkürzung von Entwurfs- und Produktionszyklen in der Industrie und der Beschleunigung der Konzeption neuer Werkstoffe. Auch für die nationale Sicherheit und Verteidigung werden Anwendungsbereiche etwa in der Entwicklung komplexer Verschlüsselungstechniken sowie in der Rückverfolgung von Cyberangriffen und entsprechenden Abwehrmaßnahmen gesehen.[5]

---

[3] *Sabine Horvath*, Wissenschaftlicher Dienst des Deutschen Bundestages: „Aktueller Begriff Big Data“ unter https://www.bundestag.de/blob/194790/.../big_data-data.pdf; (letzter Abruf: 25.8.2018).

[4] Vgl. *Andreas Weigend*, Data For The People, S. 31 ff..

[5] Vgl. Vorschlag für eine Verordnung des Rates zu Gründung des gemeinsamen Unternehmens für europäisches Hochleistungsrechnen (COM (2018) 8 final).

Gleichzeitig kristallisieren sich Anwendungsbereiche heraus, die Risiken bergen oder schlicht mit unserem Rechtssystem unvereinbar sind. So berechnet in fast jedem US-Bundesstaat vor Gericht eine Software die Rückfallwahrscheinlichkeit von Straftätern. In Großbritannien und den Vereinigten Staaten werden Bewerber auf einen Arbeitsplatz in online - Auswahlverfahren ohne menschliche Beteiligungen aussortiert. Dabei werden auch Erkenntnisse, die im Rahmen des Kreditscorings gewonnen wurden, verarbeitet.

B. Algorithmen

Als Unterkategorie zum Thema Big Data kann man Algorithmen begreifen. Diese kommen bei Big Data-Anwendungen bei den unterschiedlichsten Datenverarbeitungsschritten zum Einsatz.[6]

I. Begriff des Algorithmus

1. Zum Begriff des Algorithmus im Allgemeinen

Algorithmen sind nicht erst im „Digitalen Zeitalter“[7] entwickelt worden. Vielmehr wird etwa der von Euklid im dritten Jahrhundert vor Christus in seiner Schrift „Die Elemente“ niedergelegte „Euklidische Algorithmus“ als einer der frühesten schriftlichen Verkörperungen von Algorithmen angesehen.[8] Der Begriff des Algorithmus wird auf den persischen Gelehrten Abu Ja`far Muhammad ibn Musa al-Chwarizmi[9] zurückgeführt, der in einer Schrift aus dem 9. Jahrhundert nach Christus ein mathematisches Lehrbuch über die indischen Zahlen verfasst hatte, das die Basis für das heutige Dezimalsystem gelegt haben soll und dessen

---

[6] Zur Definition des Begriffs „Datenverarbeitung“ vgl. Art. 4 Nr. 2 der Datenschutz-Grundverordnung (DS-GVO).

[7] So wörtlich: *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 Fußnote 2. Der Beginn des „Digitalen Zeitalters“ wird im Jahr 2002 verortet, da die Menschheit in diesem Jahr erstmals in der Lage gewesen sein soll, mehr Informationen digital als analog zu speichern: https://de.wikipedia.org/wiki/Digitale_Revolution#cite_note-HilbertLopez2011-2 (letzter Abruf: 25.8.2018).

[8] *Ziegenbalg/Ziegenbalg/Ziegenbalg*, Algorithmen von Hammurapi bis Gödel, S. 9, abrufbar unter http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf ((letzter Abruf: 25.8.2018).

[9] Die Schreibweise für den Namen variiert teilweise, so dass sich etwa anstelle von „al-Chwarizmi“ „al-Khowarizm“ oder „al-Khwarismi“ sowie andere Schreibweisen zu finden sind. So etwa bei: *Ziegenbalg et al*, S. 19, http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf: 25.8.2018), bei: https://de.wikipedia.org/wiki/Al-Chwarizmi (letzter Abruf: 25.8.2018), *Zweig*, Arbeitspapier: Was ist ein Algorithmus?, abrufbar unter: https://algorithmwatch.org/de/arbeitspapier-was-ist-ein-algorithmus/ oder http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/Algorithmus/index.html (letzter Abruf: 25.8.2018).

lateinische Übersetzung seines vom Geburtsort abgeleiteten Namensbestandteils „al-Chwarizmi“ „Algoritmi“ lautete.[10]

Der Begriff Algorithmen umfasst in seiner allgemeinsten, fachdisziplinen-übergreifenden Bedeutung ein aus einzelnen Handlungsschritten bestehendes abstrakt und abschließend definiertes „schematisches Problemlösungsverfahren“[11]. Anders ausgedrückt geht es um einen „Lösungsplan“[12], der in detailliert umschriebenen, miteinander verknüpften Lösungsschritten „Eingabedaten in Ausgabedaten“ umsetzt.[13] Damit reicht die Anwendungsbreite von alltäglichen Handlungsleitfäden wie hinreichend präzise verfassten[14] Kochrezepten, Bedienungsanleitungen, Formeln zur Berechnung des sogenannten Body-Mass-Index (BMI)[15] oder zur Bestimmung des Osterdatums nach dem gregorianischen Kalender (sogen. „Oster-Algorithmus“)[16] bis hin zu Aufgabenlösungsanleitungen in den unterschiedlichsten Gebieten der Wissenschaft (Logik, Philosophie, mathematische Wissenschaften, Sprachwissenschaften, Sozialwissenschaft, Naturwissenschaften).[17]
Eine elementare Rolle spielen Algorithmen in der Mathematik und in der Informatik. Ihre Bedeutung für diese beiden Wissenschaften in der Gesamtschau wird dahingehend beschrieben, dass die Algorithmik ein zentrales Themengebiet ist, in dem sich beide Wissenschaften „überschneiden“ und sich thematische

[10] *Ziegenbalg et al*, S. 19, http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf: 25.8.2018); https://de.wikipedia.org/wiki/Al-Chwarizmi; *Zweig, Katharina*, Arbeitspapier: Was ist ein Algorithmus? Abrufbar unter: https://algorithmwatch.org/de/arbeitspapier-was-ist-ein-algorithmus/ (letzter Abruf: 25.8.2018).
[11] *Broy*, Informatik. Eine grundlegende Einführung, S. 31; *Mellouli*, Algorithmen in: Enzyklopädie der Wirtschaftsinformatik. Online Lexikon, abrufbar unter: http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/Algorithmus/index.html (letzter Abruf: 25.8.2018).
[12] *Czernik*, Was ist ein Algorithmus? – Definition und Beispiele, abrufbar unter: https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/ (letzter Abruf: 25.8.2018).
[13] *Czernik*, Was ist ein Algorithmus? – Definition und Beispiele, abrufbar unter https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/ (letzter Abruf 25.8.2018).
[14] Da eine charakteristische Eigenschaft von Algorithmen darin besteht, dass sie zu einem reproduzierbaren Ergebnis führen, erfüllt ein Kochrezept die Anforderungen an einen Algorithmus nur, wenn es so bestimmt verfasst ist, dass es keine „Auslegungsspielräume“ enthält, die auf Erfahrungswissen des Verwenders abzielen: *Hromkovic*, Sieben Wunder der Informatik, S. 37.
[15] *Czernik*, Was ist ein Algorithmus? – Definition und Beispiele, abrufbar unter: https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/ (letzter Abruf 25.8.2018).
[16] Vgl. zur „Gaußschen Osterformel“: https://de.wikipedia.org/wiki/Gau%C3%9Fsche_Osterformel (letzter Abruf 25.8.2018).
[17] https://de.wikipedia.org/wiki/Algorithmus (letzter Abruf 25.8.2018); *Ziegenbalg et al*, S. 18, http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf 25.8.2018).

Schnittmengen bilden.[18] Aber auch in der Mathematik und Informatik gibt es, soweit ersichtlich, keine „allgemein anerkannte“ Definition des Algorithmus[19]. Hier wie in einschlägigen Enzyklopädien[20] finden sich vielmehr zahlreiche, häufig in den Kernelementen übereinstimmende Definitionen, die der eingangs angeführten allgemeinen Begriffsumschreibung nahe kommen.[21] Ist der Algorithmus in einer „Sprache“ bzw. einer Zeichenabfolge formuliert, der einer Ausführung durch einen Computer zugänglich ist, so spricht man von einem „Programm“.[22]

Bei aller begrifflichen Unschärfe gibt es gleichwohl charakteristische Eigenschaften von Algorithmen, die nach jedenfalls verbreiteter Auffassung für Algorithmen prägend sind und daher zu deren Umschreibung herangezogen werden können.

Demnach muss das Problemlösungsverfahren, das einen Algorithmus ausmacht, in einem endlichen Text bzw. einer endlichen Zeichenfolge beschrieben sein („Endlichkeit“)[23], so präzise formuliert sein, dass es von Mensch und/oder Computer ohne Weiteres umgesetzt werden kann („Eindeutigkeit“[24] und „Ausführbarkeit“[25]) und schließlich ein die Aufgabenstellung zutreffend lösendes, bei gleicher Dateneingabe reproduzierbares Ergebnis liefern

---

[18] https://de.wikipedia.org/wiki/Algorithmus (letzter Abruf 25.8.2018); *Ziegenbalg et al*, S. 18, http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (abgerufen am 10.1.2018).

[19] *Promberger/Dobler*, Algorithmen und Datenstrukturen, S. 32.

[20] Vgl. etwa die Zusammenstellung bei: *Ziegenbalg et al*, S. 21 – 23, http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (abgerufen am 10.1.2018).

[21] So etwa: *Vieth/Müller-Eiselt*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 9, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf 25.8.2018) in Anlehnung an die klassische Definition von *Cormen/Leiserson/Rivest/Stein*, Introduction to Algorithms; vgl. etwa auch die Definition bei *Broy*, Informatik. Eine grundlegende Einführung, S. 31 oder bei *Ziegenbalg et al*, S. 23, abrufbar unter: http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf 25.8.2018).

[22] *Ziegenbalg et al*, S. 25, abrufbar unter: http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf; Promberger/Dobler, Algorithmen und Datenstrukturen, S. 82.

[23] *Promberger/Dobler*, Algorithmen und Datenstrukturen, S. 34; abrufbar unter https://de.wikipedia.org/wiki/Algorithmus#Algorithmus_und_Programme; Ziegenbalg et al, S. 18 (letzter Abruf: 25.8.2018), http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf: 25.8.2018).

[24] *Promberger/Dobler*, Algorithmen und Datenstrukturen, S. 34; *Cormen*, Algorithms unlocked, S. 1 f.; *Ziegenbalg et al*, S. 24, abrufbar unter: http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf: 25.8.2018).

[25] *Promberger/Dobler*, Algorithmen und Datenstrukturen, S. 34; abrufbar unter https://de.wikipedia.org/wiki/Algorithmus#Algorithmus_und_Programme.

(„Korrektheit“)[26]. Ferner wird, wenn dies auch keine essentielle Eigenschaft eines Algorithmus sein mag, gefordert, dass der Algorithmus bei jedweder Dateneingabe zur Vermeidung einer sogenannten „Endlosschleife“ nach einer endlichen Zahl von Schritten zu einem Ende kommt[27] und „zeiteffizient“ ausgelegt ist.[28]

2. Zum Begriff des Algorithmus im Kontext der Diskussion um die Algorithmenregulierung

Die obige Darstellung der vielfältigen Einsatzmöglichkeiten zeigt, dass man algorithmische Entscheidungssysteme nicht per se fürchten muss. Viele algorithmische Entscheidungssysteme bergen weder Gefahren, noch drohen Diskriminierungen oder Teilhabeausschluss. Beispielhaft kann hier das Navigationssystem genannt werden, dass mit einem mehr oder weniger tauglichen Schnellster-Weg-Algorithmus ausgestattet ist. Im schlechtesten Fall weist der Algorithmus einfach nicht den schnellsten Weg aus. Die Verbraucher werden das Produkt meiden, da es den gewünschten Erfolg nicht herbeiführt. Eine staatliche Kontrolle ist nicht erforderlich.

Darüber hinaus drängt sich rein praktisch ferner auf, dass es kein einheitliches Kontrollwerkzeug für alle erdenklichen algorithmischen Entscheidungssysteme geben wird. Ganz allgemeine Kontrollen scheitern bereits an der Vielfältigkeit und schlichten Masse von Algorithmen. Matt Cutts, Head of Googles Webspam Team, wurde beispielsweise damit zitiert, dass Google im Verlauf des Jahres 2012 665 Änderungen am Ranking-Algorithmus vorgenommen habe.[29] Jede dieser Änderungen im Einzelnen nachzuvollziehen, dürfte schlicht nicht leistbar sein.
Wenn es um die Kontrolle von algorithmischen Entscheidungssystemen geht, ist vielmehr sektorspezifisch zu fragen, in welchen Bereichen diese in besonderem Maße Risiken in sich bergen, die sich im hier zu untersuchenden Bereich des Zivilrechts beispielsweise in Form von Diskriminierung und Teilhabeausschluss ausdrücken. So wie eine rein menschlich getroffene Entscheidung ohne Zuhilfenahme technischer Einrichtungen nicht neutral ist, ist dies auch kein

---

[26] *Promberger/Dobler*, Algorithmen und Datenstrukturen, S. 34; *Cormen*, Algorithms unlocked, S. 2.
[27] Teilweise wird dies auch für eine unverzichtbare Eigenschaft von Algorithmen gehalten: https://www.datenschutzbeauftragter-info.de/was-ist-ein-algorithmus-definition-und-beispiele/ (letzter Abruf 25.08.2018); a.A.: *Ziegenbalg et al*, S. 24, abrufbar unter: http://www.ziegenbalg.ph-karlsruhe.de/materialien-homepage-jzbg/Manuskripte/AHG-1u2.pdf (letzter Abruf 25.8.2018).
[28] *Cormen*, Algorithms unlocked, S. 4; abrufbar unter https://de.wikipedia.org/wiki/Algorithmus#Algorithmus_und_Programme (letzter Abruf 25.8.2018).
[29] https://www.sistrix.de/frag-sistrix/google-algorithmus-aenderungen/google-page-layout-algorithm-update-ads-above-the-fold/wie-haeufig-nimmt-google-algorithmus-aenderungen-vor/ (letzter Abruf: 25.8.2018).

Algorithmus.[30] Wissenschaftler, Algorithmendesigner und Programmierer entwickeln eine Handlungsanweisung, die potentiell millionenfach ausgeführt wird, ohne dass die physische Anwesenheit der Entwickler erforderlich ist und ohne die Begrenzung menschlicher Kapazitäten.[31] Im Laufe des Entwicklungsprozesses kann es, bewusst oder unbewusst, zu Weichenstellungen kommen, die nachher in der Anwendung zu diskriminierenden Ergebnissen führen. Denkbar sind konzeptionelle Fehler im Algorithmendesign, die dazu führen, dass der Algorithmus das mathematische Problem, für das er entwickelt wurde, schlicht nicht löst.[32] Denkbar sind ferner Implementierungsfehler. Hierbei wird beispielsweise der eigentlich korrekte Algorithmus fehlerhaft programmiert. Bedeutsam sind auch Fehler in der Modellierungsphase. Bei der Modellierung werden Modellierungsentscheidungen getroffen. Für das „Kürzeste-Wege-Problem" muss zum Beispiel genau festgelegt werden, welche Arten von Daten genutzt werden können (aktuelle Verkehrsdichte, Kapazitäten der Straßen, Länge der Straßen, aktuelle Baustellen) und nach welchen Parametern optimiert werden soll (Minimierung der Gesamtlänge oder Minimierung der Fahrtzeit oder möglichst schöne Strecke oder möglichst wenig Autobahn). An dieser Stelle ist Platz für subjektive Entscheidungen der Designer. Die nächste Fehlerquelle besteht in fehlerhaften oder unzureichenden Daten. Der Algorithmus benötigt Eingabedaten, die in ihrer Qualität stark variieren können. Insbesondere bei selbstlernenden Algorithmen können die Daten zum Training des Algorithmus unzureichend sein, indem nicht genügend Daten für alle zu unterscheidenden Klassen vorhanden sind. Schließlich kann auch ein an sich korrekter Algorithmus aufgrund der Interaktion mit den Nutzern zu gesellschaftlich unerwünschten Nebenwirkungen führen. Dieses Phänomen ist insbesondere bei der automatischen Suchvervollständigung aufgetreten.

In Kenntnis möglicher Fehlerquellen sind zunächst diejenigen Algorithmen zu extrahieren, die von Computerprogrammen mit „Außenwirkung" gegenüber Dritten, seien es Nutzer der Programme oder sonstige Betroffene, ausgeführt werden.[33] Diese Algorithmen entfalten regelmäßig Außenwirkung durch das Treffen von Entscheidungen, die die Belange des Nutzers oder der sonstigen Betroffenen berühren, da sie in Entscheidungssysteme eingebunden sind. Dies

---

[30] *Busch*, Algorithm Accountability, S. 20, abrufbar unter: http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf (letzter Abruf 25.8.2018).

[31] *Zweig*, Algorithm Watch, 1. Arbeitspapier: Was ist ein Algorithmus, abrufbar unter: https://algorithmwatch.org/de/arbeitspapier-was-ist-ein-algorithmus/ (letzter Abruf: 25.8.2018).

[32] Vollständige Darstellung der Fehlerquellen in: *Zweig*, Algorithm Watch, 2. Arbeitspapier: Überprüfbarkeit von Algorithmen, abrufbar unter https://algorithmwatch.org/de/zweites-arbeitspapier-überprüfbarkeit-algorithmen/ (letzter Abruf: 25.8.2018).

[33] So wörtlich *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 Fußnote 1.

wird mit den Begriffen „algorithmische Entscheidungsfindung“[34] bzw. „algorithmenbasierte Entscheidungsprozesse“[35] umschrieben.

In einem weiteren Schritt ist zu fragen, welche weiteren Klassifizierungsmerkmale herangezogen werden können, um relevante Algorithmen herauszufiltern. Dabei wird insbesondere von Autoren, die eine Regulierung befürworten, weiterhin danach differenziert, welche Eingriffstiefe im Rahmen einer etwaigen Regulierung in Betracht käme. *Martini* umschreibt (potentiell) regulierungsbedürftige digitale Algorithmen mit der Formulierung „Algorithmen in persönlichkeitssensiblen Feldern“[36]. Für solche Algorithmen kann er sich Regelungen zur Verbesserung der Transparenz (Kennzeichnungspflichten, Begründungspflichten) vorstellen.[37] Die weitere Eingriffsschwelle, die darüber hinausgehende Eingriffe (wie z.B. Vorab-Kontrollverfahren) ermöglicht, beschreibt er als Algorithmen in „besonders persönlichkeitssensiblen“[38] Entscheidungsbereichen. Bei beiden Kategorien wird indes darauf abgehoben, dass die vorgeschlagenen Klassifizierungsmerkmale einer erheblichen Konkretisierung anhand hinreichend bestimmter Kriterien bedürfen, deren Normierung dem Gesetzgeber obliege.[39]

Der Verbraucherzentrale Bundesverband e.V. zielt in seinem Thesenpapier „Algorithmenbasierte Entscheidungsprozesse“ auf eine dreistufige Überprüfung ab. Auf der ersten Stufe steht zunächst sozusagen das Herausfiltern der digitalen Algorithmen, die einer weiteren Prüfung und mithin auch einer Regulierung bedürftig sein könnten. Hierfür schlägt das Papier das Kriterium vor, dass ein algorithmischer Entscheidungsprozess „signifikante“ bzw. „große Auswirkungen

---

[34] *Ernst*, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, 1026; *Vieth/Müller-Eiselt*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 10, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf 25.8.2018).

[35] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 3, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf 25.8.2018). Teilweise wird insoweit auch auf den angelsächsischen Terminus „algorithmic decision making“ abgestellt und auch im Deutschen von „ADM-Prozessen“ gesprochen: Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 3, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf 25.8.2018); Algorithm Watch, Das ADM – Manifest, abrufbar unter: https://algorithmwatch.org/de/das-adm-manifest-the-adm-manifesto/ (letzter Abruf 25.8.2018); *Lischka*, Neun Chancen, neun Risiken algorithmischer Entscheidungsfindung, abrufbar unter: http://www.konradlischka.info/2017/05/blog/neun-chancen-neun-risiken-algorithmischer-entscheidungsfindung/ (letzter Abruf 25.8.2018).

[36] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1020).

[37] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1020).

[38] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1021).

[39] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1021).

auf Individuen und Gesellschaft“ haben könnte.[40] Als Kriterien für diese Prüfung werden die „politische und ökonomische Macht des Betreibers“, die Abhängigkeit vom Zugang zu dem von der Entscheidungsfindung betroffenen Angebot, die „Auswirkung“ des Entscheidungsprozesses „auf die weitere Lebensgestaltung des Betroffenen“ oder die Zahl der Betroffenen angeführt.[41] Wird auf dieser Stufe jedenfalls festgestellt, dass der algorithmische Entscheidungsprozess „gesellschaftlich relevant“[42] ist, so seien Kennzeichnungspflichten in Betracht zu ziehen.[43] Bei Feststellung „signifikanter Auswirkungen auf Individuen und Gesellschaft“ sollten für einen zweiten Schritt Rechtsgrundlagen für eine Einsichtnahme geschaffen werden, die neben der Prüfung persönlicher und gesellschaftlicher Folgewirkungen insbesondere auch eine Überprüfung der Übereinstimmung mit den gesetzlichen Anforderungen umfasse.[44] Auf der Grundlage der Überprüfung könne bei Schaffung entsprechender rechtlicher Grundlagen in einem dritten Schritt über etwaige Maßnahmen entschieden werden. Unabhängig von dieser „Drei-Schritt-Prüfung“ komme ein Zulassungs- bzw. Vorabkontrollverfahren stets dann in Betracht, wenn die Entscheidungsergebnisse des Algorithmus mit „Risiken für Leib und Leben“ verbunden seien.[45]

Demgegenüber stellen *Vieth/Wagner* in einer Expertise für die Bertelsmann Stiftung für eine Klassifizierung von Algorithmen nach ihrer potentiellen Regulierungsrelevanz auf das Kriterium der „Teilhaberelevanz“[46] ab. Dabei

---

[40] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 9, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[41] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 9, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[42] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 10, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[43] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 10, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[44] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 10 f., abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[45] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 9, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[46] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 22, abrufbar unter: https://www.bertelsmann-

gehen auch sie mit Blick auf dieses Kriterium von unterschiedlichen Eingriffs- bzw. Regulierungsstufen in Abhängigkeit von dem Ausmaß der mit dem Algorithmus potentiell verbundenen „Teilhabewirkung“ aus.[47] Ferner wollen auch sie mit Blick auf das von ihnen für relevant erachtete Differenzierungskriterium nicht sämtliche Algorithmen auf ihre Regulierungsbedürftigkeit hin untersuchen, sondern Algorithmen erst ab einer „bestimmten Grundschwelle von Teilhabewirkung“ einer Prüfung zuführen.[48] Die Teilhaberelevanz wollen die Autoren nicht „binär“[49] bestimmen, sondern anhand dreier als maßgeblich erachteter Kriterien („Akteure“, „soziale Einbettung“ und „Konsequenzen“[50]), denen wiederum weiteren Unterkriterien zugeordnet sind. Dies sind die Kriterien „Wettbewerb“ und „Abhängigkeit“ (für das Hauptkriterium „Akteure“),[51] „Selbstbestimmung“ und „Anpassung“ (für das Hauptkriterium „soziale Einbettung“)[52] sowie „Reichweite“ und „Systemveränderung“ (für das Hauptkriterium „Konsequenzen“).[53]

Busch unterscheidet in seinem Gutachten zum ABIDA – Projekt nach dem mit einem Algorithmus verbundenen „Grad der Gefährdung“ und dem „Rang der gefährdeten Rechtsgüter“ und schlägt eine an diesen Kriterien ausgerichtete „Kontrolldichte“ vor, die in einen „Regulierungsmix aus behördlicher Kontrolle,

---

stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[47] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 22, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[48] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 22, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[49] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 22, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[50] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 22, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[51] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 22, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[52] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, *Gütersloh* 2017, S. 23, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

[53] *Vieth/Wagner*, Teilhabe, ausgerechnet. Wie algorithmische Prozesse Teilhabechancen beeinflussen können, Gütersloh 2017, S. 23, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Teilhabe_ausgerechnet.pdf (letzter Abruf: 25.8.2018).

zivilrechtlichen Rechtsbehelfen und Selbstregulierung“ münden soll.[54] Gesetzgeberische Eingriffe sollen von Kennzeichnungspflichten für „sensible Bereiche“ bis hin zu normativen Vorgaben für die Algorithmenentwicklung und einem „Vorabgenehmigungsverfahren“ für „besonders gefahrträchtige Anwendungen“ reichen.[55]

II. Anwendungsgebiete von Algorithmen im Kontext des Arbeitsauftrages

Von den vielfältigen Algorithmen mit Außenwirkung sollen in diesem Bericht, ausgerichtet an dem Arbeitsauftrag, die häufig thematisierten Anwendungsbereiche von Algorithmen in den Bereichen der personalisierten Werbung, personalisierten Trefferlisten und fortlaufend aktualisierten Informationsangebote (sogen. „newsfeed“) sowie der personalisierten Preise untersucht werden.

1. Personalisierte Trefferlisten sowie personalisierte fortlaufend aktualisierte Informationsangebote (sogenannte „Newsfeeds“)

Da Unternehmen, die Internetsuchmaschinen, Handelsplattformen und Soziale Online-Netzwerke mit Newsfeed-Funktionen (= Intermediäre[56]) betreiben, die von ihnen entwickelten und eingesetzten Algorithmen, die Suchergebnisse oder Newsfeeds erzeugen und steuern, regelmäßig als Geschäftsgeheimnis hüten und allenfalls grundlegende Informationen zu deren Funktionsweise veröffentlichen, ist das Ausmaß der Heranziehung und Gewichtung personenbezogener Daten der Nutzer mit der Folge starker oder geringer Personalisierung der Treffer- bzw. Newsfeedliste naturgemäß von Dienst zu Dienst verschieden und für die einzelnen Anbieter weder den Nutzern noch der (Fach-)Öffentlichkeit im Detail bekannt.[57] Es ist allerdings angesichts der Zweckbestimmung und des Geschäftsmodells Sozialer Online-Netzwerke für jeden Nutzer offenkundig, dass diese dessen im Rahmen der Anlegung des Benutzeraccounts und der Nutzung

---

[54] *Busch*, Algorithmic Accountability, S. 71, abrufbar unter: http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf (letzter Abruf: 25.8.2018).

[55] *Busch*, Algorithmic Accountability, S. 71 f., abrufbar unter: http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf. (letzter Abruf: 25.8.2018).

[56] Zur Begriffsdefinition: vgl. https://www.die-medienanstalten.de/themen/intermediaere/ (letzter Abruf: 25.8.2018).

[57] Vgl. etwa die Darstellung öffentlich bekannter Informationen zu personalisierten Kriterien für den google- und den Facebook-Algorithmus: *Lischka/Stöcker*, Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier im Auftrag der Bertelsmann Stiftung, *Gütersloh* 2017, S. 22 ff, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digitale_Oeffentlichkeit_final.pdf (letzter Abruf: 25.8.2018).

des Dienstes durch Veröffentlichen, Aufrufen, Teilen, Kommentieren und Liken von Inhalten sowie durch das Begründen und Beenden von „Freundschaften“ oder „Follower“-Beziehungen erzeugte Daten speichern und als einen Parameter für ihren Newsfeed-Algorithmus heranziehen,[58] der sich grundsätzlich – ebenso wie Trefferlisten in Suchmaschinen und Handelsplattformen – an einer Sortierung angezeigter Daten nach deren Relevanz für den Nutzer orientiert.[59] Das Ausmaß der Personalisierung und deren Gewichtung im Rahmen des Newsfeed-Algorithmus ist essentieller Bestandteil der Geschäftspolitik des jeweiligen Betreibers und häufig Gegenstand allgemeiner Statements der Betreiber zu Änderungen des Algorithmus sowie Gegenstand diesbezüglicher grundlegender öffentlicher Debatten.[60] Auch bei Internethandelsplattformen, insbesondere wenn deren Nutzer über ein Benutzerkonto angemeldet und identifiziert sind, dürfte es der allgemeinen Nutzererwartung entsprechen, dass der Algorithmus, der die vom Nutzer gesuchten Produkte in einer Trefferliste anzeigt, bei der Sortierung der Suchergebnisse unter Relevanzgesichtspunkten die bereits gespeicherten Kundendaten einbezieht und damit das Suchergebnis personalisiert. Selbst wenn beispielsweise die digitale Plattform Amazon ihren Algorithmus ebenso wenig wie die anderen Anbieter im Detail offenlegt, kann man bereits der Datenschutzerklärung auf der Webseite der Plattform und damit einer Verlautbarung des Unternehmens selbst entnehmen, dass die Plattform „alle Informationen speichert und erfasst“, die der Nutzer „auf der Webseite eingibt oder in anderer Weise übermittelt“.[61] Darüber hinaus werden auch geräte- und softwarebezogene Informationen erhoben sowie Informationen zum

[58] Dabei können die in Bezug auf die Interaktion von Nutzern hinsichtlich einer Veröffentlichung erhobenen Daten sehr vielfältig und weitreichend sein. Zum Twitter-Algorithmus wurde etwa bekannt, dass er auch die Lesezeiten der Tweets als Kriterium für die Relevanzsortierung heranzieht, *Mühlenmeier*, Twitter schreibt mit, wie lange ein Tweet gelesen wird, abrufbar unter: https://netzpolitik.org/2017/twitter-schreibt-mit-wie-lange-ein-tweet-gelesen-wird/ (letzter Abruf: 25.8.2018).

[59] *Brühl/Stratmann*, So baut Zuckerberg den Facebook-Algorithmus um, http://www.sueddeutsche.de/digital/facebook-so-baut-zuckerberg-den-facebook-algorithmus-um-1.3822756 (aufgerufen am 16.1.2018); *Bauer*, 6 Fakten zum Instagram Algorithmus: So gewinnst Du an Relevanz, https://onlinemarketing.de/news/wissenwerte-fakten-instagram-algorithmus-maximierung-relevanz (aufgerufen am 16.1.2018).

[60] *Brühl/Stratmann*, So baut Zuckerberg den Facebook-Algorithmus um; abrufbar unter: http://www.sueddeutsche.de/digital/facebook-so-baut-zuckerberg-den-facebook-algorithmus-um-1.3822756 (letzter Abruf: 25.8.2018); *Bauer*, 6 Fakten zum Instagram Algorithmus: So gewinnst Du an Relevanz, abrufbar unter: https://onlinemarketing.de/news/wissenwerte-fakten-instagram-algorithmus-maximierung-relevanz (letzter Abruf: 25.8.2018); *Mühlenmeier*, Twitter schreibt mit, wie lange ein Tweet gelesen wird, abrufbar unter: https://netzpolitik.org/2017/twitter-schreibt-mit-wie-lange-ein-tweet-gelesen-wird/ (letzter Abruf: 25.8.2018).

[61] https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE (letzter Abruf: 25.8.2018).

Nutzerverhalten wie etwa die Dauer des Verweilens bei einem Post,[62] „die Dauer des Besuchs auf einer Detailseite, Informationen zur Interaktion zwischen Seiten (z.B. Scrolling, Klicken, Mouse-overs) und über das Verlassen der Seite“.[63] Dabei legt Amazon ausdrücklich offen, dass die Daten auch dazu verwendet werden, das „Einkaufserlebnis individuell zu gestalten und stetig zu verbessern“, wozu auch gehört, dem Kunden „Produkte oder Dienstleistungen zu empfehlen, die ihn interessieren könnten“.[64] Damit ergibt sich schon aus den Verlautbarungen von Amazon selbst, dass der seitens des Unternehmens eingesetzte Sortieralgorithmus auch individuelle Parameter zum Zwecke einer personalisierten Trefferliste verwendet. Dies liegt auch im Trend weiterer Internethandels- oder vertriebsplattformen wie etwa der Unternehmen Zalando[65], Ebay[66] oder Booking.com[67], die erklärtermaßen mittels Algorithmen erzeugte Suchergebnisse in jüngerer Zeit stärker personalisiert haben oder zeitnah beabsichtigen, dies zu tun. Auf der anderen Seite konnten etwa im Zusammenhang mit der Bundestagswahl 2017 bei Google keine hinreichenden Anhaltspunkte für Personalisierungen erkannt werden.[68]

2. Personalisierte Werbung

Bei der Nutzung zahlreicher Internetdienste (Suchmaschinen, Nachrichtenportale, Soziale Netzwerke, Handelsplattformen) wird Werbung von Drittanbietern eingespielt. Hierbei kommen regelmäßig digitale Algorithmen zum Einsatz, um die angezeigte Werbung möglichst zielgruppenorientiert zu präsentieren. Diese

---

[62] *Lischka/Stöcker*, Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier im Auftrag der Bertelsmann Stiftung, *Gütersloh* 2017, S. 22 ff, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digitale_Oeffentlichkeit_final.pdf (letzter Abruf: 25.8.2018).

[63]https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE (letzter Abruf: 25.8.2018).

[64]https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE (letzter Abruf: 25.8.2018).

[65] *Penke*, Personalisierte Shops: Zalando investiert zweistelligen Millionenbetrag, abrufbar unter: https://www.gruenderszene.de/allgemein/zalando-amazon-otto-investment-personalisierung (letzter Abruf: 25.8.2018).

[66] *Pohlgeers*, Ebay garantiert die schnelle Lieferung und will mehr Personalisierung, abrufbar unter: https://www.onlinehaendler-news.de/handel/internationales/28659-ebay-garantiert-schnelle-lieferung-mehr-personalisierung.html (letzter Abruf: 25.8.2018).

[67] https://news.booking.com/bookingcom-mit-neuem-tool-fur-die-personalisierte--reise--und-hotel-suche-nach-interessen-und-hobbies/ (letzter Abruf: 25.8.2018).

[68] *Krafft/Gamer/Laessing/Zweig*, Filterblase geplatzt? Kaum Raum für Personalisierung bei Google-Suche zur Bundestagswahl 2017, abrufbar unter: https://algorithmwatch.org/de/filterblase-geplatzt-kaum-raum-fuer-personalisierung-bei-google-suchen-zur-bundestagswahl-2017/ (letzter Abruf: 25.8.2018).

Algorithmen ziehen dabei personenbezogene Nutzerdaten heran, die beispielsweise aus der aktuellen Nutzung des besuchten Internetdienstes in Echtzeit (z.B. Inhalt der Dateneingabe in das Eingabefeld einer Suchmaschine, Tippverhalten bei der Bedienung der PC-Tastatur[69], Scrollverhalten, Erfassung gerätebezogener Informationen (wie verwendetes PC-Modell, Version des verwendeten Betriebssystems, Gerätekennungen[70], IP-Adresse[71]) resultieren, bei früheren Besuchen der Seite erhoben und z.B. mit Hilfe von Cookies[72] gespeichert wurden[73] oder nach Authentifizierung des Nutzers von Datenhändlern in Echtzeit erworben werden, um diese zur Platzierung einer individualisierten Werbung zu verwenden.[74] Hierbei können zugleich auch die infolge der Nutzung des Internetdienstes generierten Nutzerdaten in Echtzeit an dritte Anbieter (wie z.B. Datenhändler) übertragen werden.[75] Dabei mögen die Geschäftspraktiken und

[69] https://de.wikipedia.org/wiki/Tippverhalten (letzter Abruf: 25.8.2018).
[70] Datenschutzerklärung von google, abrufbar unter: https://www.google.de/policies/privacy/ (abgerufen am 16.01.2018); Datenschutzerklärung von amazon, abrufbar unter:https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE (letzter Abruf: 25.8.2018).
[71] Datenschutzerklärung von google, abrufbar unter: https://www.google.de/policies/privacy/ (letzter Abruf: 25.8.2018); Datenschutzerklärung von amazon, abrufbar unter: https://www.amazon.de/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=201909010#GUID-9DFA0CFF-9E83-4207-8EE5-5B1B8CFC3F4A__SECTION_B1A612A0C0F44BECB53C001C486B5CFE (letzter Abruf: 25.8.2018).
[72] Cookies sind kleine Textdateien, die eine Wiedererkennung des vom Nutzer verwendeten Endgeräts ermöglichen. Besucht der Nutzer die Webseite erneut, erkennt die Webseite das gespeicherte Cookie und kann so das Nutzungsverhalten des Nutzers (besuchte Seiten, Warenkorb etc.) auswerten (vgl. *Weidert/ Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutzgrundverordnung, BB 2017, 1858 (1861)).
[73] Z.B. mit Hilfe von Cookies auf dem Rechner abgelegter Dateien, die bei erneutem Aufruf angesteuert werden (Cookies) oder mittels Auslesen des Webspeichers des Nutzerbrowsers: abrufbar unter: https://de.wikipedia.org/wiki/Cookie (letzter Abruf: 25.8.2018); Datenschutzerklärung von google, abrufbar unter: https://www.google.de/policies/privacy/ (letzter Abruf: 25.8.2018).
[74] *Hawiger*, Personalisierte Werbung: Wie unsere Person selbst an verschiedenen Geräten identifizierbar wird, abrufbar unter: https://netzpolitik.org/2015/personalisierte-werbung-wie-unsere-person-selbst-an-verschiedenen-geraeten-identifizierbar-wird/ (letzter Abruf: 25.8.2018); *Tanner*, *Connectivity*, How ads follow you from phone to desktop to tablet, abrufbar unter: https://www.technologyreview.com/s/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/ (letzter Abruf: 25.8.2018); *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 51 ff., abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018).
[75] Vgl. etwa die Übersicht zur Übertragung von Nutzungsdaten aus der Nutzung deutschsprachiger Nachrichten-Portale an „externe Services“ bei *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 51 ff., abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018) unter Berufung auf die instruktive Seite: von @stefanwehrmeyer, @annabelchurch, @pudo, We

technischen Lösungen ebenso vielfältig sein wie der Grad der Individualisierung der gespeicherten Nutzerprofile[76] und der algorithmenbasierten Werbeannoncen.[77] Gleichwohl wird die praktische Bedeutung personalisierter Werbung im Internet so eingeschätzt, dass sie zwischenzeitlich das Schalten von Werbung, das zu angezeigten bzw. abgerufenen Seiteninhalten passt, nahezu vollkommen verdrängt habe[78] und zum „Standard“[79] gehöre. Dabei wird personalisierte Werbung als „Vorstufe“ zu einer Preisdifferenzierung nach personenbezogenen Kriterien (siehe dazu nachfolgend II. 3) gewertet.[80]

Eine zentrale Komponente personalisierter Online-Werbung ist die Fähigkeit der Werbeanbieter, die Werbung so zielgenau wie möglich an die Konsumenten anzupassen und ihnen maßgeschneidert zukommen zu lassen.[81] Dies wird auch als Targeting, also als an Zielgruppen ausgerichtete Werbung bezeichnet.[82] Dabei wird zwischen diversen Werbeformen unterschieden. Allein beim bloßen Content-Targeting, bei dem die Werbung bloß in einem passenden Umfeld geschaltet wird, spielt der Aspekt der Personalisierung keine Rolle. Alle weiteren

---

used to read the newspapers, now the news reads us, abrufbar unter: http://newsreadsus.okfn.de/ (letzter Abruf: 25.8.2018).

[76] So wird etwa von Anbieterseite angeführt, es gebe keine gespeicherten Nutzerprofile mit Klarnamen, sondern nur Datenpakete mit Identifikationsnummern: *Hawiger*, Personalisierte Werbung: Wie unsere Person selbst an verschiedenen Geräten identifizierbar wird, abrufbar unter: https://netzpolitik.org/2015/personalisierte-werbung-wie-unsere-person-selbst-an-verschiedenen-geraeten-identifizierbar-wird/ (letzter Abruf: 25.8.2018).

[77] *Schneider*, Personalisierte Werbung: Durchs Netz verfolgt, abrufbar unter: http://www.tagesspiegel.de/wirtschaft/streitthema-tracking-personalisierte-werbung-durchs-netz-verfolgt-/6445032.html, wonach die Ergebnisse teilweise unscharf seien, da eine Zuordnung des Nutzers zu einer Personengruppe offenbar nur anhand grober Parameter (z.B. Geschlecht) erfolge.

[78] *Weinland*, Online Marketing Trends 2014 – Personalisierung und Targeting als Chance, abrufbar unter: https://www.marketing-boerse.de/Fachartikel/details/1407-Onlinemarketing-Trends-2014---Personalisierung-und-Targeting-als-Chanc/46183 (letzter Abruf: 25.8.2018).

[79] *Reisch/Büchel/Joost/Zander-Hayat*, Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel. Veröffentlichung des Sachverständigenrats für Verbraucherfragen, Berlin 2016, S. 22, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2 (letzter Abruf: 25.8.2018).

[80] *Reisch/Büchel/Joost/Zander-Hayat*, Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel. Veröffentlichung des Sachverständigenrats für Verbraucherfragen, Berlin 2016, S. 22, abrufbar unter https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2 (abgerufen am 17.1.2018).

[81] *Spies*, USA: Personalisierte Werbung und gläserne Websurfer – Deep Packet Inspection MMR 2008, XII (XII).

[82] Vgl. etwa Wikipedia unter „targeted advertising“, https://de.wikipedia.org/wiki/Targeted_Advertising (letzter Abruf: 25. 8.2018), vgl. auch unter https://www.clicks.de/blog/personalisierte-werbung-vor-und-nachteile-fuer-ihr-unternehmen (letzter Abruf: 25.8.2018).

Formen von Targeting stellen Formen von personalisierter Werbung dar. Hierbei wird zwischen folgenden Targeting-Methoden, bei denen es sich jeweils um personalisierte Werbung handelt, unterschieden:

- Semantisches Targeting

  Dabei wird die Produktwerbung dem Nutzer auch auf Webseiten präsentiert, die einen ähnlichen Inhalt haben, wie das beworbene Produkt und unter Verwendung von Cookies versucht, passende Werbung auf den Nutzer abzustimmen.

- Behavioral Targeting

  Bei dieser Form der Werbung werden ebenfalls technische Daten ausgelesen, aber zusätzlich verschiedene Merkmale herangezogen und berücksichtigt (etwa besuchte Seiten, installierte Schriftarten oder Plug-Ins, geographische Einordnung mittels der IP-Adresse). Damit kann ein dynamisches Verhaltensprofil erstellt werden, das kontinuierlich wächst und angepasst wird. Es wird nicht nur das aktuelle, sondern auch das längerfristige Interesse des Nutzers berücksichtigt.

- Retargeting

  Hier wird mit den gleichen Techniken wie beim Behavioral-Targeting versucht, verloren gegangene Kunden zurückzugewinnen (etwa wenn ein Produkt bei einem Anbieter angeschaut oder in einen Warenkorb gelegt, aber dann doch nicht bestellt wurde durch gezielte weitere Bewerbung dieses Produkts).

- Social-Media-Targeting

  Auch hierbei werden die o.g. Techniken eingesetzt und Werbung in einem sozialen Netzwerk eingeblendet.

- Psychografisches Targeting

  Bei dieser Targetingmethode geht es darum, die Persönlichkeit von Nutzern in Form von Maßzahlen als Profile darstellbar zu machen (Verhaltensprofile) und daraus individuelle Handlungstendenzen und Unterschiede in der Wahrnehmung abzuleiten und diese Erkenntnisse bei der Werbung zu nutzen.

- Search Intent Targeting

  Hierbei werden Nutzer einer Website in Echtzeit mit Werbung angesprochen, noch während sie auf dieser Website suchen.[83]

[83] Vgl. etwa Wikipedia unter „targeted advertising“, https://de.wikipedia.org/wiki/Targeted_Advertising (letzter Abruf: 25.8.2018) und unter unter https://www.clicks.de/blog/personalisierte-werbung-vor-und-nachteile-fuer-ihr-unternehmen (letzter Abruf: 25.8.2018); vgl. auch *Spies*, USA: Personalisierte Werbung und gläserne Websurfer – Deep Packet Inspection MMR 2008, XII (XII).

Bei derartigen Verfahren ist es bereits seit vielen Jahren gängige Praxis, dass für derartige Verfahren personalisierter Werbung zum einen persönliche Daten, die Nutzer bei Anmeldung für eine Website angegeben hatten (wie Name, E-Mail-Adresse, Postadresse oder Geburtsdatum) verwendet werden, wie auch Daten über die Dauer der Nutzung oder einzelne Seitenabrufe oder Downloads. Typischerweise erhobene Nutzerdaten waren schon vor zehn Jahren etwa die IP-Adresse des Nutzers, sein Nutzername und Passwort und die besuchten Subsites. Bereits damals wurden freiwillig eingegebene weitere persönliche Daten genutzt, wie Geschlecht, Wohnort, Kinder, Beziehungsstatus, besondere Vorlieben (Lieblingsmusik, -filme, Hobbys etc.) und es wurden mittels Software die Surfgewohnheiten des Nutzers möglichst umfänglich ermittelt und ausgewertet und sich der Nutzerprofile oder statistischer Auswertungen über das Verhalten des Nutzers bedient.[84] Auch in aktuelleren Auseinandersetzungen mit der Thematik wird darauf hingewiesen, dass Anbieter von Internetseiten umfangreiche Daten über die Nutzer ihrer Dienste erlangen und zu Profilen zusammentragen können, indem sie etwa die IP-Adresse, Fingerprints oder Cookies verwenden, was dazu führt, das Anbieter immer besser über ihre (potentiellen) Kunden Bescheid wissen und ihre Datenbanken sich an Geschäfte oder Suchvorgänge erinnern, die der Kunde längst vergessen hat. Zwar ist die Verwendung von solchen Techniken seit der Cookies-Richtlinie (2009/136/EG) nur noch mit Einwilligung des Nutzers zulässig, ohne diese Einwilligung können aber viele Dienste gar nicht mehr genutzt werden.[85] Für sämtliche Formen personalisierter Werbung ist grundsätzlich[86] der Einsatz von Algorithmen erforderlich.

Bei der personalisierten Werbung stellt sich im Kern also das Problem, dass über lange Zeiträume äußerst detailliert umfangreiche Daten über die Nutzer gesammelt und zu Profilen verarbeitet werden und dass bereits anhand von relativ wenigen Informationen sehr aussagekräftige Persönlichkeitsprofile erstellt werden können. Der Psychologe Michal Kosinski hat etwa einen Algorithmus geschrieben, der die Persönlichkeit von Menschen einschätzen soll. Als Grundlage für diese Einschätzung bzw. die Erstellung eines Persönlichkeitsprofils dienen diesem Algorithmus „Likes“, die ein Nutzer im Internet (insbesondere auf Facebook) gesetzt hat. Diesem Algorithmus sollen 10 „Likes“ im Internet genügen, um die Persönlichkeit eines Menschen besser einzuschätzen, als seine Kollegen; 100 um sie besser einzuschätzen als Familienangehörige und 250 um

[84] *Bauer*, Personalisierte Werbung auf Social Community Websites; Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen, MMR 2008, 435 (435/436); *Spies*, USA: Personalisierte Werbung und gläserne Websurfer – Deep Packet Inspection MMR 2008, XII (XII).

[85] Vgl. *Rott*, Der „Durchschnittsverbraucher“ – ein Auslaufmodell angesichts personalisierten Marketings? VuR 2015, 163 (165) mwN.

[86] Lediglich beim semantischen Targeting könnte personalisierte Werbung theoretisch auch ohne Einsatz von Algorithmen erfolgen.

besser zu sein, als der Lebenspartner.[87] Derartige Algorithmen wurden etwa auch von der Firma Cambridge Analytica verwendet, die maßgeblich an dem sog. Facebook-Datenskandal beteiligt war (vgl. dazu ausführlich noch unten).

Damit sind aber in erster Linie Probleme des Datenschutzes angesprochen und weniger zivilrechtliche Fragestellungen. Folgerichtig wird das Problem der personalisierten Werbung in der Literatur insbesondere vor dem Hintergrund des Geltungsbeginns der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 hinsichtlich des Datenschutzes diskutiert. Unter zivilrechtlichen Aspekten wird das Thema hingegen nur vereinzelt angesprochen.

Zwar liegt der Schwerpunkt der Bearbeitung nach der Zielsetzung der Arbeitsgruppe im Zivilrecht. Da aber die aktuelle Diskussion um personalisierte Werbung nahezu ausschließlich im Bereich des Datenschutzrechts geführt wird, hier im Wesentlichen die relevanten Probleme zu verorten sind und das Datenschutzrecht insoweit zivilrechtliche Funktionen übernimmt, indem es faktisch Anforderungen für die Zulässigkeit eines „Bezahlens mit Daten“ aufstellt, soll in dem Kapitel zur konkreten Betrachtung rechtspolitischer Handlungsoptionen für personalisierte Werbung (E. III. 3.) zuerst ein kurzer Abriss zu der Problematik der datenschutzrechtlichen Fragestellungen erfolgen (Kapitel 1, E. II. 3. a) bis c)). Anschließend sollen die im engeren Sinn zivilrechtlichen Aspekte personalisierter Werbung angesprochen werden (Kapitel 1, E. II. 3. d).

3. Personalisierte Preise

Unter „personalisierten Preisen“ versteht man das Phänomen, dass ein Anbieter ein bestimmtes Produkt/eine bestimmte Dienstleistung nicht allen Kunden zu einem Einheitspreis anbietet, sondern zur selben Zeit potentiellen Kunden gegenüber die Preise nach personenbezogenen Kriterien differenziert.[88] Dabei kommt im vorliegenden thematischen Kontext in Betracht, die Preisbildung digitalen Algorithmen zu überlassen, in die auch personenbezogene Daten der

[87] Vgl. etwa Süddeutsche Zeitung vom 3./4.3.2018, S. 51 „Der Vermesser der Seele“, noch in 2016 wurde sein Modell so beschrieben, dass es 19 Facebook-Likes benötigt, um eine Person besser einschätzen zu können, als ein durchschnittlicher Arbeitskollege, 70 Likes um die Menschenkenntnis eines Freundes zu überbieten, 150 um die der Eltern und 300 um die des Partners/ der Partnerin zu überbieten (vgl. Beitrag über Michal Kosinski www.dasmagazin.ch vom 12.3.2016 „Ich habe nur gezeigt, dass es die Bombe gibt“). Der Algorithmus wurde offenbar in jüngster Zeit noch weiter optimiert.

[88] *Zander-Hayat/Reisch/Steffen*, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, 403 (404); *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 2, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018).

Internetkunden (wie z.B. benutztes Endgerät, Wohnort, Zugehörigkeit zu einer bestimmten Kunden- oder Zielgruppe, häufig besuchte Websites, bisheriges Kaufverhalten etc.) einfließen.[89] Erfolgt im Rahmen der Verwendung personenbezogener Daten im Preisbildungsalgorithmus nicht nur eine pauschale Zuordnung zu verschiedenen Kunden- oder Zielgruppen, sondern eine individuelle Preisbildung derart, dass der Preis exakt auf den konkreten Internetnutzer zugeschnitten ist, so liegt eine personalisierte Preisbildung im engeren Sinne vor.[90]

Dieses Phänomen ist von anderen Phänomenen[91] abzugrenzen. Zu erwähnen ist hierbei insbesondere das im Onlinehandel verbreitete[92] „dynamic pricing", wonach Preise nicht festgeschrieben und von Zeit zu Zeit nach Maßgabe von Angebot und Nachfrage aktualisiert werden, sondern fortwährend anhand bestimmter Kriterien (wie z.B. Angebot und Nachfrage, Lagerbestand, Wettbewerbsbeobachtung, Such- und Kaufverhalten der Kunden, Tageszeit etc.) mittels Algorithmen an das Marktgeschehen angepasst werden.[93] Gleichfalls nicht mit personalisierten Preisen gleichzusetzen ist die sogenannte „Suchdiskriminierung", bei der mittels Einbeziehung personenbezogener Nutzerdaten, die zum Beispiel Rückschluss auf dessen Zahlungsbereitschaft oder Kaufkraft zulassen, durch algorithmische Prozesse eine Veränderung der Reihenfolge in der Trefferliste mit dem Ziel erfolgt, dass die Aufmerksamkeit des Kunden auf Angebote einer bestimmten Preisklasse gelenkt werden soll, ohne dass aber eine Anpassung der Preise für die angezeigten Produkte bzw. Dienstleistungen erfolgt.[94] Soweit ersichtlich, besteht für den deutschen Markt –

---

[89] *Zander-Hayat/Reisch/Steffen*, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, 403 (404); Verbraucherzentrale Bundesverband e.V., Personalisierte Preise. Diskussionspapier des Verbraucherzentrale Bundesverbands, 23. September 2016, S. 3, abrufbar unter: https://www.vzbv.de/sites/default/files/vzbv_position_preisdifferenzierung_16-09-21_pdf.pdf (letzter Abruf: 25.8.2018).

[90] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 5, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[91] Neben den hier erwähnten Abgrenzungsfällen wird auch häufig die Preisdifferenzierung mittels mobiler Coupons erwähnt, die im Ergebnis bei dynamischer Ausgestaltung zu (verdeckter) individueller Preisdifferenzierung führen könnte: vgl. http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[92] *Busch*, Algorithmic accountability, S. 13, abrufbar unter: http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf (letzter Abruf: 25.8.2018).

[93] *Zander-Hayat/Reisch/Steffen*, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, 403 (404); *Ernst*, Algorithmische Entscheidungsfindung und personenbezogene Daten JZ, 2017, 1026 (1034).

[94] *Zander-Hayat/Reisch/Steffen*, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, 403 (404).

anders als etwa für den US-amerikanischen Markt – bislang Einigkeit, dass es an fundierten empirischen Belegen für verbreitete personalisierte Preisbildung im Online-Handel fehlt.[95] Eine Studie im Auftrag des Sachverständigenrats für Verbraucherfragen aus dem Jahr 2016 stützt dieses Ergebnis und konnte personalisierte Preisbildung in nennenswertem Umfang lediglich im Bereich höherpreisiger Pauschalreisen feststellen.[96] Auch die im Rahmen der Sachverhaltsaufklärung seitens der Länderarbeitsgruppe durchgeführte Expertenanhörung hat hierzu keine abweichenden Erkenntnisse erbracht.

Allerdings besteht Einigkeit, dass algorithmenbasierte personalisierte Preisbildung im Onlinehandel auch auf dem deutschen Markt technisch möglich wäre und daher in Zukunft praktische Relevanz entfalten könnte. Die in der vorgenannten Studie geäußerte Einschätzung, dass die verbreitete Einführung personalisierter Preise auf dem deutschen Markt nicht zuletzt mangels hinreichenden Wissens der Unternehmen über Zahlungsbereitschaften der Kunden und der Schwierigkeiten des Preisabgleichs bei mehreren Vertriebswegen „unwahrscheinlich sei“[97], steht die in der Literatur geäußerte Einschätzung

---

[95] *Zander-Hayat/Reisch/Steffen*, Personalisierte Preise – Eine verbraucherpolitische Einordnung, VuR 2016, 403 (405 f.); *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 2, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018); Verbraucherzentrale Bundesverband e.V., Personalisierte Preise. Diskussionspapier des Verbraucherzentrale Bundesverbands, 23. September 2016, S. 3, abrufbar unter: https://www.vzbv.de/sites/default/files/vzbv_position_preisdifferenzierung_16-09-21_pdf.pdf (letzter Abruf: 25.8.2018); *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 2, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018*); Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018); vgl. ferner das Diskussionspapier des Händlerbundes e.V., der eine Praxis der personalisierten Preisdifferenzierung im deutschen Online-Handel als „extrem selten und in einem gesunden Wettbewerb nicht marktfähig“ bewertet: Händlerbund e.V., Diskussionspapier zur aktuellen Debatte um „Dynamic Pricing“ und „individualisierte Preise“, Berlin 2016, S. 4, abrufbar unter: https://www.haendlerbund.de/de/downloads/stellungnahmen/dynamic-pricing.pdf (letzter Abruf: 25.8.2018).

[96] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 2, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[97] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 2, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

entgegen, dass sich bei einem Rückgang derzeit bestehender praktischer Hindernisse die Praxis der im Onlinehandel auf dem deutschen Markt tätigen Unternehmen „wahrscheinlich ändern“ werde.[98]

C. Bestehender Rechtsrahmen für Big Data-Anwendungen

Wie in den dargestellten Fallgruppen gezeigt, aber auch darüber hinaus, können sich bei Big Data-Anwendungen ganz grundsätzliche Fragen von Diskriminierung, Teilhabe und Transparenz stellen. Nachfolgend sollen zunächst bestehende rechtliche Rahmenbedingungen dargestellt werden.

I. Verfassungsrecht

1. Vorbemerkung

Im Hinblick auf die Digitalisierung der Gesellschaft erscheint eine Reihe von Grundrechten von Bedeutung. Zu nennen ist das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, insbesondere in seiner speziellen Ausprägung des Schutzes der informationellen Selbstbestimmung. Auch der Schutz des Telekommunikationsgeheimnisses nach Art. 10 GG sowie die Gleichheitsgrundrechte in Art. 3 GG spielen im Rahmen der Digitalisierung eine Rolle.

Dabei binden die Grundrechte zunächst nach Art. 1 Abs. 3 GG die Gesetzgebung, die vollziehende Gewalt und die Rechtsprechung. Sie sind in erster Linie dazu bestimmt, die Freiheitssphäre des Einzelnen vor Eingriffen der öffentlichen Gewalt zu sichern.

Bedient sich der Staat, etwa zum Erlass eines Verwaltungsaktes, einer automatischen Einrichtung nach § 35a des Verwaltungsverfahrensgesetzes, ist er dabei unproblematisch an die Grundrechte gebunden.

Daneben definieren die Grundrechte eine objektive Werteordnung und begründen als objektive Prinzipien staatliche Schutzpflichten. Sie verpflichten den Gesetzgeber, ein hinreichendes Maß an Schutz gegen nicht-staatliche Beeinträchtigungen zu gewährleisten, namentlich auch gegenüber Grundrechtsbeeinträchtigungen durch Privatrechtssubjekte.[99] Dabei kommt dem Gesetzgeber ein weiter Einschätzungs-, Wertungs- und Gestaltungsbereich zu, der auch Raum lässt, etwa konkurrierende öffentliche und private Interessen zu berücksichtigen. Das Bundesverfassungsgericht kann eine Verletzung der

---

[98] *Reisch/Büchel/Joost/Zander-Hayat*, Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel, Veröffentlichung des Sachverständigenrats für Verbraucherfragen, Januar 2016, S. 2, abrufbar unter: https://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/01192016_Digitale_Welt_und_Handel.pdf?__blob=publicationFile&v=2 (letzter Abruf: 25.8.2018).

[99] Kiel/Lunk/Oetker/*Fischinger*, Münchener Handbuch zum Arbeitsrecht, § 7, Rn. 13.

Schutzpflichten nur feststellen, wenn die öffentliche Gewalt Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder offensichtlich die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das Schutzziel zu erreichen.[100]

Schließlich enthalten einige wenige grundrechtliche Bestimmungen ausdrückliche Regelungen zur Wirkung zwischen Privaten, sogenannte Dritt- oder Horizontalwirkung. Hierzu zählt Art. 9 Abs. 3 S. 2 GG, der die Nichtigkeit von Abreden vorsieht, die das Recht auf Bildung von Vereinigungen zur Wahrung der Arbeits- und Wirtschaftsbedingungen einschränken oder zu behindern suchen.

Soweit in Teilen der Literatur[101] und in der arbeitsgerichtlichen Rechtsprechung[102] darüber hinaus eine grundsätzliche unmittelbare Drittwirkung der Grundrechte angenommen wurde, konnte sich dies nicht durchsetzen. Vielmehr wird allgemein von einer lediglich mittelbaren Drittwirkung der Grundrechte ausgegangen. Nach dieser auf Günter Dürig zurückgehenden Lehre finden die Grundrechte in das Zivilrecht über unbestimmte Rechtsbegriffe oder Generalklauseln Einzug.

In seiner Entscheidung zu Bürgschaftsverträgen hat das Bundesverfassungsgericht eine Ausstrahlungswirkung des Grundrechts der allgemeinen Handlungsfreiheit aus Art. 2 Abs.1 GG (hier in Form der Privatautonomie, als Selbstbestimmung des Einzelnen im Rechtsleben) auf die Auslegung von zivilrechtlichen Generalklauseln wie § 138 Abs. 2 BGB angenommen.[103] Da alle Beteiligten des Zivilrechtsverkehrs den Schutz des Art. 2 Abs. 1 GG genössen, dürfte nicht nur das Recht des Stärkeren gelten.[104] Das Gericht lässt in dieser Entscheidung eine Tendenz erkennen, den Einzelnen in seinem Grundrecht auf freie Entfaltung der Persönlichkeit auch gegen private Dritte abzusichern. Eine Weiterentwicklung dieser Rechtsprechung ist denkbar, wenn der Einsatz von Big Data-Anwendungen den Einzelnen zum wehr- und hilflosen Objekt elektronischer Entscheidungsfindung in wichtigen Lebensbereichen machen sollte.

In jüngerer Rechtsprechung hat das Bundesverfassungsgericht passend hierzu ausgeführt, dass je nach Gewährleistungsinhalt und Fallgestaltung die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates nahe- oder gleichkommen könne. Für den Schutz der Kommunikation käme das insbesondere dann in Betracht, wenn private Unternehmen die Bereitstellung schon der Rahmenbedingungen öffentlicher Kommunikation selbst übernehmen und damit in Funktionen eintreten würden, die wie die Sicherstellung der Post-

[100] BVerfG, Beschl. v. 29.10.1987 - 2 BvR 624, 1080, 2029/83, BVerfGE 77, 170 (214f); BVerfG, Beschl. v. 30.11.1988 - 1 BvR 1301/84, BVerfGE 79, 174 (202).
[101] *Nipperdey*, Gleicher Lohn der Frau für gleiche Arbeit, RDA 1950, 121 ff.
[102] BAG, Urt. v. 3.12.1954 - 1 AZR 150/54, BAGE 1, 185 (193).
[103] BVerfG, Urt. v. 19.10.1993 – 1 BvR 567/89 – BVerfGE 89, 214 (230 ff.).
[104] BVerfG, Beschl. v. 19.10.1993 - 1 BvR 567/89, BVerfGE 89, 214 .

und Telekommunikationsdienstleistungen früher dem Staat als Aufgabe der Daseinsvorsorge zugewiesen waren.[105]

Auch die Gleichheitsgebote des Grundgesetzes richten sich zunächst an alle Staatsgewalt. Davon nicht ausgeschlossen ist der allgemeine Gleichheitssatz aus Art. 3 Abs. 1 GG, obgleich der Wortlaut „vor dem Gesetz" zunächst lediglich auf die Rechtsanwendungsgleichheit abzustellen scheint.[106]

Aus Art. 3 Abs. 2 und 3 GG leiten die herrschende Meinung[107] und die Rechtsprechung[108] zudem Schutzpflichten ab.[109] Dem Gesetzgeber kommt danach die Aufgabe zu, Sicherungsvorkehrungen gegen Diskriminierungen aufgrund des Geschlechtes, der Abstammung, der Rasse, der Sprache, der Heimat und Herkunft, des Glaubens, der religiösen oder politischen Anschauungen sowie bei Behinderungen zu treffen.

Wie bei den Freiheitsgrundrechten wird auch bei den Gleichheitsgrundrechten die so genannte mittelbare Drittwirkung, also deren Ausstrahlungswirkung in das Privatrecht, überwiegend angenommen.[110] Die Ausstrahlungswirkung wird dabei im Wesentlichen davon abhängig sein, ob ein dem Staat/Bürger-Verhältnis vergleichbares strukturelles Ungleichgewicht zwischen den Vertragspartnern herrscht. An ein solches ist im Arbeits- oder Mietrecht aber auch bei monopolartigen Strukturen zu denken. Der Rückgriff auf die Gleichheitssätze im Privatrecht erfolgt jedoch mit Zurückhaltung. Beim Abschluss von Verträgen nehmen die Vertragspartner ihre individuelle Handlungsfreiheit nach Art. 2 Abs. 1 GG wahr. Schon aus Gründen der Rechtssicherheit darf ein Vertrag nicht bei jeder Störung des Verhandlungsgleichgewichts infrage gestellt oder korrigiert werden.[111] Die bloße Ausnutzung der den Parteien freistehenden rechtlichen Gestaltungsmöglichkeiten hat das Bundesverfassungsgericht nicht veranlasst, eine entsprechende Regelung am Maßstab des Art. 3 Abs. 1 GG zu messen.[112]

---

[105] BVerfG, Urt. v. 22.2.2011 – 1 BvR 699/06, BVerfGE 128, 226 („Fraport-Urteil").
[106] Vgl. z.B. Dreier/*Heun*, GG, Art. 3, Rn. 47; BVerfG, Beschl. v. 12.10.1951 – 1 BvR 201/51, BVerfGE 1, 14 (52) .
[107] Von Münch/Kunig/*Boysen*, GG, Art. 3, Rn. 47.
[108] BVerfG, Urt. v. 16.11.1993 – 1 BvR 258/86, BVerfGE 89, 276.
[109] Ob dies auch bei Art. 3 Abs. 1 GG der Fall ist, wird sehr kontrovers diskutiert; vgl. hierzu Mangoldt/Klein/Stark/*Wollenschläger*, GG, Art. 3 Abs. 1, Rn. 173 ff.
[110] Mangoldt/Klein/Stark/*Wollenschläger*, GG, Art. 3 Abs. 1, Rn. 62; Mangoldt/Klein/Stark/*Baer/Markard*, GG, Art. 3 Abs. 3, Rn. 414; kritisch: von Münch/Kunig/*Boysen*, GG, Art. 3, Rn. 50, 146.
[111] OLG München, Urt. v. 22.4.1999 - U (K) 2149/98, WuW 2000, 515.
[112] BVerfG, Urt. v. 10.01.1995 – 1 BvF 1/90, BVerfGE 92, 26 (51).

2. Die relevanten Grundrechte im Überblick:

a. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG - Grundrecht auf informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung steht im Zentrum der grundrechtlichen Beurteilung von Big Data-Anwendungen.

Ausgangspunkt für die Anerkennung eines Rechts auf informationelle Selbstbestimmung war das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983.[113]

Grundrechtlich gewährleistet ist danach die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Denn wer, so das Bundesverfassungsgericht, nicht mit hinreichender Sicherheit überschauen könne, welche ihn betreffende Information in bestimmten Bereichen seiner sozialen Umwelt bekannt sei, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermöge, könne in seiner Freiheit aus eigener Selbstbestimmung zu planen oder zu entscheiden, wesentlich gehemmt werden. Mit dem Recht auf informationelle Selbstbestimmung sei eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der der Bürger nicht mehr wissen könnte, wer was wann und bei welcher Gelegenheit über ihn wisse. Freie Entfaltung der Persönlichkeit setze unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.[114]

Einschränkungen des Grundrechts sind im überwiegenden Allgemeininteresse hinzunehmen. Diese Beschränkungen bedürfen einer förmlichen gesetzlichen Grundlage, die dem Gebot der Normenklarheit und Normbestimmtheit entspricht und dem Grundsatz der Verhältnismäßigkeit genügt.[115]

Das Grundrecht auf informationelle Selbstbestimmung findet seine Entsprechung im Recht auf Schutz personenbezogener Daten nach Art. 8 der Charta der Grundrechte der Europäischen Union und wird durch dieses im unionsrechtlich geprägten Bereich des Datenschutzrechts nunmehr weitgehend verdrängt.

b. Art. 10 GG - Brief-, Post- und Fernmeldegeheimnis

Art. 10 GG schützt die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation.[116] Verpflichtet ist jeder Träger staatlicher Gewalt. Durch Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten wird in das

[113] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1.
[114] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 43.
[115] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209, 269, 362, 420, 440, 484/83, BVerfGE 65, 1, 44.
[116] BVerfG, Beschl. v. 3.3.2004 – 1 BvF 3/92, BVerfGE 110, 33 (53).

Grundrecht eingegriffen. Beschränkungen bedürfen einer gesetzlichen Grundlage. Nach allgemeinen Grundsätzen muss die Ermächtigung ausreichend bestimmt sein, das Zitiergebot ist zu achten und die Grundrechtsschranke ist am Grundsatz der Verhältnismäßigkeit zu messen. Spezifika von Informationseingriffen wie die Streubreite von Datenspeicherungen oder die Heimlichkeit des Zugriffs auf geschützte Kommunikationsvorgänge begründen eine besondere Intensität des Eingriffs, deren Verhältnismäßigkeit im engeren Sinne für Zwecke der Strafverfolgung nur bei einem durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat bejaht werden kann.[117] Ist der absolute Kernbereich der Persönlichkeit betroffen, soll gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nach Möglichkeit der Eingriff bereits auf der Erhebungsebene unterbleiben. Ist dies nicht möglich, sind geeignete Vorgaben für die Durchsicht der Daten zu normieren. Bei Kernbereichsbezug sind diese unverzüglich zu löschen.[118]

c. Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG - Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausprägung des allgemeinen Persönlichkeitsrechts

Die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausprägung des allgemeinen Persönlichkeitsrechts schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte, wie insbesondere Art. 10 oder Art. 13 GG, sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist.[119] Das Bundesverfassungsgericht hat in seinem Urteil vom 27. Februar 2008 zu Vorschriften zur Onlinedurchsuchung im Verfassungsschutzgesetz von Nordrhein-Westfalen ausgeführt, dass es der lückenschließenden Gewährleistung des allgemeinen Persönlichkeitsrechts insbesondere bedürfe, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und der gewandelten Lebensverhältnisse kommen könne. Eine solche Lücke hat das Bundesverfassungsgericht insbesondere dann ausgemacht, wenn die Nutzung informationstechnischer Systeme als solche überwacht wird oder Speichermedien durchsucht werden. Unter einem informationstechnischen System ist jedes System zu verstehen, das elektronisch Daten verarbeitet.[120] Erforderlich ist darüber hinaus, dass das System alleine oder in der technischen Vernetzung personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten kann, dass ein Zugriff es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen

[117] Dreier/*Hermes*, GG, Art. 10, Rn. 69; BVerfG, Urt. v. 2.3.2010 – 1 BvR 256/08 u.a., BVerfGE 125, 260.
[118] BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, BVerfGE 141, 220.
[119] BVerfG, Urt. v. 27.2.2008 – 1 BvR 595/07, NJW 2008, 822.
[120] *Hornung*, Ein neues Grundrecht – der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme, CR 2008, 299 (302).

oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Ferner müsse der Betroffene das System als eigenes nutzen und deshalb den Umständen nach davon ausgehen dürfen, dass er alleine oder zusammen mit anderen zur Nutzung berechtigter Personen über das System selbstbestimmt verfügt. Ein Eingriff liegt bei jeder Erhebung von Daten aus dem System vor, aber auch, wenn Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können. Der Schutzbereich ist nicht auf heimliche Zugriffe beschränkt. Die Rechtfertigung beim heimlichen Eingriff kommt nur in Betracht, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für besonders gewichtige Rechtsgüter wie Leib, Leben und Freiheit der Person sowie Bestand oder die Sicherheit des Bundes oder eines Landes, vorliegen. Diese Beschränkungen bedürfen einer förmlichen gesetzlichen Grundlage, die dem Gebot der Normenklarheit und Normbestimmtheit entspricht und dem Grundsatz der Verhältnismäßigkeit genügt. Der heimliche Eingriff unterliegt zudem grundsätzlich dem Vorbehalt richterlicher Anordnung. Es gilt der gleiche Kernbereichsschutz wie bei Art. 10 GG.

d. Art. 3 GG - Gleichheit

Der allgemeine Gleichheitssatz des Art. 3 Abs. 1 GG gebietet allen Trägern öffentlicher Gewalt, wesentlich Gleiches gleich und wesentlich Ungleiches ungleich zu behandeln.[121] Er gilt sowohl für ungleiche Belastungen als auch für ungleiche Begünstigungen.[122] Verboten ist auch ein gleichheitswidriger Ausschluss[123], bei dem eine Begünstigung einem Personenkreis gewährt, dem anderen aber sachgrundlos vorenthalten wird.[124] Differenzierungen bedürfen stets der Rechtfertigung durch Sachgründe, die dem Differenzierungsziel und dem Ausmaß der Ungleichbehandlung angemessen sind. Der Gleichheitssatz ist dann verletzt, wenn eine Gruppe von Grundrechtsberechtigten im Vergleich zu einer anderen anders behandelt wird, obwohl zwischen beiden Gruppen keine Unterschiede von solcher Art und solchem Gewicht bestehen, dass sie die unterschiedliche Behandlung rechtfertigen können.[125]

Dabei gilt ein stufenloser, am Grundsatz der Verhältnismäßigkeit orientierter, verfassungsrechtlicher Prüfungsmaßstab, dessen Inhalt und Grenzen sich nicht abstrakt, sondern nur nach den jeweils betroffenen unterschiedlichen Sach- und Regelungsbereichen bestimmen lassen.[126]

---

[121] BVerfG, Beschl. v. 15.7.1998 – 1 BVR 1554/89, BVerfGE 98, 365 (385), st. Rspr..
[122] BVerfG, Besch. v. 11.10.1988, 1 BvR 777, 882, 1239/85, BVerfGE 79, 1, 17; BVerfG, Beschl. v. 21.7.2010 – 1 BvR 611/07, 1 BvR 2464/07, BVerfGE 126, 400 (416).
[123] BVerfG, Beschl. v. 31.1.1996 – 2 BvL39/93, BVerfGE 93, 386, 396.
[124] BVerfG, Beschl. v. 8.6.2004 - 2 BvL 5/00, BVerfGE 110, 412 (413); BVerfG, Beschl. v. 21.7.2010 – 1 BvR 611/07, 1 BvR 2464/07126, 400 (416).
[125] BVerfG, Beschl. v. 7.10.1980 – 1 BvL 50,89/79, 1 BvR 240/79, BVerfGE 55, 72 (88).
[126] BVerfG, Beschl. v. 21.7.2010, 1 BvR 611/07, 1 BvR 2464/07, BVerfGE 126, 400 (416); BVerfG, Beschl. v. 21.6.2011 – 1 BvR 2035/07, BVerfGE 129, 49.

e. Zwischenergebnis

Es steht zu erwarten, dass die Übermacht internationaler Technologieunternehmen wieder verstärkt den Wunsch nach grundrechtlich veranlasster Korrektur privatrechtlicher Verträge hervorruft und die Debatte um den Einfluss der Grundrechte neu entfacht. Erste Hinweise hierauf bietet auch das Fraport-Urteil[127] des Bundesverfassungsgerichts. Jedenfalls dürfte der Gesetzgeber aufgrund der Wirkung der Grundrechte als objektivem Wertekanon und der ihm danach auferlegten Schutzpflichten immer wieder punktuell zu einem Eingreifen gehalten sein.

II. Datenschutzrecht

Überall dort, wo Big Data-Anwendungen personenbezogene Daten zum Gegenstand haben, trifft das Datenschutzrecht wesentliche Regelungen. Personenbezogene Daten stehen unter dem Schutz der Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DS-GVO).

Das Recht zum Schutz personenbezogener Daten ist durch die seit dem 25. Mai 2018 (Art. 99 Abs. 2 DS-GVO) geltende Datenschutz-Grundverordnung europaweit weitgehend einheitlich geregelt. Sie dient – ihrem Titel entsprechend – nicht nur dem Schutz personenbezogener Daten, sondern eröffnet auch einen umfassenden rechtlichen Rahmen für die Verarbeitung personenbezogener Daten durch Wirtschaftsakteure. Dieser rechtliche Rahmen enthält nicht nur gesetzliche Regelungen des „Ob" einer Verarbeitung personenbezogener Daten, sondern auch Rechtsgrundlagen für das „Wie" der Datenverarbeitung, beispielsweise einer transparenten Nutzung. Die Begriffe „personenbezogene Daten" und „Verarbeitung" sind dabei denkbar weitgefasst, so dass eine Vielzahl von Internet-Anwendungen und Hintergrunddienste die Schutzmechanismen des Datenschutzrechts auslösen.

1. Anwendungsbereich der Datenschutz-Grundverordnung

Ziel der Datenschutz-Grundverordnung ist nicht nur der Schutz personenbezogener Daten, sondern auch der der Grundrechte und Grundfreiheiten von natürlichen Personen allgemein (Art. 1 Abs. 2 DS-GVO); gleichwohl ist Voraussetzung für die Eröffnung des Anwendungsbereichs der Verordnung „die

[127] BVerfG, Urt. v. 22.2.2011 – 1 BvR 699/06, BVerfGE 128, 226, s. oben unten Kapitel 1 C. I. 1. und Fn. 105.

ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in Dateisystemen gespeichert sind oder werden sollen“ (Art. 2 Abs. 1 DS-GVO).

Die Datenschutz-Grundverordnung ist damit lex-specialis für Verarbeitungsvorgänge, die personenbezogene Daten betreffen. Entscheidend ist deshalb der Begriff des personenbezogenen Datums. Er ist in Art. 4 Nr. 1 DS-GVO legal definiert. Danach sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“

Voraussetzung ist also die Identifizierbarkeit einer Bezugsperson bei der Verarbeitung von Daten. Die Datenschutz-Grundverordnung unterscheidet hier zunächst zwischen den zwei Polen vollständiger Anonymisierung, bei der ein Personenbezug unwiederbringlich verloren geht und einer Pseudonymisierung, bei der sich vom Verantwortlichen mit vertretbarem Aufwand ein Personenbezug wiederherstellen lässt, „Identifizierbarkeit“ also gegeben ist. Dazwischen entsteht ein Graubereich, der mit der Rechtsprechung der Gerichte, insbesondere des Europäischen Gerichtshofs (EuGH),[128] zur Richtlinie 95/46/EG[129] nur im Ansatz einer klaren Auslegung zugänglich ist. In diesen Bereich fallen diejenigen Daten, bei denen es für den Verantwortlichen in der Theorie möglich, in der Praxis aber mit unverhältnismäßigem Aufwand verbunden ist, einen Personenbezug wiederherzustellen oder der Verantwortliche unter Einschaltung eines Dritten den Personenbezug wiederherstellen kann.

Einen mehr oder minder aufschlussreichen Klärungsversuch unternimmt der Unionsgesetzgeber im 26. Erwägungsgrund zur Datenschutz-Grundverordnung: Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person auch nur indirekt zu identifizieren. Für die Frage der Identifizierbarkeit sind alle objektiven Faktoren relevant, wie die Kosten der Identifizierung, der dafür erforderliche Zeitaufwand, verfügbare Technologien und die technologische Entwicklung.[130]

---

[128] EuGH, Urt. v. 19.10.2016 – C-582/14 – Breyer gegen Deutschland; EuGH, Urt. v. 24.11.2011 – C-70/10 - Scarlet Extended.

[129] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[130] Vgl. den 26. Erwägungsgrund zur Datenschutz-Grundverordnung.

Durch den begrifflichen Einschluss von pseudonymisierten Daten ist klargestellt, dass kein Namensbezug entstehen muss,[131] sondern die Identifizierbarkeit (Wiedererkennbarkeit) einer bestimmten Person sich auch anhand anderer Merkmale bestimmen kann wie beispielsweise IP-Adressen, Cookies oder Gerätekennungen.[132] Gerade letztere Mittel dürften im Rahmen der personalisierten Werbung zur Anwendung kommen: Verwender von Cookies verarbeiten personenbezogene Daten, indem sie die auf grundsätzlich nicht namentlich identifizierbaren Rechnern abgelegten Cookies mit ihren Kundendatenbanken abgleichen, den Internetnutzer identifizieren, um ihn dann mit E-Mails oder personalisierter Werbung erneut auf ihre Produkte aufmerksam zu machen.

Durch das Hinreichen einer Identifizierbarkeit anhand weiterer Merkmale oder Kombinationen solcher Merkmale hat der Unionsgesetzgeber „Big Data"-Sammlungen weitreichender dem EU-Datenschutzrecht und den damit verbundenen Einschränkungen unterworfen, als man zunächst glauben mag: Die technischen Möglichkeiten, aus der Kombination verschiedener Datencontainer einzelne Personen auch aus einer großen Referenzgruppe individuell auszusondern, werden von den betroffenen Personen wie von den Verantwortlichen nämlich häufig unterschätzt.[133]

Dies dürfte nicht zuletzt daran liegen, dass die betroffenen Personen jeweils im Einzelfall eine Entscheidung über die Einwilligung in die Erhebung und Speicherung einzelner personenbezogener Daten treffen, sich aber des Risikos einer weiteren Nutzung, in die sie ebenfalls einwilligen, nicht bewusst sind. Auch eine Verarbeitung zur „Wahrnehmung berechtigter Interessen" erscheint dem Laien zunächst unverdächtig (vgl. Art. 6 Abs. 1 Buchst. f DS-GVO und bisher schon § 28 Abs. 1 S. 1 Nr. 2 BDSG a. F.). Hinzu kommt die Möglichkeit des Verarbeiters, die Daten (vermeintlich) zu anonymisieren, so dass sie für ihn den Personenbezug verlieren; übermittelt er diese Datensammlung an einen Dritten, ist ihm womöglich nicht bewusst, dass eine Identifizierbarkeit anhand anderer Merkmale, zu denen der Empfänger über eigene Daten verfügt, nach wie vor gegeben ist.

---

[131] Vgl. den 26., 28. und 30. Erwägungsgrund zur Datenschutz-Grundverordnung.

[132] Für den Schutz personenbezogener Daten im Kontext von Kommunikationsdiensten gilt freilich die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), die sog. „ePrivacy-Richtlinie", deren Vorgaben im Telekommunikationsgesetz umgesetzt sind. Die als deren Nachfolgerin vorgesehene ePrivacy-Verordnung befindet sich derzeit im EU-Gesetzgebungsverfahren und soll auch Kommunikationsdienste im weiteren Sinne (sog. „Over-the-top-Dienste") erfassen.

[133] Anschaulich ist die Treffsicherheit, mit der soziale Netzwerke wie Facebook ihren Nutzern „Freunde" vorschlagen: Es genügt offenbar die Auswertung von Netzwerken, um mit einiger Zielsicherheit Bekanntschaften ausmachen zu können.

Der EuGH verfolgte in seiner Rechtsprechung zur Auslegung des Begriffs der „personenbezogenen Daten“ einen relativen Ansatz, indem er auf die tatsächlichen und rechtlichen Möglichkeiten des Datenverarbeiters abstellte.[134] In der Entscheidung „Breyer“ untersuchte der Gerichtshof zunächst die abstrakte Möglichkeit des Personenbezugs. Lässt sich dieser nicht vom Verarbeiter allein herstellen, sondern benötigt er dazu eine dritte Stelle, fragt der Gerichtshof weiter, ob diese Möglichkeit ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann.[135] Es kann nicht sicher eingeschätzt werden, ob der EuGH Art. 4 Nr. 1 DS-GVO wie Art. 2 Buchst. a der Richtlinie 95/46/EG auslegen wird; denkbar ist auch die Annahme einer absoluten Betrachtungsweise, bei der schon allein die Möglichkeit, dass ein Dritter in der Lage ist, einen Personenbezug herzustellen, ohne Betrachtung der Wahrscheinlichkeit, dass Verarbeiter und Dritter zusammenwirken, für hinreichend befunden wird.[136]

Nicht wenige Big Data-Anwendungen dürften aber ungeachtet dieser Unsicherheit in den Anwendungsbereich der Datenschutz-Grundverordnung fallen, da das zusammenwirkende Verarbeiten personenbezogener Daten, um diese zu „veredeln“, indem einzelne Datensätze um weitere Kriterien angereichert werden, nicht selten Zweck der Verarbeitung ist.

Davon zu unterscheiden sind Big Data-Anwendungen, bei denen der Personenbezug für den Verarbeiter nicht entscheidend ist, sondern vielmehr aus den Datensammlungen Erkenntnisse gezogen werden, mit deren Hilfe dann Daten einer dritten Person gegen ein Raster aus einer Vielzahl von Faktoren, die vom Verarbeiter als relevant für eine automatisiert zu treffende Entscheidung angesehen werden, gelegt werden. Hier werden nicht (zwingend) die personenbezogenen Daten derjenigen Personen verarbeitet, die Eingang in den Datencontainer gefunden haben, auf dessen Grundlage ein Algorithmus automatisierte Entscheidungen trifft (Profiling); es werden die personenbezogenen Daten eines Bewerbers, eines Antragstellers o. ä. mit den Erkenntnissen aus riesigen Datenmengen abgeglichen, verarbeitet werden also (auch) dessen personenbezogene Angaben. Relevant ist in diesem Zusammenhang nicht der Schutz der gesammelten Daten, sondern der betroffenen Person vor einer sie womöglich in ihren Rechten verletzenden automatisierten Entscheidung.[137]

Selbst wenn man für die Übermittlung einen Schutz durch die Datenschutz-Grundverordnung ablehnt, weil die Daten für die übermittelnde Stelle aufgrund der bloßen Nutzung der Angaben der betreffenden Personen keinen

[134] EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 – Breyer, Tz. 43 ff.
[135] EuGH, a.a.O., Tz. 45.
[136] Vgl. *Kühling*/Buchner/ Klar, DS-GVO, Art. 4 Nr. 1 Rn. 25.
[137] Vgl. dazu unten 5.a.

Personenbezug mehr haben,[138] liegt doch bei der empfangenden Stelle, die über weitere Daten verfügt, welche die betroffene Person identifizierbar machen, eine Erhebung personenbezogener Daten vor. Dies hätte zunächst eine Pflicht zur Benachrichtigung der betroffenen Person gemäß Art. 14 Abs. 1 DS-GVO zur Folge, da personenbezogene Daten über die betroffene Person bei Dritten erhoben wurden; in den meisten Fällen wird allerdings Art. 14 Abs. 5 Buchst. b DS-GVO ein Absehen von der Information der betroffenen Person gestatten. Nach dieser Ausnahmevorschrift besteht keine Informationspflicht, „wenn und soweit die Erteilung dieser Information sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde".[139] Der Name und die Adresse der Person, deren Datensatz sich in dem genutzten Container befindet, wird dem Verarbeiter aber regelmäßig nicht bekannt sein, auch wenn eine Person – anhand anderer Merkmale – individualisierbar bleibt. Dementsprechend ist ihr Interesse gering anzusetzen und kann leicht durch das Interesse des Verantwortlichen, den Ermittlungsaufwand zu betreiben, überwogen werden.

Im räumlichen Anwendungsbereich ergeben sich mit der Datenschutz-Grundverordnung wichtige Veränderungen gegenüber dem bisher geltenden Datenschutzrecht. Gemäß Art. 3 DS-GVO gilt das Marktortprinzip, d. h., die Datenschutz-Grundverordnung findet auch auf Unternehmen Anwendung, die über keine Niederlassung in der Europäischen Union verfügen, aber hier ihre Dienstleistungen anbieten. Mit dieser Klausel ist ein weitreichender Ausgriff des europäischen Datenschutzrechts verbunden, wobei dessen Durchsetzung im Ausland sich erst noch erweisen muss.

2. Datenschutzrechtliche Erlaubnistatbestände

Die Verarbeitung personenbezogener Daten ist auch im privatrechtlichen Bereich nur gestattet, wenn der Verantwortliche sich auf einen gesetzlichen Erlaubnistatbestand oder eine wirksame Einwilligungserklärung berufen kann. Die zentrale Rechtsvorschrift für die Beurteilung der Zulässigkeit von Verarbeitungen personenbezogener Daten ist Art. 6 DS-GVO.[140] Für die hier interessierenden privatrechtlichen Datenverarbeitungen sind die Erlaubnistatbestände nach Art. 6 Abs. 1 Buchst. a (Einwilligung), Buchst. b (Vertragserfüllung) und Buchst. f DS-GVO (Wahrnehmung berechtigter Interessen des Verantwortlichen oder eines Dritten) von Bedeutung.

---

[138] Angesichts der Definition in Art. 4 Nr. 1 DS-GVO dürfte es sich aber regelmäßig lediglich um eine Pseudonymisierung handeln, durch welche die Daten ihren Personenbezug nicht verlieren.

[139] Siehe dazu unten 5. b.

[140] Die Verarbeitung besonderer Kategorien personenbezogener Daten wie z. B. Gesundheitsdaten ist in Art. 9 DS-GVO geregelt. Näheres dazu unten in Kapitel 2.

a. Verarbeitung zur Vertragserfüllung, Art. 6 Abs. 1 Buchst. b DS-GVO

Gemäß Art. 6 Abs. 1 Buchst. b DS-GVO ist die Verarbeitung personenbezogener Daten zulässig für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen. Die Vorschrift ist schon ihrem Wortlaut nach eng zu verstehen: die Datenverarbeitung ist auf das zur Vertragserfüllung oder Anbahnung notwendige Maß beschränkt. Nach Vertragsbeendigung müssten die personenbezogenen Daten folglich wieder gelöscht werden, vgl. Art. 5 Abs. 1 Buchst. a und Art. 17 Abs. 1 Buchst. a DS-GVO.

Weiterverarbeitungen aufgrund von Verträgen, die ein Vertragspartner mit Dritten hat, sind ebenso nach dem Wortlaut von Art. 6 Abs. 1 Buchst. b DS-GVO ausgeschlossen wie nach dem Zweckbindungsgebot aus Art. 5 Abs. 1 Buchst. b DS-GVO eigene Weiterverarbeitungen. Zwar fallen auch Verarbeitungen, die für die Anbahnung des Vertrages stattfinden, unter die Vorschrift. Will der Verantwortliche jedoch die erhobenen Daten einer algorithmenbasierten, vollautomatisierten Entscheidung unterwerfen, ist nach Art. 22 Abs. 1 und 2 Buchst. c DS-GVO in den meisten Fällen auch künftig eine ausdrückliche Einwilligung erforderlich.[141] Eine Sammlung der Daten auch nach Vertragserfüllung ist durch Art. 6 Abs. 1 Buchst. b DS-GVO nicht gedeckt. Art. 6 Abs. 4 DS-GVO gestattet die Weiterverarbeitung nur unter sehr engen, mit den meisten kommerziellen Zielen nicht zu vereinbarenden Voraussetzungen.

Auch zur personalisierten Preisbildung dürfte Art. 6 Abs. 1 Buchst. b DS-GVO keine ausreichende Rechtsgrundlage bereitstellen, da die Auswertung der Daten der betroffenen Personen nicht objektiv zur Anbahnung eines Vertrages „erforderlich“ sind. Sie dienen allenfalls der Wahrnehmung eines wirtschaftlichen Interesses des Anbieters (dazu sogleich).

b. Verarbeitung aufgrund berechtigter Interessen, Art. 6 Abs. 1 Buchst. f DS-GVO

Interessant ist die Frage, ob die Aufnahme von personenbezogenen Daten in Datencontainer und deren Übermittlung an Dritte über die Klausel in Art. 6 Abs. 1 Buchst. f DS-GVO gerechtfertigt werden kann. Danach ist die Verarbeitung von Daten rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Die Klausel erlaubt im

[141] Siehe dazu unten 3.

Unterschied zu Art. 6 Abs. 1 Buchst. b DS-GVO auch eine Verarbeitung zu außerhalb der Vertragserfüllung liegenden Zwecken.[142]

Mit dem Auffangtatbestand ist aufgrund seiner Unbestimmtheit eine immense Rechtsunsicherheit verbunden.[143] Im Zuge seiner Anwendung ist nämlich im Einzelfall eine umfassende Abwägung zwischen den berechtigten Interessen des Verantwortlichen oder eines Dritten mit den Interessen, Grundrechten und Grundfreiheiten der jeweils von der Datenverarbeitung betroffenen Person durchzuführen. Durch das Merkmal des „berechtigten" Interesses dürfte trotz der Wertungsoffenheit eine gewisse Einschränkung verbunden sein. In vielen Fällen wird auch die vorzunehmende Abwägung bei Big Data-Anwendungen nicht zu Gunsten des Verantwortlichen ausfallen. Wie die Abwägung im Einzelnen durchzuführen ist und wer die Darlegungslast für ein Überwiegen der Interessen der jeweils betroffenen Person trägt, ist noch nicht hinreichend geklärt.[144]

Allerdings wurde im Laufe des Gesetzgebungsverfahrens auch der Vorschlag diskutiert, eine Verarbeitung personenbezogener Daten stets dann zu erlauben, wenn die Verarbeitung auf pseudonymisierte Daten beschränkt ist und der betroffenen Person ein Widerspruchrecht gegen die Verarbeitung eingeräumt wird. Dieser Vorschlag konnte sich zwar nicht durchsetzen. Jedoch kann eine solche Art der Datenverarbeitung im Rahmen der Abwägung berücksichtigt werden und wegen der mit der Pseudonymisierung einhergehenden Minderung des Gewichts der Interessen der betroffenen Person den Ausschlag dafür geben, dass die Abwägung zu Gunsten des Verantwortlichen ausfällt und die Verarbeitung zulässig wird.[145] Eine solche Auslegung liegt insbesondere deswegen nahe, weil die jeweils betroffene Person gemäß Art. 21 Abs. 1 S. 1 DS-GVO das Recht hat, aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen die Verarbeitung sie betreffender Daten gemäß Art. 6 Abs. 1 Buchst. f DS-GVO einzulegen. In diesem Fall darf der Verantwortliche die Daten nach Art. 21 Abs. 1 S. 2 DS-GVO nicht mehr „zur Wahrnehmung berechtigter Interessen" verarbeiten, wenn er nicht zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Eine Verarbeitung ist weitergehend auch dann zulässig, wenn sie der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Der genannten allgemeinen Interessenabwägung ist jedoch von vornherein die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO entzogen, weil insoweit der strenge Ausnahmekatalog des Art. 9 Abs. 2 DS-GVO gilt.[146]

---

[142] Paal/Pauly/*Frenzel*, DSGVO/BDSG, Art. 6 Rn. 28.
[143] Kühling/*Buchner/Petri*, DS-GVO und BDSG, Art. 7 Rn. 142; Paal/Pauly/*Frenzel*, DSGVO/BDSG, Art. 6 Rn. 27.
[144] Kühling/*Buchner/Petri*, DS-GVO und BDSG, Art. 6 Rn. 149.
[145] Kühling/*Buchner/Petri*, DS-GVO und BDSG, Art. 6 Rn. 154.
[146] Kühling/*Buchner/Petri*, DS-GVO und BDSG, Art. 6 Rn. 149.

Da die Frage, wie die Interessenabwägung im Einzelnen durchzuführen ist, offen ist, wird abzuwarten sein, ob Art. 6 Abs. 1 Buchst. f DS-GVO von privaten Verantwortlichen für Big Data-Anwendungen weitgreifend fruchtbar gemacht werden kann. Allerdings zeigen insbesondere die Einschränkungen der Art. 9 und 21 DS-GVO, dass bei der Verarbeitung von personenbezogenen Daten nach Art. 6 Abs. 1 Buchst. f DS-GVO sehr stark auf den konkreten Einzelfall und die Art der jeweils zu verarbeitenden Daten zu achten ist. Die Inanspruchnahme ist damit stets mit einem gewissen Risiko für den Verantwortlichen verbunden, dass dieser rechtssicher nur mit einer wirksamen Anonymisierung umgehen kann.

Für die Bewertung einer personalisierten Preisbildung, die, soweit sie mit der Verarbeitung personenbezogener Daten einhergeht, allenfalls nach Art. 6 Abs. 1 Buchst. f DS-GVO gerechtfertigt sein kann, dürfte ausschlaggebend sein, ob sich die Auswertung von bestimmten personenbezogenen Daten als legitimes wirtschaftliches Interesse begreifen lässt; unterstellt man dies, müsste die Verarbeitung zur Wahrung dieses Interesses auch „erforderlich" sein, was zweifelhaft ist. Andernfalls wäre für die Bereitstellung personenbezogener Daten für die Preisbildung eine Einwilligung erforderlich.[147] Dass entsprechende Einwilligungen erteilt werden, ist nicht völlig abwegig, da eine personalisierte Preisbildung selbstverständlich auch zu Gunsten des Konsumenten ausfallen kann (personalisierter Rabatt). Ein Schlüssel dürfte die Transparenz der Preisbildung sein.

3. Die Einwilligung nach Art. 7 DS-GVO

Die Einwilligung ist eine einseitige Erklärung der betroffenen Person, mit der sie in dem rechtlich begrenzten Ausmaß auf den Schutz ihrer personenbezogenen Daten verzichtet. Einen unmittelbaren Vorteil bewirkt sie für die einwilligende Person also nicht, so dass diese regelmäßig Zurückhaltung walten lassen wird, ihre Einwilligung zu erteilen. Selbst wenn eine Einwilligung erteilt wird, setzt sie Big Data-Anwendungen enge Grenzen, denn sie wird gemäß Art. 6 Abs. 1 Unterabs. 1 Buchst. a DS-GVO nur für bestimmte Zwecke erteilt. Eine Weiterverarbeitung zu anderen Zwecken ist nach Art. 5 Abs. 1 Buchst. b DS-GVO grundsätzlich, vor allem zu kommerziellen Zwecken, unzulässig.

Die Voraussetzungen einer Einwilligung in die Verarbeitung personenbezogener Daten ergeben sich aus einer Zusammenschau von Art. 4 Nr. 11, Art. 6 Abs. 1 Buchst. a und Art. 7 in Verbindung mit den Erwägungsgründen der DS-GVO. In formeller Hinsicht muss die Ausgestaltung der Einwilligungserklärung gemäß Art. 7 Abs. 2 S. 1 DS-GVO transparent sein, wenn die Erklärung auch andere Sachverhalte betrifft. Der Einwilligende muss vor der Einwilligung gemäß Art. 7

[147] Davon geht der Verbraucherzentrale Bundesverband in seinem Diskussionspapier „Personalisierte Preise" aus, abrufbar unter https://www.vzbv.de/sites/default/files/vzbv_position_preisdifferenzierung_16-09-21_pdf.pdf, (letzter Abruf: 25.8.2018).

Abs. 3 S. 3 DS-GVO darüber in Kenntnis gesetzt werden, dass er seine Einwilligung jederzeit widerrufen kann. Die Einwilligung muss vor der Verarbeitung erfolgen, in die eingewilligt wird.[148] Sie muss von der einwilligenden Person selbst oder von einem zu einem bestimmten Zweck ermächtigten Vertreter erteilt werden. Zudem wird dem Verantwortlichen gemäß Art. 7 Abs. 1 DS-GVO die Nachweispflicht der erfolgten Einwilligung auferlegt. In materiell-rechtlicher Hinsicht muss die Einwilligung freiwillig, mit Einwilligungsbewusstsein und in informierter Weise erfolgen. Zudem muss die Einwilligung bestimmt und der Einwilligende einsichtsfähig sein.[149]

Diese Regelungen werfen hinsichtlich eines Bewerbers, Antragstellers o. ä. grundsätzlich keine Probleme auf, weil er in die Datenverarbeitung zum Zwecke der Auswertung seiner Bewerbung oder seines Antrags einwilligen wird und die dargelegten Voraussetzungen diesbezüglich eingehalten werden können.

Problematisch ist die Frage einer möglichen Einwilligung jedoch hinsichtlich der Daten aus dem Datencontainer, mit denen die Daten des Bewerbers oder Antragstellers abgeglichen werden. Denn soweit man diesbezüglich einen Personenbezug annimmt,[150] müsste eine Einwilligung die oben beschriebenen Voraussetzungen erfüllen. Hierbei werden insbesondere die materiellen Voraussetzungen der Freiwilligkeit („in informierter Weise“) sowie die Bestimmtheit oftmals nur schwer erreicht werden können. Denn die Freiwilligkeit setzt nach Art. 7 Abs. 4 in Verbindung mit Art. 4 Nr. 11 DS-GVO eine Gesamtabwägung der Kriterien des Ungleichgewichts, der Erforderlichkeit, der vertragscharakteristischen Leistung, der zumutbaren Alternative sowie des angemessenen Interessenausgleichs voraus.[151] Diese Beurteilung des Gesamtkontextes verringert die Rechtssicherheit des Rückgriffs auf die Einwilligung, sodass es für einen Verantwortlichen faktisch schwierig wird, die Wirksamkeit einer Einwilligung zu beurteilen. Zudem dürfte die erforderliche Gesamtabwägung in der geschilderten Fallkonstellation dazu führen, dass oftmals keine wirksame Einwilligung vorliegt. Denn das Kriterium des Ungleichgewichts spricht gegen eine wirksame Einwilligung, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht und es daher in Anbetracht aller Umstände in dem speziellen Einzelfall unwahrscheinlich ist, dass die Einwilligung freiwillig erteilt worden ist.[152] Ein solches Ungleichgewicht wird sehr schnell vorliegen, weil ein automatischer Abgleich einer Bewerbung oder eines Antrags mit Daten aus einem bereitgestellten Datencontainer wohl nur von einem Großunternehmen vorgenommen werden wird und die diesbezügliche Einwilligung desjenigen, dessen Daten in einen Datencontainer aufgenommen werden, sehr weit und unbestimmt gefasst sein müsste. Weiterhin wäre auch das Kriterium der Erforderlichkeit hier schwer zu erfüllen. Denn nicht erforderlich ist

[148] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 30.
[149] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 20.
[150] Siehe oben,1.
[151] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 41.
[152] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 42.

eine Einwilligung dann, wenn sie über das hinausgeht, was für die bestimmte Vertragserfüllung erforderlich ist.[153] Für die Erforderlichkeitsprüfung muss daher der jeweilige Vertragszweck genau bestimmt und festgestellt werden, ob es sich um eine vertragscharakteristische Leistung handelt. Sollte der Vertragszweck nicht in einer transparenten Weise darauf gerichtet sein, die Daten einer Person in den Datencontainer mit der Möglichkeit einer weiteren Verarbeitung derselben aufzunehmen, würde es oftmals an der Erforderlichkeit fehlen. Das Kriterium der zumutbaren Alternative wird in der vorliegenden Fallkonstellation nur dann Probleme bereiten, wenn dem Verantwortlichen eine Monopolstellung hinsichtlich einer bestimmten Leistung zukommt. Denn in diesem Fall hätte die jeweilige Person keinen zumutbaren anderweitigen Zugang zu einer gleichwertigen vertraglichen Leistung.[154] Hinsichtlich des Kriteriums des angemessenen Interessenausgleichs muss beachtet werden, dass der weiter verwertbare Datencontainer viele Nutzungsmöglichkeiten bietet, sodass der Daten bereitstellenden Person eine entsprechend großzügige Gegenleistung eingeräumt werden müsste.

In Rahmen der Gesamtabwägung der Kriterien ist festzuhalten, dass die Freiwilligkeit der Einwilligung in vielen Fällen zweifelhaft wäre.

Die Voraussetzung der Informiertheit wird ebenfalls nur schwer eingehalten werden können. Denn hierzu muss der Einwilligende vor Beginn der Datenerhebung insbesondere darüber in Kenntnis gesetzt werden, welche Art von Daten zu welchem Zweck verarbeitet werden, wer die verantwortliche datenverarbeitende Stelle ist, wie diese zu erreichen ist und an welche Dritten die Daten im Falle der Übermittlung weitergegeben werden.[155] Insbesondere die Information, an welche Dritten die Daten weitergegeben werden, wird ein Unternehmen oder eine Behörde, die Datencontainer an Dritte übermitteln will, oftmals nicht herausgeben wollen oder können.

Auch die Voraussetzung der Bestimmtheit der Einwilligung, die unmittelbar aus dem Zweckbindungsgrundsatz folgt, wird stets Probleme aufwerfen. Denn hiernach dürfen Daten nur für festgelegte, eindeutige, und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine pauschale Einwilligungsklausel wäre danach unwirksam.[156] Dies bedeutet, dass ein Unternehmen, das einen Datencontainer schafft, den es Dritten für bestimmte algorithmische Entscheidungsverfahren zur Verfügung stellt, diesen Zweck vor der Erhebung der Daten verfolgen muss. Soll der Zweck erst nach der Datenerhebung hinzutreten, müsste eine diesbezügliche Einwilligung eingeholt werden. „Datenraffinerien“ werden an dieser Schranke regelmäßig scheitern, da ihr Erwerb der personenbezogenen Daten kein Selbstzweck, sondern nur Mittel für die Weiterverarbeitung für beliebige, zum

[153] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 46.
[154] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 52.
[155] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 59.
[156] *Kühling/Buchner*, DS-GVO und BDSG, Art. 7 Rn. 61-62.

Zeitpunkt der Einwilligung kaum vorhersehbare Zwecke ist, die ihrerseits nicht mehr von der ursprünglichen Einwilligung abgedeckt sind. Die Einholung einer neuen Einwilligung für Weiterverarbeitungen dürfte im Big Data-Bereich regelmäßig zu aufwendig sein.

Insgesamt lässt sich festhalten, dass der Einholung einer wirksamen Einwilligung in der vorliegenden Fallgestaltung beträchtliche Hürden gegenüberstehen. Beachtet man schließlich, dass eine wirksam eingeholte Einwilligung nach Art. 7 Abs. 3 S. 1 DS-GVO jederzeit widerrufen werden kann, was die Pflicht zur Löschung (Art. 17 Abs. 1 Buchst. b DS-GVO) und zur Benachrichtigung aller Empfänger der Daten zur Folge hat (Art. 19 S. 1 DS-GVO), erweist sich die Einwilligung letztlich als ungeeignet, um sie für Big Data-Sammlungen und deren Anwendung nutzbar zu machen.

4. Zusammenfassung: Zulässigkeit der Datenverarbeitung

Die Verarbeitung von personenbezogenen Daten im Big Data-Bereich nach der Datenschutz-Grundverordnung dürfte nur unter engen Grenzen zulässig sein. Anwender anonymisierter Datencontainer laufen bei allzu feinmaschiger Auswertung Gefahr, in den Anwendungsbereich der Datenschutz-Grundverordnung zu fallen, die eine Weiterverarbeitung der Daten stark erschwert. Das europäische Datenschutzrecht legt eine streng anonymisierte Datenverarbeitung nahe – sofern diese erfolgt, trifft es keine Regelungen.

5. Die konkrete Ausgestaltung der Verarbeitung

Das Datenschutzrecht stellt auch nach der Klärung der Frage des „ob“ einer zulässigen Verarbeitung personenbezogener Daten nicht unerhebliche Hürden hinsichtlich des „wie“ einer nach Art. 6 DS-GVO erlaubten Datenverarbeitung auf. Zu nennen sind hier

- Transparenzpflichten nach Art. 13 f. DS-GVO und
- Rechte der von einer Algorithmen-Entscheidung betroffenen Person nach Art. 12, 15 ff. DS-GVO, aber auch
- Pflicht zum Treffen von Sicherheitsvorkehrungen (Art. 32 DS-GVO),
- Pflicht zu datenschutzfreundlichen Technikgestaltungen und Voreinstellungen (Art. 25 DS-GVO),
- Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung bei Einsatz neuer und risikoträchtiger Technologien (Art. 35 DS-GVO) einschließlich der Konsultation der Aufsichtsbehörde (Art. 36 DS-GVO),
- Pflicht zur Einrichtung von Datenschutzbeauftragten beim Verantwortlichen (Art. 37 ff. DS-GVO),

- Mechanismen der regulierten Selbstregulierung wie Verhaltensnormsetzung durch Verbände und Zertifizierungslösungen (Art. 40 ff. DS-GVO) sowie nicht zuletzt
- eine effektive datenschutzrechtliche Aufsicht (Art. 51 ff. DS-GVO).

Zu den neuen Betroffenenrechten nach der Datenschutz-Grundverordnung gehören auch das Recht auf Löschung („Recht auf Vergessenwerden“) gemäß Art. 17 DS-GVO und das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO. Das Recht auf Löschung, das nach Widerruf einer Einwilligung oder nach Widerspruch gegen eine gesetzlich gestattete Datenverarbeitung eingreift, wird verlängert durch die Pflicht zur Mitteilung der Löschung nach Art. 19 DS-GVO. So wird dem von der Rechtsprechung des EuGH[157] entwickelten und in die Datenschutz-Grundverordnung übernommenen „Recht auf Vergessenwerden“ eine gewisse Durchschlagskraft verliehen. Durch die Mitteilung wird die Daten verarbeitende Stelle gleichsam „bösgläubig“ gemacht; stützt sich beispielsweise eine Big Data-Anwendung allein auf eine Einwilligung, die widerrufen wird, unterliegt auch der Verantwortliche einer solchen Anwendung der Löschungspflicht. Zwar steht die Mitteilungspflicht unter einem Verhältnismäßigkeitsvorbehalt; berücksichtigt man allerdings, dass der Verantwortliche, der die Daten bei der betroffenen Person erhoben hat, zu Transparenz und Rechenschaft verpflichtet ist, wird ihm der Empfänger der von ihm übermittelten Daten in aller Regel bekannt sein, so dass er sich kaum auf Unverhältnismäßigkeit wird berufen können. Auch diese Pflichten könnten im Big Data-Bereich mittelbar zur Vornahme wirksamer Anonymisierungen führen.

Speziell mit Blick auf die algorithmenbasierte Verarbeitung ist Art. 22 DS-GVO in den Blick zu nehmen, der die Zulässigkeit vollautomatisierter Entscheidungsfindung regelt, sowie die flankierenden Transparenzgebote nach Art. 12 ff. DS-GVO.

a. Datenschutzrechtliche Zulässigkeit einer vollautomatisierten Entscheidung

Bei der rechtlichen Situation des Antragstellers oder Bewerbers, dessen Antrag oder Bewerbung durch einen Algorithmus mit den Daten aus dem Datencontainer abgeglichen werden soll, um eine Entscheidung über den Antrag oder die Bewerbung zu treffen, ist Art. 22 DS-GVO zu beachten. Nach Art. 22 Abs. 1 DS-GVO hat die jeweils 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 beeinträchtigt. Klassisches Beispiel eines

[157] EuGH, Urt. v. 13.5.2014 – C-131/12 - Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, in juris.

solchen Profilings ist die Erstellung von Profilen zur Persönlichkeit, zum Verhalten oder zu Aufenthaltsorten und Bewegungen durch Sammlung und Auswertung von Daten. Diese Daten können beispielsweise durch Tracking beziehungsweise Webtracking und im Internet hinterlassenen Cookies, freiwillig oder zumindest mit Einwilligung veröffentlichte Informationen z. B. zu sozialen Kontakten, politischer Einstellung, persönlichen Vorlieben, finanziellen Verhältnissen, gesundheitlicher Situation und weiteren Angaben, die ein modellhaftes, auf Algorithmen beruhendes Gesamtbild einer individuellen Persönlichkeit ergeben, auch durch die Sammlung von Informationen aus der Nutzung „smarter" Geräte wie Smartphones, Haushaltsgeräte, Kraftfahrzeuge oder auch „Wearables" wie z. B. „Gesundheitsarmbänder" gesammelt und zu Profilen verarbeitet werden, mit denen künftige Nutzerdaten abgeglichen werden.[158]

Der Anwendungsbereich des Art. 22 Abs. 1 DS-GVO ist jedenfalls dann eröffnet, wenn die Entscheidung über den Antrag oder die Bewerbung allein aufgrund des automatisierten Abgleichs mit den Daten aus dem Datencontainer durch den Algorithmus erfolgt und die Entscheidung negativ ausfällt.[159] Denn für eine „Entscheidung" ist es erforderlich, dass eine tatsächliche Wahlmöglichkeit besteht.[160] Eine Entscheidung, die ausschließlich auf einer automatisierten Datenverarbeitung beruht, liegt vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.[161] Davon zu unterscheiden sind die Entscheidungsunterstützung und -vorbereitung durch automatisierte Verarbeitungen.[162] Die Haltung des Europäischen Parlaments, das grundsätzliche Verbot nach Art. 22 Abs. 1 DS-GVO schon bei nur „vorrangig automatisierten Entscheidungen" vorzusehen, konnte sich im Gesetzgebungsverfahren nicht durchsetzen.[163] Für eine inhaltliche Bewertung und darauf gestützte Entscheidung einer natürlichen Person kann es schon ausreichend sein, wenn sich die Überprüfung des seitens des Algorithmus automatisiert gefundenen Ergebnisses durch eine informierte und gegebenenfalls zur Abweichung befugte natürliche Person auf das Herausgreifen nicht plausibler Entscheidungen beschränkt. [164] Sollte eine solche Nachprüfung vorgenommen werden, die sich nicht nur in einer bloßen Stichprobenkontrolle erschöpft,[165] so wäre der Anwendungsbereich der Norm nicht eröffnet. Zudem liegt von

[158] Vgl. Wikipedia-Eintrag zu „Profiling" (https://de.wikipedia.org/wiki/Profiling), (letzter Abruf: 25.8.2018); mehr zu „Wearables" in Form von Gesundheitsarmbändern unter Kapitel 2 II.
[159] Vgl. auch den 71. Erwägungsgrund zur Datenschutz-Grundverordnung.
[160] *Ernst*, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, 1026 (1029).
[161] *Ernst*, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, 1026 (1029f.); Paal/Pauly/*Martini*, DSGVO/BDSG, Art. 22 Rn. 16.
[162] Paal/Pauly/*Martini*, DSGVO/BDSG, Art. 22 Rn. 20.
[163] Vgl. Gola/*Schulz*, DS-GVO, Art. 22 Rn. 12.
[164] Kühling/*Buchner*, DS-GVO und BDSG, Art. 22 Rn. 15.
[165] Kühling/*Buchner*, DS-GVO und BDSG, Art. 22 Rn. 15.

vornherein keine Entscheidung aufgrund einer ausschließlich automatisierten Verarbeitung vor, wenn die automatisierte Datenverarbeitung nur der Unterstützung der Entscheidungsfindung einer natürlichen Person dient.[166]

Wenn also Anträge und Bewerbungen zumindest einer Nachprüfung einer informierten und gegebenenfalls zur Abweichung befugten natürlichen Person unterliegen werden, fällt der Abgleich der erhobenen personenbezogenen Daten mit dem aus Big Data gewonnenen Raster schon aus dem Anwendungsbereich der Norm heraus. Dieses Ergebnis ist auch mit dem Schutzzweck der Norm vereinbar. Zweck der Norm des Art. 22 Abs. 1 DS-GVO ist nicht, eine höhere Ergebnisrichtigkeit der jeweiligen Entscheidung zu erreichen. Sollte eine natürliche Person aufgrund derselben Daten sowie einem vergleichbaren Verarbeitungsvorgang zu demselben (falschen) Ergebnis kommen, würde diese Entscheidung schon gar nicht in den Anwendungsbereich des Art. 22 Abs. 1 DS-GVO fallen. Normzweck ist es vielmehr zu verhindern, dass ein Gefühl des Ausgeliefertseins und der Hilflosigkeit gegenüber der automatisierten Entscheidungsfindung zum Prinzip des gesellschaftlichen Alltags wird. Zudem wird die menschliche Individualität geschützt.[167]

Sollte eine Entscheidung über den Antrag oder die Bewerbung allein aufgrund eines Profilings erfolgen, wäre der Anwendungsbereich des Art. 22 Abs. 1 DS-GVO eröffnet, wenn die Entscheidung über einen Antrag oder eine Bewerbung für die betroffene Person negativ ausfällt. Denn dann läge eine Entscheidung vor, die ihr gegenüber rechtliche Wirkung entfaltet oder sie zumindest in ähnlicher Weise erheblich beeinträchtigt. Für die alternative Konstellation, in der die Entscheidung für die betroffene Person ausschließlich positiv ausfällt, ist noch nicht geklärt, ob die Verarbeitung in den Anwendungsbereich des Art. 22 Abs. 1 DS-GVO fällt. Gegen die Anwendung von Art. 22 Abs. 1 DS-GVO bei für die betroffene Person rein positiven Entscheidungen spricht die Alternative „oder sie in ähnlicher Weise erheblich beeinträchtigt“. Denn eine erhebliche Beeinträchtigung liegt bei einer ausschließlich positiven Entscheidung nicht vor.[168]

Art. 22 Abs. 2 DS-GVO normiert Ausnahmen vom grundsätzlichen Verbot nach Abs. 1. Dieses Verbot automatisierter Entscheidungsfindung gilt nicht, wenn die Entscheidung

- für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist (a),
- aufgrund von Rechtsvorschriften der Union oder der Mitgliedsstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und

[166] Kühling/*Buchner*, DS-GVO und BDSG, Art. 22 Rn. 14.
[167] *Ernst*, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, 1026 (1030).
[168] Kühling/*Buchner*, DS-GVO und BDSG, Art. 22 Rn. 25; a. A. Paal/Pauly/*Martini*, DSGVO/BDSG, Art. 22 Rn. 28, der auf die Beeinträchtigung des Schutzzwecks abstellt.

Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten (b) oder

- die Entscheidung mit Einwilligung der betroffenen Person erfolgt (c).

Eine weitreichende Ausnahme sieht Art. 22 Abs. 2 Buchst. a DS-GVO danach für Vertragsabschlüsse vor. Der Begriff der Erforderlichkeit ist hier weit zu verstehen und verlangt keine Alternativlosigkeit der automatisierten Entscheidungsfindung, sondern lediglich einen unmittelbaren Zusammenhang mit dem Vertragsschluss. Eine echte Einschränkung stellt das Tatbestandsmerkmal daher nicht dar, sondern eröffnet die Ausnahme vom Verbot nach Absatz 1 letztlich für alle vertragsbezogenen Datenverarbeitungen.

Eine automatische Entscheidungsfindung kann grundsätzlich gemäß Art. 22 Abs. 2 Buchst. b DS-GVO auch durch eine Rechtsvorschrift der Union oder eines Mitgliedsstaates zugelassen werden, wenn die Rechtsvorschrift angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthält. Für zivilrechtliche Konstellationen dürfte die Vorschrift eher unerheblich sein.

Die Ausnahme gemäß Art. 22 Abs. 2 Buchst. c DS-GVO verlangt die Einwilligung der betroffenen Person. Für diese gelten grundsätzlich die schon zuvor dargelegten Grundsätze.[169] Zusätzlich fordert Art. 22 Abs. 2 Buchst. c DS-GVO die Ausdrücklichkeit der Einwilligung. Dies bedeutet, dass sich die Einwilligung ausdrücklich auch darauf beziehen muss, dass eine den Einzelnen betreffende Entscheidung ausschließlich auf einer automatisierten Datenverarbeitung beruht.[170]

Weiterhin müssen seitens des Verantwortlichen nach Art. 22 Abs. 3 DS-GVO angemessene Maßnahmen getroffen werden, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens ein Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört. Diese angemessenen Maßnahmen decken sich mit denjenigen bei Art. 22 Abs. 2 Buchst. b DS-GVO. Zudem gelten auch hier die Informationspflichten der Art. 13 Abs. 2 Buchst. f bzw. Art. 14 Abs. 2 Buchst. g DS-GVO und Art. 22 Abs. 4 DS-GVO ist als Begrenzung ebenfalls anwendbar, wobei hier grundsätzlich auf Art. 9 Abs. 2 Buchst. a DS-GVO (Einwilligung) abgestellt werden kann.

Die Garantien nach Art. 22 Abs. 3 DS-GVO, insbesondere das Recht, die Entscheidung einer zumindest der nochmaligen Überprüfung durch eine Person unterziehen zu lassen, dürften letztlich die eigentliche Bedeutung des Art. 22 DS-GVO ausmachen; dies dürfte bei entsprechender Auslegung in Anbetracht des 71. Erwägungsgrundes zur Datenschutz-Grundverordnung zumindest auch eine rudimentäre Erläuterung umfassen, nicht jedoch umfassende Information über die

[169] Siehe oben 3.
[170] Kühling/*Buchner*, DS-GVO und BDSG, Art. 22 Rn. 42.

Auskunft nach Art. 15 DS-GVO hinaus. Der Wortlaut von Art. 22 DS-GVO gibt dafür keine entsprechenden Anhaltspunkte und der Erwägungsgrund erlangt als solcher keine Rechtsverbindlichkeit, so dass allenfalls eine entsprechend weite Auslegung, nicht aber ein eigenes „Recht auf Erläuterung“ in Betracht kommt. Durch die Vorschrift kann eine Entscheidung nach Maßstäben bewirkt werden, wie sie auch vor dem Zeitalter der komplexen digitalen Algorithmen bereits galten – eine von einer natürlichen Person getroffene Entscheidung, die mit Unterstützung von IT-Verfahren ergeht.

b. Transparenz

Aus Art. 13 Abs. 2 Buchst. f bzw. Art. 14 Abs. 2 Buchst. g DS-GVO folgen Informationspflichten, nach denen der Verantwortliche sowohl über das Bestehen einer automatisierten Entscheidungsfindung informieren muss als auch über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Datenverarbeitung für die jeweils betroffene Person. Art. 13 Abs. 2 Buchst. f und Art. 14 Abs. 2 Buchst. g DS-GVO gewähren wohl keinen Anspruch auf Offenlegung des mathematischen Algorithmus, sondern nur eine allgemeinverständliche Beschreibung (vgl. Art. 12 Abs. 1 DS-GVO) der Berechnungsgrundlagen und der Methodik der Berechnung.[171] Nach dem 71. Erwägungsgrund zur Datenschutz-Grundverordnung „sollte der für die Verarbeitung Verantwortliche geeignete mathematische oder statistische Verfahren für das Profiling verwenden, technische und organisatorische Maßnahmen treffen, mit denen in geeigneter Weise insbesondere sichergestellt wird, dass Faktoren, die zu unrichtigen personenbezogenen Daten führen, korrigiert werden, das Risiko von Fehlern minimiert wird und personenbezogene Daten in einer Weise sichern, dass den potenziellen Bedrohungen für die Interessen und Rechte der betroffenen Person Rechnung getragen wird und mit denen Diskriminierung verhindert wird.“ Im Normtext findet sich diese Vorgabe freilich nicht wieder. Problematisch ist die Information der betroffenen Person über die involvierte Logik freilich auch dann, wenn es sich um selbstlernende Algorithmen handelt. Hier werden dem Verwender nicht selten wichtige Informationen fehlen, wenn der Algorithmus eigenständig neue Kategorien von entscheidungsrelevanten Daten bildet oder eigenständig deren Gewichtung vornimmt. Da Art. 13 Abs. 2 Buchst. f DS-GVO innerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung eine Form der „Algorithmentransparenz“ vorsieht, wird gespannt abzuwarten sein, wie weitreichend die Vorschrift von den Aufsichtsbehörden und Gerichten verstanden wird; dass bei einem Einsatz selbstlernender Algorithmen der Hinweis auf diesen Umstand genügt, erscheint bei dem Wortlaut der Norm eher unwahrscheinlich.

Auch über das zugrundeliegende Datenmaterial lassen sich so keine verwertbaren Erkenntnisse gewinnen, da allein die Information darüber, dass ein aus

[171] *Eßer*/Kramer/Lewinski/Auernhammer, DSGVO – BDSG, Art. 13 DSGVO Rn. 35; Paal/*Pauly*, DSGVO, Art. 13 Rn. 31.

Referenzdaten gewonnenes Raster verwendet wird, genügen dürfte.[172] Mit den wohl synonymen Begriffen „Tragweite und angestrebte Auswirkungen“ dürfte der Unionsgesetzgeber meinen, dass der Verantwortliche das Tableau möglicher Entscheidungen gegenüber der betroffenen Person offenlegen muss,[173] zum Beispiel, dass anhand der erhobenen Daten bei einer online-Darlehensprüfung sowohl das „ob“ des Vertragsschlusses als auch das „wie“ der Darlehensvergabe (Zinssätze, Tilgungsfristen, weitere Darlegungslasten des Darlehensnehmers usw.) bestimmt wird.

Nach dem Erwägungsgrund 71 zur Datenschutz-Grundverordnung muss der betroffenen Person zudem ein Anspruch auf Erläuterung der Entscheidung eingeräumt werden. Diese weitgehenden Informationspflichten könnten der mit der Automatisierung beabsichtigten Beschleunigung womöglich entgegenwirken, was sich mit dem Wortlaut von Art. 22 Abs. 3 DS-GVO in Einklang bringen ließe („Darlegung des eigenen Standpunkts“, „Anfechtung der Entscheidung“). Zudem dürfen Entscheidungen aufgrund der Ausnahme gemäß Art. 21 Abs. 4 DS-GVO nicht auf besonderen Kategorien von Daten gemäß Art. 9 Abs. 1 DS-GVO beruhen, wenn nicht Art. 9 Abs. 2 Buchst. a (Einwilligung) oder g (erhebliches öffentliches Interesse) DS-GVO einschlägig ist.

Aus Art. 13 Abs. 3 und Art. 14 Abs. 4 DS-GVO folgen Informationspflichten auch für den Fall, dass der Verantwortliche die Daten zu anderen als dem ursprünglichen Erhebungszweck weiterverarbeiten will. Echte Wirkung dürfte dieses Gebot jedoch nur erheben, soweit die Weiterverarbeitung durch den Verarbeiter erfolgt, der die Daten bei der betroffenen Person erhoben hat (Art. 13 Abs. 3 DS-GVO). Weiterverarbeitungen durch Erwerber von Datencontainern dürften bei Pseudonymisierung, wenn der Verantwortliche nicht im Besitz des Schlüssels ist, nach Art. 14 Abs. 5 Buchst. b DS-GVO mit einem Ausschluss der Informationspflicht verbunden sein, weil es für den Verantwortlichen nur mit nach der Datenschutz-Grundverordnung unverhältnismäßigem Aufwand möglich ist, die Information vorzunehmen.

c. Datenschutz-Folgeabschätzung

Gemäß Art. 35 Abs. 1 DS-GVO hat der Verantwortliche eine Datenschutz-Folgeabschätzung durchzuführen, wenn die Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Näher ausgeführt wird dies in Art. 35 Abs. 3 DS-GVO; ein hohes Risiko wird angenommen bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für

[172] Anders wohl Kühling/Buchner/*Bäcker*, DS-GVO und BDSG, Art. 13 Rn. 54.
[173] Vgl. *Bäcker*, in: Kühling/Buchner, Kommentar DS-GVO und BDSG, 2. Aufl. 2018, Art. 13 Rn. 55.

Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen (Art. 35 Abs. 3 Buchst. a DS-GVO). Diese Voraussetzungen dürften sowohl bei der Einführung von neuen Big Data-Anwendungen als auch beim Einsatz von Algorithmen zur Verarbeitung personenbezogener Daten erfüllt sein. Zum Inhalt der Datenschutz-Folgeabschätzung sieht Art. 35 Abs. 7 Buchst. c und d DS-GVO auch eine Risikobewertung und eine Darstellung der Maßnahmen zur Bewältigung dieser Risiken vor. Art. 36 DS-GVO bestimmt eine Pflicht zur Konsultation der Aufsichtsbehörde für den Fall der Ermittlung eines „hohen Risikos“. Inwieweit dies auch die Untersuchung von Algorithmen mit einbezieht, ist noch nicht geklärt; da allerdings die automatisierte Entscheidungsfindung auch als Verarbeitung personenbezogener Daten angesehen wird, spricht einiges dafür, dass Algorithmen Gegenstand der Folgenabschätzung sind.

Welchen Stellenwert diese Verträglichkeitsprüfung erhält, muss sich erst noch im Vollzug der Datenschutz-Grundverordnung erweisen; dass die Datenschutz-Aufsichtsbehörden aufgrund der Folgenabschätzung zu einer Art „Algorithmen-Überprüfungsstelle“ werden, ist allerdings derzeit nicht zu erkennen – hierfür dürfte es vielfach schon am erforderlichen Fachpersonal der auf klassischen Datenschutz spezialisierten Aufsichtsbehörden fehlen. Für die Überprüfung einer Folgenabschätzung zum Einsatz komplexer Algorithmen bedarf es zunächst Standards für eine nachvollziehbare und prüffähige Darstellung durch den Verantwortlichen; die Datenschutz-Grundverordnung verlangt lediglich vage eine „systematische Beschreibung“ (Art. 35 Abs. 7 Buchst. a DS-GVO). Dies könnte auch die Offenlegung des Quellcodes einschließen, den zu prüfen jedoch einen erheblichen Ressourceneinsatz bedeuten dürfte. Das gilt es freilich auch bei der Erbringung der Datenschutz-Folgenabschätzung zu beachten; werden die Anforderungen an die beizubringenden Unterlagen und die Aussagekraft der Folgenabschätzung zu hoch angesetzt, drohen sie zu einer unverhältnismäßigen Belastung zu werden. Zu begrüßen wären diesbezügliche Leitlinien des Europäischen Datenschutzausschusses (vgl. Art. 70 Abs. 1 S. 2 Buchst. e DS-GVO).

Aussichtsreicher als eine ad-hoc Kontrolle von Datenschutz-Folgeabschätzungen dürfte aus Sicht der Aufsichtsbehörden die Entwicklung anerkannter Verhaltensregeln (Art. 40 DS-GVO) sein, die im Rahmen der Datenschutz-Folgenabschätzung immerhin „gebührend zu berücksichtigen“ sind (Art. 35 Abs. 8 DS-GVO). Da die Aufsichtsbehörde über ein umfangreiches Instrumentarium verfügt, das gegen den Verantwortlichen zur Anwendung kommen kann, dürfte ein gewisser Druck erzeugt werden, diese Verhaltensregeln zu beachten, auch wenn eine Bußgeldsanktionierung nach Art. 83 Abs. 5 DS-GVO nicht vorgesehen ist.

d. Rechenschaftspflicht

Eine im Bereich der Big Data-Anwendungen und des Einsatzes von Algorithmen, insbesondere solche mit fortgeschrittener Architektur, nicht unerhebliche Veränderung könnte auch Art. 5 Abs. 2 DS-GVO mit sich bringen. Danach ist der Verantwortliche auch für die Einhaltung der datenschutzrechtlichen Grundsätze verantwortlich und muss sie nachweisen können („Rechenschaftspflicht“). In diesen Grundsätzen finden zahlreiche konkrete Pflichten wie etwa die Transparenzpflichten nach Art. 12 ff. DS-GVO Widerhall (vgl. z. B. Art. 5 Abs. 1 Buchst. a DS-GVO). Gerade im Bereich der automatisierten Verarbeitung etwa mit Algorithmen könnte dies dazu führen, dass sich eine Art „accountability by design“ durchsetzt, indem Verwender von Algorithmen aus datenschutzrechtlichen Gründen eine gewisse Vorsorge bei der Gestaltung ihrer Algorithmen walten lassen. Für den Datenschutz als solchen ist dies bereits durch das Prinzip des „privacy by design“ verbürgt, das sich in Art. 25 DS-GVO wiederfindet. Ob und inwieweit diese Ansätze sich durchsetzen, wird allerdings auch davon abhängen, wie weitreichend das neue Datenschutzrecht, das den Aufsichtsbehörden eine Vielzahl von Kontrollmöglichkeiten lässt, vollzogen wird.

III. Allgemeines Gleichbehandlungsgesetz

Will man den Rechtsrahmen für Big Data Anwendungen bestimmen und geht es um Diskriminierungsverbote und Teilhabe, stellt sich die Frage nach der Relevanz des Allgemeinen Gleichbehandlungsgesetzes (AGG).

Wo Algorithmen automatisiert entscheiden, werden die implementierten Maßstäbe immer wieder gleichförmig angewandt. Etwaige Rechtswidrigkeiten und andere Fehler dieser Maßstäbe haben deshalb eine besonders große Tragweite. Sie fließen in jede Entscheidung ein, selbst wenn sie sich nicht auch in jeder am Ende auswirken. Soweit die den Entscheidungen zugrunde liegenden Algorithmen für Dritte nicht verstehbar sind – gemeint ist hier nicht mathematisches Verständnis, sondern Transparenz, welche Aspekte in welcher Weise zu welchen Ergebnissen führen können –, ist ihnen eine rechtliche Überprüfung der Entscheidung nicht möglich. Das ist zivilrechtlich unproblematisch, soweit Entscheidungen einer rechtlichen Überprüfbarkeit entzogen sind, der freie Wille also unbeschränkt ist - was in unserem auf Privatautonomie beruhenden Zivilrecht ja nicht selten ist. Soweit aber die bürgerliche Rechtsordnung die Entscheidungsmöglichkeiten von Rechtssubjekten einengt, ist es notwendig, die Entscheidung auf die Wahrung dieser Grenzen überprüfen zu können. Das mehrere EU-Richtlinien zur Gleichbehandlung umsetzende AGG vom 14. August 2006 stellt solche Grenzen auf, soweit es Benachteiligungen verbietet. Fraglich ist, ob und wie weit das AGG de lege lata

den von ihm verfolgten Schutz vor Diskriminierung auch gegenüber algorithmenbasierten Entscheidungsprozessen gewährt. Das wird bezweifelt. So hält *Martini* eine Ergänzung des Katalogs der Anwendungsfälle des § 2 Abs. 1 AGG um eine Nr. 9 für Ungleichbehandlungen, die auf einer algorithmenbasierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen, für erwägenswert.[174]

Folgende Beispiele sollen das Problem veranschaulichen:

a) Auf der Homepage der Bank B kann online ein Kleinkredit beantragt werden. Über die jeweilige Zusage wird – nach ausdrücklicher Einwilligung der Antragsteller[175] *– automatisch, innerhalb weniger Minuten und allein aufgrund einer algorithmenbasierten Datenauswertung entschieden.*

b) Auch die Sparkasse S bietet auf ihrer Homepage die Möglichkeit, einen Kleinkredit online zu beantragen. Die Anträge werden von Mitarbeiter X geprüft, der innerhalb einiger Tage über eine Zusage entscheidet.

Frau F und Herr M aus Kiel befinden sich in ähnlichen Lebenssituationen. Beide beantragen etwa zeitgleich jeweils einen Kleinkredit in derselben Höhe bei B und bei S. Nur M erhält Zusagen. F kennt M, weiß von seinen Zusagen und argwöhnt, dass sie wegen ihres Geschlechts gegenüber M benachteiligt worden sei. Auf Nachfragen von F erklärt B, so habe nun einmal der Computer entschieden. S weist eine unzulässige Benachteiligung durch X zurück.

Das AGG normiert Benachteiligungsverbote für das – für die vorliegende Fragestellung nicht interessierende – Arbeitsrecht und, in § 19, für das Zivilrecht. Das zivilrechtliche Benachteiligungsverbot hat zwei Stufen.

---

[174] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1021).

[175] Ob das gewählte Beispiel ohne ausdrückliche Einwilligung der Antragsteller datenschutzrechtlich zulässig wäre, ist fraglich. Art. 22 Abs. 1 DSGVO bestimmt die grundsätzliche Unzulässigkeit solcher automatisierten Entscheidungen. Die hier gewählte Ausnahme für den Fall einer ausdrücklichen Einwilligung der betroffenen Person bestimmt Art. 22 Abs. 2 c) DSGVO. Vom Verständnis des weiteren Erlaubnistatbestands in Art. 22 Abs. 2 a) DSGVO, namentlich der darin vorausgesetzten Erforderlichkeit für den Abschluss oder die Erfüllung eines Vertrags hängt ab, ob das Beispiel auch ohne ausdrückliche Einwilligung zulässig wäre. Kühling/*Buchner*, DSGVO, Art. 22 Rn. 30, nimmt die Erforderlichkeit schon an, wenn ein unmittelbarer sachlicher Zusammenhang zwischen automatisierter Entscheidung und konkretem Zweck des Rechtsgeschäfts besteht, den er beispielsweise in Fällen der Kreditvergabe bejaht. Für ein großzügiges Verständnis des Begriffs der Erforderlichkeit (mit dem mutmaßlich selben Ergebnis für die Beurteilung der Online-Kreditvergabe) spricht sich auch *Plath*, BDSG/DSGVO, Art. 22 DSGVO Rn. 8, aus. Nach *Härting*, Internetrecht, Datenschutzrecht Rn. 292, setzt die Erforderlichkeit dagegen voraus, dass die automatisierte Entscheidung zu den vertraglich geschuldeten Dienstleistungen gehört – demgemäß hält er die Online-Kreditvergabe ohne ausdrückliche Einwilligung gemäß Art. 22 Abs. 1 DSGVO für unzulässig.

Vor Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft schützt es weitreichender, nämlich bei der Begründung, Durchführung und Beendigung zivilrechtlicher Schuldverhältnisse im Sinne von § 2 Abs. 1 Nr. 5 bis 8 AGG. Dabei legt § 2 Abs. 1 Nr. 8 AGG den zivilrechtlichen Anwendungsbereich des AGG als Grundnorm fest.[176] Beschränkend ist hier allein das Erfordernis des der-Öffentlichkeit-zur-Verfügung-Stehens. Die Auslegung dieser Voraussetzung ist streitig,[177] wobei die unterschiedlichen Auffassungen kaum und in dem hier interessierenden Bereich algorithmenbasierter Entscheidungsprozesse gar keine praktische Relevanz haben. Schon mit der engeren Auslegung, die fordert, dass der Anbieter seine angebotene Leistung nicht nur einmal erbringen kann, werden die Fälle, in denen auf Anbieterseite mit algorithmenbasierten Entscheidungen realistisch gerechnet werden kann, alle umfasst. Der weiteren Auslegung, nach der alle Leistungen erfasst werden, die öffentlich angeboten werden – auch wenn der Anbieter sie nur einmal erbringen kann – bedarf es also in unserem Zusammenhang nicht.

Der Schutz vor einer Benachteiligung wegen des Geschlechts, der Religion, einer Behinderung, des Alters oder der sexuellen Identität ist schwächer als der wegen der Rasse oder der ethnischen Herkunft ausgestaltet: Zum einen ist er beschränkt auf die in § 19 Abs. 1 Nr. 1 AGG legaldefinierten Massengeschäfte, Fälle nachrangiger Bedeutung des Ansehens der Person und Versicherungen – wobei auch dieser Aspekt für die hier in Rede stehenden Fälle algorithmenbasierter Entscheidungsprozesse keine praktisch relevante Einschränkung darstellen sollte. Zum anderen besteht insoweit die Möglichkeit der Rechtfertigung der Benachteiligung durch einen sachlichen Grund gemäß § 20 Abs. 1 AGG.

Die Beispielsfälle fallen unter das zivilrechtliche Benachteiligungsverbot. Zwar stellen Kleinkreditverträge keine Massengeschäfte gemäß § 19 Abs. 1 Nr. 1 AGG dar, weil sie entgegen der Legaldefinition gerade nicht „ohne Ansehen der Person" abgeschlossen werden. Das Ansehen der Person hat aber bei Kleinkreditverträgen eine nachrangige Bedeutung, so dass es sich um den Massengeschäften gleichgestellte Verträge handelt.[178]

Die Aufzählung von Benachteiligungsgründen in den §§ 1 und 19 Abs. 1 AGG ist abschließend,[179] so dass Ansprüche nach dem AGG nicht auf die Unzulässigkeit einer Benachteiligung z. B. aus Gründen der Gesundheit, der

[176] Ziffer 8 wird von den Ziffern 5 bis 7 ergänzt, Palandt/*Ellenberger*, BGB, § 2 AGG Rn. 8.
[177] Zum Streitstand s. Palandt/*Ellenberger*, a.a.O., § 2 AGG Rn. 9 mwN.
[178] So Palandt/*Grüneberg*, a.a.O., § 19 AGG Rn. 3; MükoBGB/*Thüsing*, § 19 AGG Rn. 25; Herberger/Martinek/Rüßmann/*Altmayer*, jurisPK-BGB, § 19 AGG Rn. 11; Staudinger/*Serr* (2018), BGB, § 19 AGG Rn. 40.
[179] Palandt/*Ellenberger*, a.a.O., § 1 AGG Rn. 1.

Finanzkraft oder der Weltanschauung[180] gestützt werden können. Dass das zivilrechtliche Benachteiligungsverbot des AGG nach § 19 Abs. 4 und 5 auf familien- und erbrechtliche Ansprüche und auf Schuldverhältnisse, die ein besonderes Nähe- oder Vertrauensverhältnis begründen, keine Anwendung findet,[181] ist mangels praktischer Bedeutung algorithmenbasierter Entscheidungen in diesen Bereichen wiederum für die hiesige Fragestellung uninteressant.

Von den in § 3 AGG aufgeführten Benachteiligungsformen sind zwei – die Belästigung gemäß Absatz 3 und die sexuelle Belästigung gemäß Absatz 4 – aufgrund der vorausgesetzten Schaffung eines würdeverletzenden Umfeldes ersichtlich nur für das Arbeitsrecht bedeutsam, so dass sie bei der vorliegenden Betrachtung ausgeklammert werden können. Interessant sind hier allein die unmittelbare Benachteiligung gemäß § 3 Abs. 1 AGG und die mittelbare gemäß Absatz 2. Beide setzen voraus, dass eine – die letztlich benachteiligte – Person aus den in §§ 1 bzw. 19 Abs. 1 AGG genannten Gründen eine weniger günstige Behandlung erfährt, erfahren hat oder erfahren würde als eine andere Person in vergleichbarer Situation.

Hier sei für den Beispielsfall a) unterstellt, dass der von B bei der automatisierten Entscheidung verwandte Algorithmus bei im Übrigen gleichen Voraussetzungen der antragstellenden Personen zu Absagen für Frauen und Zusagen für Männer führen kann.
Für Beispielsfall b) sei unterstellt, dass Mitarbeiter X zu der Meinung neigt, dass Frauen generell in Geldangelegenheiten irrational agierten und deshalb weniger kreditwürdig seien.

In § 21 AGG sind die aus einer unzulässigen Benachteiligung folgenden Ansprüche des Verletzten formuliert: Beseitigung, Unterlassung und Schadensersatz. Sie richten sich gegen den Leistungsanbieter,[182] in den Beispielsfällen also gegen B und S. Der Leistungsanbieter haftet für alle Personen, derer er sich zur Erfüllung seiner Verbindlichkeit gegenüber dem Anspruchsteller bedient.[183] In Betracht kommt für die Zurechnung also in Fall b) der Mitarbeiter X. Im Fall a) ist an all die Personen zu denken, welche für B den unzulässig

[180] Anders als im Arbeitsrecht besteht im Zivilrecht – gesetzgeberisch gewollt (Palandt/*Grüneberg*, a.a.O., § 19 Rn. 1) – kein Schutz nach dem AGG wegen Benachteiligungen aus Gründen der Weltanschauung, vgl. §§ 1 und 19 Abs. 1 AGG.
[181] Z. T. wird dies für unionsrechtlich problematisch erachtet, s. nur Staudinger/*Rieble*, a.a.O., Einl. AGG § 1 Rn. 17 mwN.
[182] Palandt/*Ellenberger*, a.a.O., § 3 AGG Rn. 1.
[183] Palandt/*Ellenberger*, a.a.O., § 3 AGG Rn. 8 mwN. Dogmatisch wird man die Zurechnung nur im Rahmen des Schadensersatzanspruchs nach § 21 Abs. 2 AGG über § 278 BGB vornehmen können, wohingegen beim Beseitigungs- und Unterlassungsanspruch eine mittelbare Störerhaftung anzunehmen sein wird (MükoBGB/*Thüsing*, a.a.O., § 21 AGG Rn. 12).

benachteiligend operierenden Algorithmus programmiert, implementiert, angelernt, also gewissermaßen „hergestellt“ oder seinen Einsatz bestimmt haben. Alternativ wird man zur Inanspruchnahme des Leistungsanbieters auch an der – dogmatisch umstrittenen[184] – Haftung für elektronische Hilfsmittel ansetzen können. Ohne die weitere Voraussetzung[185] des Verschuldens der benachteiligenden Person[186] sind dies ein Beseitigungsanspruch („Abstellen der Benachteiligung für die Zukunft“) und – bei Erstbegehungs-[187] oder Wiederholungsgefahr – ein Unterlassungsanspruch. Erst bei Vorliegen eines Verschuldens besteht der Schadensersatzanspruch gemäß § 21 Abs. 2 S. 1 AGG.

Das Verschulden des Anspruchsgegners wird von § 21 Abs. 2 S. 2 AGG vermutet. Der notwendige Entlastungsbeweis erstreckt sich auch auf das Verschulden von Erfüllungsgehilfen.[188]

An dieser Stelle liegt es nahe, unmittelbare und mittelbare Benachteiligungen differenziert zu betrachten, weil sich bei der unmittelbaren Benachteiligung durch eine algorithmenbasierte Entscheidung das verbotene Kriterium selbst im Algorithmus befinden müsste, während bei der mittelbaren Benachteiligung die (Zusammen-) Wirkung anderer Kriterien zur Diskriminierung führt.

Im Beispielsfall a) läge eine unmittelbare Benachteiligung vor, wenn der Algorithmus eine Geschlechterdifferenzierung dergestalt vornimmt, dass Frauen bei der Entscheidung eine geringere Kreditwürdigkeit zugebilligt wird als Männern. Leicht wäre dies zu erfahren, wenn der Algorithmus nach dem Geschlecht fragt, schwieriger, wenn er es aus anderen Angaben wie z. B. dem Vornamen ableitet. Eine unmittelbare Benachteiligung läge aber auch vor, wenn es zu der Benachteiligung von Frauen dadurch kommt, dass der von B bei den

---

[184] S. hierzu nur MükoBGB/*Grundmann*, § 278 BGB Rn. 46 mwN.; Palandt/*Grüneberg*, a.a.O., § 278 BGB Rn. 11.

[185] Soweit es die Benachteiligung aus Gründen der Rasse, der ethnischen Herkunft oder des Geschlechts betrifft, wird diese Voraussetzung teilweise für europarechtswidrig gehalten – so MükoBGB/*Thüsing*, a.a.O., § 21 AGG Rn. 44 und 47, der hinsichtlich der Diskriminierung wegen Rasse und ethnischer Herkunft auf den Inhalt der RL 2000/43 EG (Antidiskriminierungsrichtlinie) vom 29.6.2000 und hinsichtlich der Diskriminierung wegen des Geschlechts auf den Inhalt der RL 2004/113 EG (Gleichbehandlungsrichtlinie) vom 13.12.2004 (Art. 3 bestimmt jeweils den Geltungsbereich) und die EuGH-Rechtsprechung („Draehmpaehl“, Urt. v. 22.4.1997 - Rs. C-180/95, NJW 1997, 1839) verweist; a. A. Erman/*Westermann*, BGB, § 21 AGG Rn. 1; Staudinger/*Serr*, a.a.O., § 21 AGG Rn. 40. Gegen die Annahme von Europarechtswidrigkeit hinsichtlich einer Diskriminierung wegen der Religion, einer Behinderung, des Alters oder sexuellen Identität spricht, dass die Ausweitung des AGG auf das Zivilrecht insoweit über die genannten RL hinausgeht, also überschießend ist – für diese Gründe wird allerdings eine weitere Richtlinie erarbeitet (Palandt/*Ellenberger*, a.a.O., Einl AGG Rn. 1).

[186] Gemeint ist auch hier der Leistungsanbieter, MükoBGB/*Thüsing*, a.a.O., § 21 AGG Rn. 12.

[187] Palandt/*Grüneberg*, a.a.O., § 21 AGG Rn. 4.

[188] Palandt/*Grüneberg*, a.a.O., § 21 AGG Rn. 5.

Entscheidungen über die Anträge von M und F eingesetzte Algorithmus „selbstlernend“ ist und zu seiner Anlernung eine Vielzahl früherer, noch „menschlich getroffener“ Entscheidungen von B eingegeben wurden. Diese früheren Entscheidungen benachteiligten Frauen – was B und auch ihren Erfüllungsgehilfen nicht bewusst war –, so dass der Algorithmus bei seinem Anlernen diese Benachteiligung von Frauen als Entscheidungsstruktur fortgeschrieben hat.

Die im Beispiel dargestellten Möglichkeiten zeigen, dass schon bei einer unmittelbaren Benachteiligung durch Algorithmen – insbesondere dann, wenn es sich um selbstlernende handelt – damit zu rechnen sein kann, dass sich der Anspruchsgegner erfolgreich exkulpieren kann. Dies gilt umso mehr für mittelbare Benachteiligungen durch algorithmenbasierte Entscheidungen. Wie es zu ihnen kommen kann, erklären *Martini/Nink*[189] verständlich: „Computeralgorithmen sind nicht davor gefeit, ihren Selektionsmechanismen diskriminierende Auslesekriterien zugrunde zu legen, weil sie mithilfe stochastischer Methoden nach statistischen Korrelationen in der Datenbasis fahnden. Sie schließen von Gruppenmerkmalen auf Fehler und Risiken und können dadurch wichtige Anhaltspunkte für rechtmäßige Eingrenzungen von Kontrollroutinen liefern. Ihrem Wesen nach können sie aber keine Kausalitäten ermitteln, die einen zuverlässigen Rückschluss auf den konkreten Einzelfall zulassen. Daraus erwächst das Risiko von (Gruppen-) Diskriminierungen.“ Würde in Beispielsfall a) der Algorithmus in solcher Weise Frauen nur mittelbar benachteiligen, wird sich der Anspruchsgegner erst recht erfolgreich entlasten können. Die sich hier bei der rechtlichen Bewertung auswirkende Besonderheit unzulässiger Benachteiligungen durch algorithmenbasierte Entscheidungen ist letztlich, dass nicht nur der benachteiligten, sondern möglicherweise auch der benachteiligenden Person und ihrer Erfüllungsgehilfen die genaue Funktionsweise des für die Entscheidung herangezogenen Algorithmus nicht bekannt ist – mit anderen Worten: der Algorithmus ist für alle Beteiligten eine Blackbox.

Angemessen erscheint es nicht, dass, bei im Übrigen vorliegenden Voraussetzungen eines Schadensersatzanspruchs nach § 21 Abs. 2 AGG, der Anspruchsgegner sich erfolgreich mit dem Vorbringen exkulpiert, er wisse nicht, was der von ihm eingesetzte Algorithmus tut. Zwar ist denkbar, in der mangelnden Durchschaubarkeit der Entscheidung selbst schon die Diskriminierung zu sehen, wobei allerdings der benachteiligenden Person offenstehen soll, das Fehlen einer Diskriminierung darzulegen und zu beweisen.[190] Zwingend wäre eine solche Lösung aber nicht. Als Zwischenfazit ist deshalb festzuhalten, dass bei algorithmenbasierten Entscheidungen eine

[189] *Martini/Nink*, Wenn Maschinen entscheiden … - vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ-Extra 10/2017, 1 (9).
[190] *v. Roetteken*, AGG, § 22 Rn. 40 mwN., juris.

Exkulpation des Anspruchsgegners leichter möglich sein kann als bei menschlichen Entscheidungen.

Fraglich ist aber auch, ob die unzulässige Benachteiligung de lege lata nicht letztlich nur weniger erfolgversprechend im Prozess verfolgt werden kann, wenn sie durch eine algorithmenbasierte Entscheidung erfolgt ist. Wie es in § 22 AGG heißt, obliegt derjenigen Person, die sich unzulässig benachteiligt sieht, im Prozess zunächst nur, Indizien zu beweisen, die eine unzulässige Benachteiligung vermuten lassen. Gelingt ihr dies, trägt die andere Seite die Beweislast für das Fehlen einer unzulässigen Benachteiligung. Was dies bedeutet, ist zum Teil streitig. Einigkeit besteht darin, dass § 22 AGG gegenüber den allgemeinen Regeln zu Gunsten der klagenden Partei das Beweismaß absenkt.

Teilweise wird vertreten, dass § 22 AGG mit der Beweislast auch gleichermaßen die Darlegungslast die Klägerseite erleichternd verteilt.[191] Diese Ansicht dürfte zutreffend sein, weil es unlogisch scheint, der Klägerseite zwar (im zweiten Schritt) zu erlauben, bloß Indizien zu beweisen, aus denen auf eine unzulässige Benachteiligung geschlossen werden kann – von ihr aber (im ersten Schritt) zu verlangen, dass sie die unzulässige Benachteiligung vollen Umfangs darstellt. Die Beweiserleichterung resultiert ja ersichtlich aus dem Umstand, dass der Klägerseite kein oder allenfalls ein beschränkter Einblick in den von ihr angegriffenen Entscheidungsprozess möglich ist, so dass man von ihr ohne eine Erleichterung auch der Darlegungslast Erklärungen „ins Blaue hinein“ verlangen würde. Gleichwohl wird vertreten, dass hier zu differenzieren sei und sich nur die Beweislast nach § 22 AGG, die Darlegungslast aber nach den allgemeinen Vorschriften, d. h. nach § 138 ZPO richte.[192]

Umstritten ist auch, ob die Beweiserleichterung vollen Umfangs,[193] oder aber nicht hinsichtlich (der äußeren Tatsache) des Vorliegens einer weniger günstigen Behandlung eingreift, sondern nur hinsichtlich (der inneren Tatsache) der Kausalität zwischen Ungleichbehandlung und einem der in § 19 AGG genannten Gründe.[194] Dieser Streit dürfte generell keine praktische Relevanz haben, weil die Ungleichbehandlung als solche von der klagenden Partei ohne Schwierigkeit auch nach den allgemeinen Regeln darzulegen und zu beweisen sein wird. Auf die Idee eines Prozesses wegen einer unzulässigen Benachteiligung wird ja nur kommen, wer weiß, dass jemand anderes eine bessere Behandlung erfahren hat. Dieser Umstand wird also – sofern er nicht sogar unstreitig ist – unproblematisch dem Strengbeweis zugänglich sein.

---

[191] Erman/*Armbrüster*, a.a.O., § 22 AGG Rn. 1; BAG, Urt. v. 25.4.2013, 8 AZR 287/08, NJOZ 2013, 1699, 1702 Rn. 36.
[192] MükoBGB/*Thüsing*, a.a.O., § 22 AGG Rn. 4; Palandt/*Grüneberg*, a.a.O., § 22 Rn. 2.
[193] So Palandt/*Grüneberg*, a.a.O., § 22 AGG Rn. 2; LAG Baden-Württemberg, Urt. v. 1.2.2011, 22 Sa 67/10, juris Rn. 38.
[194] MükoBGB/*Thüsing*, a.a.O., § 22 AGG Rn. 6; Erman/*Armbrüster*, a.a.O.

§ 22 AGG senkt das Beweismaß dahin ab, dass der klagenden Partei nur obliegt zu erreichen, dass die Indizien, aus denen man in der Zusammenschau aufgrund allgemeiner Lebenserfahrung auf die überwiegende Wahrscheinlichkeit einer unzulässigen Benachteiligung schließen kann,[195] mit überwiegender Wahrscheinlichkeit zu vermuten sind.[196]

Die Frage, was gemäß § 22 AGG konkret von der klagenden Partei vorzutragen und zu beweisen ist, unterliegt gemäß § 286 Abs. 1 ZPO der Würdigung des Tatsachengerichts aufgrund seiner freien Überzeugung. Die dazu ersichtliche Kasuistik stammt aus dem Arbeitsrecht, wo das AGG eine ungleich höhere praktische Bedeutung hat als im Zivilrecht. Sie gibt für die Situation, dass die jeweils angegriffene Entscheidung algorithmenbasiert getroffen wurde, positiv nichts her.

Festgestellt werden kann allerdings, dass die vergleichende Darstellung von zwei Einzelfällen allein für ein schlüssiges Klagevorbringen nicht genügt,[197] weil sich daraus nicht ergibt, dass die Entscheidung aufgrund eines nach dem AGG unzulässig diskriminierenden Kriteriums gefallen wäre. Die von einer algorithmenbasierten Entscheidung unzulässig benachteiligte Person wird also – selbstverständlich, ohne „ins Blaue hinein" Behauptungen aufstellen zu dürfen[198] – Indizien, aus denen auf eine unzulässige Benachteiligung geschlossen werden kann, vortragen müssen, obwohl ihr die Entscheidungsstruktur des entscheidenden Algorithmus gar nicht bekannt ist.

F wird im Beispielsfall a) nur vortragen können, dass M anders als sie eine Zusage von B erhalten habe. Darüber hinaus kann sie darstellen, dass und warum sie meint, dass die Entscheidungsvoraussetzungen – abgesehen vom Geschlecht – bei ihr und M gleich bzw. hinreichend ähnlich seien. Das ist aber nicht mehr als die vergleichende Darstellung von zwei Einzelfällen. Nach dem Ausgeführten wird sie damit ihrer Darlegungslast auch nach dem erleichterten Maßstab von § 22 AGG nicht genügen.

Jedenfalls derzeit ist auch nicht davon auszugehen, dass sich die Darlegungsschwierigkeiten einer unzulässig durch eine algorithmenbasierte Entscheidung benachteiligten Person dadurch erübrigen, dass ihr die für den Prozessvortrag nötigen Informationen aufgrund des Datenschutzrechts zur Verfügung stünden oder von der benachteiligenden Person zur Verfügung zu stellen wären. Zwar sind, wie oben unter C. II. gezeigt, gemäß Art. 13 Abs. 2 Buchst. f DS-GVO dem Betroffenen einer automatisierten Entscheidungsfindung

---

[195] BAG, Urt. v. 24.4.2008 - 8 AZR 257/07, NJW 2008, 3658 Leitsatz 2.
[196] Vgl. MükoBGB/*Thüsing*, a.a.O., § 22 AGG Rn. 2; Palandt/*Grüneberg* a.a.O., § 22 AGG Rn. 2.
[197] BAG, Urt. v. 24.4.2008, a.a.O., Leitsatz 1.
[198] Palandt/*Grüneberg*, a.a.O., § 22 AGG Rn. 2.

„aussagekräftige Informationen“ unter anderem „über die involvierte Logik“ zu erteilen, ein entsprechender Auskunftsanspruch gegenüber dem Verantwortlichen ist in Art. 15 Abs. 1 Buchst. h DS-GVO normiert. Bislang ist aber noch unklar, was diese Informationspflicht genau umfasst. Zudem dürfte, wie unter D. II. gezeigt wird, die Prüfung von Algorithmen im Hinblick auf die Frage, ob ihren Selektionsmechanismen diskriminierende Auslesekriterien zugrunde liegen, eine regelmäßig unlösbare Aufgabe darstellen.

Die Darlegungsschwierigkeiten der unzulässig benachteiligten Person werden auch nicht geringer, wenn sich die Beklagtenseite – wie B im Beispielsfall a) – darauf zurückzieht, dass der Computer so nun einmal entschieden habe. Denn die Verweigerung einer Auskunft über die Kriterien, die für die angegriffene Entscheidung maßgebend waren, stellt für sich betrachtet noch kein Indiz im Sinne von § 22 AGG dar.[199] Davon ist nach der Rechtsprechung des EuGH zwar eine Ausnahme zu machen, wenn die Verweigerung die mit den Richtlinien, die dem AGG zugrunde liegen, verfolgten Ziele zu beeinträchtigen droht.[200] Diese Ausnahme setzt aber wiederum die Darstellung des Anspruchstellers voraus, dass und warum gerade die Verweigerung der Auskunft für sich betrachtet eine Benachteiligung begründet.[201] Abstrakt-generell lässt sich aber wohl nicht sagen, dass die Verweigerung der Auskunft über die Funktionsweise des Algorithmus eine Benachteiligung begründet, weil die angegriffene Entscheidung mit eben diesem Algorithmus getroffen wurde. Wäre dies richtig, müsste man konsequenterweise der Klägerseite im Falle einer durch einen Menschen getroffenen Entscheidung auch das Recht zubilligen, diesen Menschen im Prozess zum Zwecke der Ausforschung seiner Entscheidungsmotive zu befragen. Bei wertender Betrachtung wird man der Beklagtenseite ihren bloßen Verweis auf eine algorithmenbasierte Entscheidung auch nicht vorwerfen können, weil ihr damit vorgetragenes Nichtwissen die Voraussetzungen von § 138 Abs. 4 ZPO erfüllt und nicht unplausibel ist, insbesondere keinen Anhalt dafür liefert, dass es sich um das bewusste Verbergen einer unzulässig benachteiligenden Entscheidungsfindung handelte.

Letztlich sind die dargestellten Darlegungsschwierigkeiten für die benachteiligte Person auch keine besonderen in dem Sinne, dass sie wesentlich darauf beruhten, dass eine algorithmenbasierte Entscheidung vorliegt.

Dies zeigt sich durch einen Vergleich der Beispielsfälle. In Fall b) wird F vor denselben Darlegungsschwierigkeiten stehen, obwohl dort der Mensch X und kein Algorithmus die diskriminierende Entscheidung getroffen hat. In beiden Fällen wird F auf weitere Informationen angewiesen sein, um in der Lage zu sein, ihrer Darlegungslast gemäß § 22 AGG nachzukommen – im Fall a) auf Informationen,

[199] BAG, Urt. v. 25.4.2013, a.a.O., 1705 Rn. 58.
[200] EuGH, Urt. v. 19.4.2012 - C-415/10, NJW 2012, 2497 Rn. 47.
[201] BAG, Urt. v. 25.4.2013, a.a.O., 1705 Rn. 59.

welche die frauendiskriminierende Funktionsweise des Algorithmus indizieren und im Fall b) auf solche, die die frauendiskriminierende Haltung von X indizieren.

Gäbe man F also in Fall a) einen Auskunftsanspruch oder würde – gleichbedeutend – die Erfüllung ihrer Darlegungslast mit der Begründung bejahen, dass B keine Auskunft über die algorithmenbasierte Entscheidung gegeben hat, würde man F im Beispielsfall a) besser stellen als im Beispielsfall b).

Als Ergebnis ist festzustellen, dass die von *Martini* vorgeschlagene Ergänzung des Katalogs der Anwendungsfälle des § 2 Abs. 1 AGG um eine Nr. 9 für Ungleichbehandlungen, die auf einer algorithmenbasierten Datenauswertung oder einem automatisierten Entscheidungsverfahren beruhen, nicht angezeigt ist. Zum einen entspräche sie nicht der Systematik des AGG, zum anderen erfasst das AGG Ungleichbehandlungen durch algorithmenbasierte Entscheidungen bereits de lege lata. Bei algorithmenbasierten Entscheidungen kann aber eine Exkulpation des Anspruchsgegners gemäß § 21 Abs. 2 S. 2 AGG leichter möglich sein als bei menschlichen Entscheidungen. Im Übrigen beschränken sich die Besonderheiten bei der rechtlichen Prüfung von algorithmisch geprägten Benachteiligungen auf Fragen der Beweisführung. So wird im Rahmen einer Beweisaufnahme ein anderes tatsächliches Geschehen aufzuklären sein, so dass andere Beweismittel im Vordergrund stehen. Steht die unzulässige Benachteiligung durch eine – im technischen, nicht rechtlichen Sinne – menschliche Entscheidung in Rede, könnte mit Urkunden oder Zeugen zu einer entsprechenden Entscheidungspraxis geklärt werden, ob eine Benachteiligung vorliegt. Hat dagegen der Mensch die Entscheidung einem algorithmisch geprägten Prozess überlassen, würde dessen Überprüfung ganz anders aussehen müssen. Die in den Algorithmus „eingebauten“ Kriterien und ihr jeweiliger Einfluss auf sein Ergebnis müssten sachverständig herausgefunden werden.[202] Eine Schlechterstellung der benachteiligten Person ergibt sich daraus aber wohl nicht.

IV. Kartellrecht

Der rechtliche Rahmen von Big Data-Anwendungen wird auch durch das Kartellrecht bestimmt, was im Rahmen dieses Berichts jedoch lediglich angerissen werden soll. Während die Digitalisierung vielfach zu einer sehr dynamischen Entwicklung von Märkten und Wettbewerb geführt hat, ist gleichzeitig festzustellen, dass sich einige marktmächtige Unternehmen

[202] Zu den Möglichkeiten der Überprüfung algorithmischer Entscheidungssysteme, s. Kapitel 1, D II.

herauskristallisiert haben.[203] Von Relevanz können daher im Rahmen von Big Data-Anwendungen insbesondere Normen gegen das missbräuchliche Ausnutzen von Marktmacht sein. In der 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen wurde klargestellt, dass die unentgeltliche Erbringung der Leistung der Annahme eines Marktes nicht entgegensteht.[204] Damit unterliegen Internetdienstleister wie Facebook oder Google der Missbrauchsaufsicht. Die Erhebung und sonstige Verarbeitung von Daten ist in der Internetökonomie ein in hohem Maße wettbewerbsrelevantes unternehmerisches Verhalten, das der Gesetzgeber in § 18 Abs. 3 GWB mit der 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen ausdrücklich als marktmachtrelevant, vor allem bei Onlineplattformen und –netz-werken, eingestuft hat. Zurzeit führt das Bundeskartellamt beispielsweise ein Verwaltungsverfahren gegen Facebook durch, in dem es einen möglichen Konditionenmissbrauch prüft. Dabei geht das Bundeskartellamt davon aus, dass es sich bei Facebook um ein marktbeherrschendes Unternehmen auf dem deutschen Markt für soziale Netzwerke handelt. Es prüft, ob die Vertragskonditionen von Facebook dem Verbraucher gegenüber unangemessen sind und zu einem Kontrollverlust für den Nutzer führen, der unter Umständen nicht mehr überschauen kann, welche Daten aus welchen Quellen für welche Zwecke zu einem detaillierten Profil zusammengeführt werden.[205]

D. Abstrakte Betrachtung der rechtspolitischen Handlungsoptionen

I. Erkenntnisse aus anderen Rechtsgebieten: Finanzmarktrecht

Bei der Untersuchung, welche rechtspolitischen Handlungsoptionen dem Gesetzgeber ganz grundsätzlich zur Verfügung stehen, um algorithmischen Entscheidungssystemen mit einem besonderen Potenzial für Diskriminierung oder Teilhabeausschluss zu begegnen, liegt es nahe, nach bereits bestehenden Regulierungen zu suchen.

Der erste Bereich, in dem die Notwendigkeit einer Regulierung von Algorithmen gesehen wurde, war der Börsenhandel.

---

[203] Wambach, Wettbewerbsregeln an die Digitalökonomie anpassen, ifo Schnelldienst 10/2018, 24. Mai 2018, S. 6 ff., https://www.cesifo-group.de/DocDL/sd-2018-10-2018-05-24.pdf (letzter Abruf: 25.8.2018).
[204] § 18 Abs. 2 GWB.
[205] Bundeskartellamt, Hintergrundinformationen zum Facebook-Verfahren des Bundeskartellamtes vom 19. Dezember 2017, abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/Hintergrundpapier_Facebook.html (letzter Abruf: 25.8.2018).

Bereits der enorme Kursrutsch am Schwarzen Montag, den 19. Oktober 1987, soll durch einen seinerzeit beliebten Programmhandel verschlimmert worden sein.[206] Auch beim so genannten „Flash Crash“ am 6. Mai 2010, bei dem völlig unvorhersehbar wesentliche Aktien-Indizes an der Wall Street einbrachen, um sich sodann ähnlich schnell zu erholen, haben Algorithmen jedenfalls verstärkend mitgewirkt. Damals verlor der Börsenindex Dow Jones kurzzeitig rund 1000 Punkte und damit etwa zehn Prozent. Dabei gingen fast eine Milliarde Dollar an Marktkapitalisierung verloren.[207] Dieses Jahr wirkten Algorithmen bei den Kurseinbrüchen am 2. Februar 2018 als Brandbeschleuniger.[208]

Im Vorgriff auf die Richtlinie (EU) 2014/65 (Market in Financial Instruments Directive II – im Folgenden „MiFID II“) wurde im Jahr 2013 das Gesetz zur Vermeidung von Gefahren und Missbräuchen im Hochfrequenzhandel verabschiedet.[209] Die Intention des Gesetzgebers richtete sich auf die Minimierung von Risiken für das Handelssystem aufgrund des Einsatzes algorithmischer Handelsprogramme. Der Einsatz dieser Programme ermöglicht es, Kauf – und Verkaufssignale in sehr kurzen Abständen von teilweise nur einigen Sekundenbruchteilen zu generieren und die Finanzinstrumente lediglich für sehr kurze Zeiträume zu halten. Damit erhöht sich die Geschwindigkeit und Komplexität des Handels, was die Gefahr der Überlastung des Handelssystems aufgrund übermäßiger Nutzung durch ein sehr hohes Orderaufkommen in sich birgt. Daneben besteht das Risiko, dass algorithmische Handelsstrategien auf andere Marktereignisse überreagieren, was die Volatilität verschärfen kann.[210]
In dem am 7. Mai 2013 verabschiedeten Gesetz[211] wurde zur Lösung des Problems der An- und Verkauf von Finanzinstrumenten an organisierten Märkten und multilateralen Handelssystemen als Wertpapierdienstleistung in der Form des Eigenhandels eingestuft. Aufgrund der Einstufung unterfielen ab diesem Zeitpunkt die an diesen Handelsplätzen aktiven Unternehmen grundsätzlich der Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht (im Folgenden: BaFin) nach dem Wertpapierhandelsgesetz. Den Unternehmen, die algorithmischen Handel betreiben, wurden besondere Organisationspflichten

[206] Handelsblatt vom 19.10.2012; Crash von 1987: Die Mutter aller Börsenpannen, abrufbar unter: http://www.handelsblatt.com/finanzen/maerkte/boerse-inside/crash-von-1987-die-mutter-aller-boersenpannen/7275944.html (letzter Abruf 25.8.2018).
[207] Handelsblatt vom 10.11.2016, „Flash-Crash“ – Händler bekennt sich schuldig, abrufbar unter: http://www.handelsblatt.com/panorama/aus-aller-welt/sechseinhalb-jahre-spaeter-flash-crash-haendler-bekennt-sich-schuldig/14822430.html (letzter Abruf: 25.8.2018); Bericht der US Commodity Futures Trading Commission und der US Securities & Exchange Commission vom 30. September 2010, abrufbar unter: https://www.sec.gov/news/studies/2010/marketevents-report.pdf. (letzter Abruf: 25.8.2018).
[208] Wirtschaftswoche vom 6.2.2018: Börsen-Crash oder Korrektur, abrufbar unter https://www.wiwo.de/finanzen/boerse/anleger-sind-in-panik-verfallen-boersen-crash-oder-korrektur/20931348.html (letzter Abruf: 15.8.2018).
[209] BGBl. 2013 S. 1162.
[210] BR-Drs. 607/12.
[211] BGBl. 2013 S. 1162.

auferlegt, nach denen sichergestellt werden muss, dass die Handelssysteme derart ausgestaltet sind, dass Störungen des Marktes unterbleiben.

Darüber hinaus gelten für Wertpapierdienstleistungsunternehmen ab dem 3. Januar 2018 neue Anzeigepflichten aufgrund der Umsetzung der Finanzmarktrichtlinie MiFID II durch das Zweite Finanzmarktnovellierungsgesetz. Wertpapierdienstleistungen sind von diesen Anzeigepflichten betroffen, wenn sie einen algorithmischen Handel im Sinne des § 80 Abs. 2 S. 1 des Wertpapierhandelsgesetzes (WpHG) betreiben, oder wenn sie gemäß § 2 Abs. 30 WpHG einen direkten elektronischen Zugang zu einem Handelsplatz anbieten.

In § 80 Abs. 2 WpHG heißt es:

„(2) Ein Wertpapierdienstleistungsunternehmen muss zusätzlich die in diesem Absatz genannten Bestimmungen einhalten, wenn es in der Weise Handel mit Finanzinstrumenten betreibt, dass ein Computeralgorithmus die einzelnen Auftragsparameter automatisch bestimmt, ohne dass 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). Auftragsparameter im Sinne des Satzes 1 sind insbesondere Entscheidungen, ob der Auftrag eingeleitet werden soll, über Zeitpunkt, Preis oder Quantität des Auftrags oder wie der Auftrag nach seiner Einreichung mit eingeschränkter oder überhaupt keiner menschlichen Beteiligung bearbeitet wird. Ein Wertpapierdienstleistungsunternehmen, das algorithmischen Handel betreibt, muss über Systeme und Risikokontrollen verfügen, die sicherstellen, dass

1. *seine Handelssysteme belastbar sind, über ausreichende Kapazitäten verfügen und angemessenen Handelsschwellen und Handelsobergrenzen unterliegen;*

2. *die Übermittlung von fehlerhaften Aufträgen oder eine Funktionsweise des Systems vermieden wird, durch die Störungen auf dem Markt verursacht oder ein Beitrag zu diesen geleistet werden könnten;*

3. *seine Handelssysteme nicht für einen Zweck verwendet werden können, der gegen die europäischen und nationalen Vorschriften gegen Marktmissbrauch oder die Vorschriften des Handelsplatzes verstößt, mit dem es verbunden ist.*

Ein Wertpapierdienstleistungsunternehmen, das algorithmischen Handel betreibt, muss ferner über wirksame Notfallvorkehrungen verfügen, um mit unvorhergesehenen Störungen in seinen Handelssystemen umzugehen, und sicherstellen, dass seine Systeme vollständig geprüft sind und ordnungsgemäß

überwacht werden. Das Wertpapierdienstleistungsunternehmen zeigt der Bundesanstalt und den zuständigen Behörden des Handelsplatzes, dessen Mitglied oder Teilnehmer es ist, an, dass es algorithmischen Handel betreibt."

Ferner wurde den Händlern aufgegeben, die verwendeten Handelsalgorithmen intern zu kennzeichnen, um eine Rückverfolgung zu ermöglichen, § 16 Abs. 2 Nr. 3 des Börsengesetzes.

Zudem wurde ein Auskunftsrecht der BaFin eingeführt, dass sich nunmehr in § 6 Abs. 4 WpHG wiederfindet. Danach kann die BaFin von einem Wertpapierdienstleistungsunternehmen, das algorithmischen Handel betreibt, jederzeit Informationen über seinen algorithmischen Handel und die für diesen Handel eingesetzten Systeme anfordern, soweit dies aufgrund von Anhaltspunkten für die Überwachung der Einhaltung eines Verbot oder Gebots des Wertpapierhandelsgesetzes erforderlich ist. Die BaFin kann insbesondere eine Beschreibung der algorithmischen Handelsstrategien, der Einzelheiten zu den Handelsparametern oder Handelsobergrenzen, denen das System unterliegt, der wichtigsten Verfahren zur Überprüfung der Risiken und Einhaltung der Vorgaben des § 80 WpHG sowie der Einzelheiten über seine Systemprüfung verlangen.

Die Umsetzung der Organisationspflichten wird nach § 89 WpHG von Wirtschaftsprüfern überprüft. Dabei findet keine Überprüfung einzelner Algorithmen statt.

Forderungen, ein spezielles Zulassungsverfahren für Algorithmen im Bereich des Hochfrequenzhandels zu etablieren, konnten sich nicht durchsetzen. Konkret gefordert wurde ein Zulassungsverfahren für Algorithmen, in dem die algorithmischen Handelssysteme vor der Nutzung im Markt einem Stresstest unterzogen werden,[212] was jedoch keine Mehrheit fand. Auch auf europäischer Ebene wurde von einem Zulassungsverfahren für Handelsalgorithmen in der Finanzmarktrichtlinie MiFID II abgesehen.

Der Weg, der im Börsenhandel gewählt wurde, um Risiken algorithmenbasierter Entscheidungsfindung zu minimieren, lässt sich nur bedingt auf den hier zu untersuchenden Einsatz von Algorithmen in zivilrechtlichen Vertragsbeziehungen übertragen. Eine Übertragung der Grundsätze könnte dort erwogen werden, wo zulassungspflichtige Märkte bestehen, wie etwa im Bereich der Krankenversicherungen. Erkenntnisse können ferner insoweit gewonnen werden, als die gesetzliche Beschreibung der algorithmischen Handlungsformen geeignet erscheint, die Realität abzubilden. Zudem zeigt sich in diesem Bereich, dass eine Kennzeichnung von Algorithmen grundsätzlich möglich ist.

---

[212] Vgl. Plenarprotokoll des Deutschen Bundestages, 17/212, 1. Beratung, Redebeitrag des Abgeordneten Dr. Carsten Siegling, 26013 A.

II. Untersuchung rechtspolitischer Handlungsoptionen

Die Diskussion um eine Beschränkung algorithmenbasierter Big Data-Anwendungen hat eine Vielzahl von Vorschlägen hervorgebracht, welche die volle Bandbreite des „Baukastens" legislativer Gestaltungsmittel ausschöpfen. Instrumente direkter Verhaltenssteuerung lassen sich dabei von Instrumenten indirekter Verhaltenssteuerung unterschieden. Direkte Verhaltenssteuerung wird durch Gesetze bewirkt, die Ge- oder Verbote aussprechen, Genehmigungsvorbehalte, Anzeigepflichten und Anmeldevorbehalte oder Nebenbestimmungen und Verträglichkeitsprüfungen vorsehen. Mit dem Einsatz eines Genehmigungsvorbehalts sind in aller Regel, je nach Ausgestaltung, schwerwiegendere Eingriffe in die unternehmerischen Freiheiten verbunden, die einen entsprechend gewichtigen Gemeinwohlbelang zur Rechtfertigung verlangen. So macht beispielsweise eine präventive Genehmigungspflicht hinsichtlich eines Algorithmus nur Sinn, wenn und soweit entsprechende Risiken des Einsatzes des betreffenden Algorithmus für die Grundrechtsausübung den enormen Aufwand, der mit der Durchführung von Genehmigungs- und womöglich Änderungsgenehmigungsverfahren verbunden ist, rechtfertigen können. Ein bloßer Anmeldevorbehalt mit stichprobenartiger Kontrolle ist hingegen ein milderes Mittel, bietet aber auch weniger Schutz vor Rechtsverstößen. Instrumente indirekter Verhaltenssteuerung sind beispielsweise Transparenzpflichten und damit korrespondierende (private) Rechte, Formen regulierter Selbstregulierung wie Zertifikatslösungen, Organisationsvorgaben an Unternehmen, Versicherungspflichten, Auskunftsansprüche und unterschiedliche Haftungsregime. Das gewünschte Verhalten soll hier mittelbar dadurch erreicht werden, dass Unternehmen sich aus wirtschaftlichen Gründen für die Einhaltung bestimmter Standards gegen besonders risikoträchtige Verhaltensweisen entscheiden.

1. Beispiele zu einzelnen Instrumenten

Das gesetzliche Ver- oder Gebot ist die schärfste Form der direkten Verhaltenssteuerung, da es bestimmte Verhaltensweisen zwingend verbietet oder anordnet, um staatliche Steuerungsziele zu erreichen. Verbote kommen in Betracht, wenn das verbotene Verhalten generell unerwünscht ist, etwa, weil es sich regelhaft in erheblicher Weise gesundheitsschädigend auswirkt, und auch nicht besonders grundrechtlich geschützt ist. Neben dem absoluten Verbot kommt ein repressives Verbot mit Befreiungsvorbehalt in Betracht, um besonderen Umständen des Einzelfalls Rechnung zu tragen.[213] Dieses Instrument wird bei grundsätzlich unerwünschtem Verhalten, das nur ausnahmsweise gestattet werden

[213] *Sparwasser/Engel/Voßkuhle*, Umweltrecht, S. 85.

kann, eingesetzt. Die Erteilung der Befreiung liegt meistens im Ermessen der Behörde. Die Einhaltung der Ver- oder Gebote wird staatlich kontrolliert.[214]

Im Kontext der Algorithmen dürften Verbote zu rechtfertigen sein, wenn ihr Einsatz die freie Entfaltung der Persönlichkeit anderer Menschen bedroht, weil die von ihnen getroffenen Entscheidungen oder ihre mittelbaren Auswirkungen den betroffenen Menschen die Möglichkeit nehmen, ein selbstbestimmtes Leben zu führen oder weil ein anderer als ein diskriminierender Einsatz nicht denkbar ist. Denkbar ist dies in existenziellen Lebensbereichen wie etwa dem diskriminierungsfreien Zugang zu grundlegenden sozialen Sicherungssystemen oder bei Entscheidungen in lebensbedrohlichen medizinischen Situationen.

Auf einer schwächeren Stufe sind gesetzliche Eröffnungskontrollen anzusiedeln, wie Genehmigungsvorbehalte, Anzeigepflichten und Anmeldevorbehalte. Genehmigungsvorbehalte sind in der Regel als präventives Verbot mit Erlaubnisvorbehalt ausgestaltet. Dabei wird ein grundsätzlich erwünschtes, oft grundrechtlich geschütztes Verhalten, zu Kontrollzwecken einem Erlaubnisvorbehalt unterworfen. Bei Vorliegen der Voraussetzungen besteht ein Anspruch auf Erteilung der Erlaubnis. Der Antragsteller trägt die Darlegungs- und Beweislast und kann etwaige Vorhaben bis zum Erlass eines positiven Bescheids nicht umsetzen. Genehmigungsvorbehalte wirken sich je nach Ausgestaltung der Anforderungen oder des Verfahrens freiheitshemmend aus; auf unternehmerischer Seite lösen sie einen Erfüllungsaufwand aus, auf staatlicher Seite müssen entsprechende fachliche Ressourcen zur Überprüfung der Anträge bereitgestellt werden. Ein Einsatz ist regelmäßig gerechtfertigt, wenn der Schutz wichtiger Rechtsgüter derartige „Kontrollerlaubnisse“ verlangt.
Ein besonders bekanntes Beispiel in diesem Zusammenhang ist der KfZ-TÜV, präziser, die nach § 29 StVZO vorgesehene Hauptuntersuchung. Diese wird auf Grundlage staatlicher Gesetze auf privatwirtschaftlicher Basis als mittelbare Staatsverwaltung in Form der Beleihung des Technischen Überwachungsvereins durchgeführt.

Der Bundesverband Verbraucherzentrale erhob die Forderung, auch Algorithmen einem so genannten „Algorithmen-TÜV“ zu unterwerfen. Algorithmen, deren Einsatz zwar nicht regelhaft schädlich für die betroffenen Personen ist, deren Fehlerhaftigkeit oder ihr missbräuchlicher Einsatz aber mit erheblichen Gefahren verbunden ist, könnten aufgrund derartiger Regelungen überwacht werden.

Dies wirft die Frage auf, wie überhaupt ein algorithmisches Entscheidungssystem überprüft werden kann. Dabei mag man zunächst an die Prüfung des offengelegten Quellcodes denken, wobei bereits der Prüfungsmaßstab fraglich sein dürfte. Für Algorithmen in den unterschiedlichsten Anwendungsbereichen gibt es bisher keine Standards, an denen sich ein Prüfer orientieren könnte. Die

[214] *Schulz/Held*, Regulierte Selbstregulierung als Form modernen Regierens, S. A-3.

nächste Problematik dürfte die Prüffähigkeit der Algorithmen an sich und der damit verbundene Aufwand sein. Außer im akademischen Bereich dürfte es unüblich sein, dem Quellcode detaillierte Beschreibungen beizufügen, die den Nachweis bringen, dass der Algorithmus die gestellte Aufgabe löst. Der Wunsch, algorithmische Entscheidungssysteme daraufhin zu überprüfen, diskriminierungsfreie Ergebnisse zu liefern, dürfte regelmäßig eine unlösbare Aufgabe darstellen. Dies gilt erst recht, wenn der Algorithmus aus zur Verfügung gestellten Datenpaketen selbst lernt. Ferner unterliegen algorithmische Entscheidungssysteme häufig einer ständigen Veränderung durch deren Entwickler, weswegen es einer Vielzahl von Informatikern bedürfte, alle diese Entwicklungen nachzuvollziehen. Schließlich kollidiert die Offenlegung des Quellcodes mit dem Schutz von Geschäftsgeheimnissen.

Eine Alternative zur Offenlegung des Quellcodes könnte die Analyse der Ergebnisse bringen, die algorithmische Entscheidungssysteme auswerfen. Hierzu müssten die jeweiligen Unternehmen Schnittstellen zur Verfügung stellen, die es dem Prüfer ermöglichten, dem algorithmischen Entscheidungssystem Testdatensätzen einzuspielen. Bei diesen Testdatensätzen könnte man je nach konkretem Anwendungsbereich einzelne Parameter variieren und die Ergebnisse sodann auf Anhaltspunkte für Diskriminierungen (gegebenenfalls unter Zuhilfenahme von eigenen Prüfalgorithmen) untersuchen. Diese Szenario wäre grundsätzlich denkbar, fordert jedoch besonders qualifiziertes Personal[215] und regelmäßig einen hohen zeitichen Aufwand. Zudem wird die hierzu nötige gesetzliche Verpflichtung der Unternehmen, Schnittstellen zur Verfügung zu stellen, lediglich in ganz besonders grundrechtsrelevanten Bereichen mit einem hohen Gefährdungspotenzial für bedeutsame Rechtsgüter verhältnismäßig sein. In diesem Zusammenhang wäre möglicherweise an autonome Mobilitätssysteme zu denken. Passend hierzu hat der TÜV Süd angekündigt, mit dem Deutschen Forschungszentrum für künstliche Intelligenz zusammenzuarbeiten, um einen TÜV für Algorithmen zu entwickeln und so Systeme zu zertifizieren, die beim autonomen Fahren im Einsatz sind.[216]

Ein deutlich milderes Mittel sind Anzeigepflichten, durch die die Behörden auf die Aufnahme oder Änderung der Tätigkeit aufmerksam gemacht werden sollen, damit diese überwacht werden kann.[217] Anmeldepflichten kommen beispielsweise dort in Betracht, wo auch ein fehlerhafter oder missbräuchlicher Freiheitsgebrauch wie etwa der Algorithmeneinsatz nicht zu schwerwiegenden Folgen für andere führen kann, so dass stichprobenartige Kontrollen ausreichen.

---

[215] Der Bundesverband Bitkom zählte zum Jahreswechsel 2017/2018 in Deutschland rund 55.000 offene Stellen für IT-Fachkräfte, vgl. Handelblatt vom 17./18./19. August 2018, S. 43.
[216] „Ein TÜV für Algorithmen“, Süddeutsche Zeitung vom 18.4.2018/ ratz.
[217] *Sparwasser/Engel/Voßkuhle*, Umweltrecht, S. 90.

Anmeldevorbehalte beinhalten freilich die Pflicht zur Vorlage relevanter Unterlagen, die ähnliche Belastungen mit sich bringen kann wie ein Genehmigungsvorbehalt, der zudem nach Erteilung der Genehmigung auch Rechtssicherheit für einen Antragsteller schafft.

Verträglichkeitsprüfungen werden beispielsweise vielfach im Umweltrecht durchgeführt. Als Beispiel kann hierfür die natura 2000-Verträglichkeitsprüfung nach § 34 des Bundesnaturschutzgesetzes genannt werden. Zweck der Verträglichkeitsprüfung ist in der Regel die formalisierte fachliche Prüfung, ob Vorhaben bestimmte Rechtsgüter erheblich beeinträchtigen. Sie sind also insbesondere in Bereichen nutzbar, in denen Unsicherheit über Auswirkungen besteht. Denkbar ist es auch, Verträglichkeitsprüfungen denjenigen zu übertragen, die den späteren Nutzen eines Vorhabens genießen; dies schont die staatlichen Ressourcen und sorgt für eine nachfragegerechte Bereitstellung der Prüfungsdienstleistung mit der Folge zügiger Verfahren.
Auch im europäischen Datenschutzrecht hat dieses Instrument mit der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO seinen Niederschlag gefunden.

Transparenzpflichten sollen unter anderem Behörden oder Personen in die Lage versetzen, informierte Entscheidungen zu treffen oder Rechtsverletzungen zu erkennen, vgl. z.B. Art. 7 Abs. 2 DS-GVO. Transparenzpflichten sensibilisieren zwar im Hinblick auf bestimmte Verhaltensweisen, hindern aber nicht deren Ausübung. Ihre Wirksamkeit hängt zum Beispiel davon ab, wie stark sich Verbraucher für die angegebenen Informationen interessieren und ob sie bereit sind, daraus Verhaltensrückschlüsse zu ziehen. Auch Transparenzpflichten können einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb darstellen, wenn mit ihnen die Offenlegung von Geschäftsgeheimnissen verbunden ist. Dennoch sind sie regelmäßig ein milderes Mittel gegenüber Ge- oder Verboten und Genehmigungspflichten. Sie kommen vor allem dann in Betracht, wenn die Information geeignet ist, den Adressaten in die Lage zu versetzen, eine freie Entscheidung über die Nutzung einer Dienstleistung zu treffen. Bleibt dem Adressaten auch nach der Lektüre keine andere Wahl, als die Bedingungen zu akzeptieren, sind unter Umständen materiell-rechtliche Pflichten zur Hebung des Schutzniveaus erforderlich. Flankieren lassen sich Transparenzpflichten mit Sanktionsregimen wie Ordnungswidrigkeiten oder Schadensersatzpflichten.

Auch die Implementierung von Haftungsregimen stellt ein Gestaltungsmittel dar, um gesetzgeberische Ziele zu erreichen. Die Aussicht, für durch Fehlverhalten verursachte Schäden aufzukommen, provoziert sorgfältigeres Verhalten. Haftungsregime bieten sich an, wenn der drohende Schaden durch die Haftung kompensiert werden kann; ist der drohende Schaden bei seinem Eintritt irreparabel, sind sie nur in Kombination mit anderen Instrumenten sinnvoll

nutzbar. Mit Blick auf Algorithmen könnten sie geeignet sein, um Diskriminierungen entgegenzuwirken.

Pflichtversicherungen, etwa in § 1 des Pflichtversicherungsgesetzes für Fahrzeughalter oder in § 51 der Bundesrechtsanwaltsordnung für Rechtsanwälte hindern nicht den Schadenseintritt, sollen aber eine nachträgliche Entschädigung des Geschädigten sicherstellen.

Unter regulierter Selbstregulierung ist eine Selbstregulierung zu verstehen, die in einen staatlichen Rahmen eingepasst ist bzw. auf rechtlicher Grundlage erfolgt.[218] Regulierte Selbstregulierung findet sich beispielsweise im Jugendmedienschutz (Jugendmedienschutz-Staatsvertrag), im Umweltrecht (Umweltaudit) und im Bilanzkontrollrecht (§§ 342b ff HGB, §§ 37 Buchst. n ff. WpHG) sowie neuerdings in § 3 Abs. 2 Nr. 3 des Netzwerkdurchsetzungsgesetzes. Private Organisationen können sich auch selbst Regeln setzen und deren Einhaltung kontrollieren. Alternativ können private Organisationen auch darauf beschränkt sein, staatlich gesetzte Normen zu kontrollieren. Ob eine regulierte Selbstregulierung möglich ist, hängt verfassungsrechtlich betrachtet von der Grundrechtsrelevanz der Materie ab. Je geringer die Gefahren für geschützte Rechtsgüter, desto eher kann die Erreichung von Steuerungszielen Privaten überlassen werden. Das bietet sich insbesondere dann an, wenn die Bereitstellung staatlicher Ressourcen aufgrund der Spezifika eines Sachverhalts flächendeckend schwierig ist und, wenn ein Eigeninteresse der regulierten Bereiche erkennbar ist; so kann es im Interesse des Verwenders eines Algorithmus sein, mit dessen Treffsicherheit oder dem Datensicherheitsniveau zu werben. Ist die Materie so komplex, dass der Verbraucher sich kaum sinnvoll mit deren Details auseinandersetzen kann, können Zertifikate anerkannter Zertifizierer einen Werbeeffekt bewirken. Missbrauch kann dadurch vorgebeugt werden, dass die Zertifizierer ihrerseits strengen Regeln und einem Sanktionsregime unterworfen werden.

Im Bereich der regulierten Selbstregulierung spielen Zertifikate, mit denen beispielsweise ein bestimmter Qualitätsstandard oder die Einhaltung einer DIN bescheinigt wird, eine bedeutende Rolle. Auch die verschiedenen technischen Überwachungsvereine (TÜV) sind in dem Bereich der Zertifizierung tätig.

Letztlich lassen sich alle Instrumente je nach Anforderungsprofil und gewünschter Wirkung miteinander kombinieren. Maßgeblich sind die klassischen Kriterien des Verhältnismäßigkeitsgrundsatzes. Gefahren und Risiken des in Rede stehenden Algorithmus für den Einzelnen, gemessen an den spezifisch einschlägigen Grundrechten und des Ausmaßes von deren Beeinträchtigung, Allgemeinwohlbelange wie Kosten wirksamer staatlicher Überwachung, Wirksamkeit des gewählten Instruments oder Instrumentenmixes.

[218] *Schulz/Held*, Regulierte Selbstregulierung als Form modernen Regierens, S. A-5.

2. Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung hält bereits ein umfangreiches Instrumentarium bereit. Als Verordnung, die nicht nur den Schutz personenbezogener Daten regelt, sondern auch Rechtsgrundlage für den freien Verkehr dieser Daten sein will (Art. 1 Abs. 1 DS-GVO), ist sie abschließend, wenn und soweit sie einschlägig ist (insbesondere personenbezogene Daten verarbeitet werden) und keine Öffnungsklauseln einen höheren Schutz personenbezogener Daten und damit auch vor algorithmenbasierter Verarbeitung gestatten. In vielerlei Hinsicht sind die Tatbestände der Datenschutz-Grundverordnung bisher noch konkretisierungsbedürftig. Generell sollten daher erste Entwicklungen in der Rechtsprechung abgewartet werden. Anders könnte dies in Regelungsbereichen sein, in denen das Recht auf informationelle Selbstbestimmung besonders sensibel berührt ist. Die Datenschutz-Grundverordnung ist eine „Grund"-Verordnung. Sie bietet einen Daten-„Grundschutz", der für bestimmte Daten durch speziellere unionsrechtliche Regelungen ausgeweitet (oder eingeschränkt) wird. Erkennbar ist aber schon jetzt, dass die Datenschutz-Grundverordnung einen Schutz der freien Entfaltung der Persönlichkeit nur bietet, soweit diese durch die Verarbeitung personenbezogener Daten bedroht ist. Der Rasterung anhand nichtpersonenbezogener Daten wie beispielsweise bestimmter, weit verbreiteter, aber doch aussagekräftiger Maschinendaten, gebietet sie keinen Einhalt.

3. Ergänzung des Allgemeinen Gleichbehandlungsgesetzes

Um die bereits vorhandenen legislativen Möglichkeiten zur Regulierung von algorithmischen Entscheidungssystemen optimal nutzen zu können, böte sich eine geringfügige Ergänzung des Allgemeinen Gleichbehandlungsgesetzes an. Wie oben unter Kapitel I C. III. gezeigt, erfasst der Schutz des AGG vor unzulässiger Benachteiligung im Zivilrecht auch algorithmenbasierte Entscheidungen, ohne hinter dem Niveau des Schutzes vor menschlich getroffenen Entscheidungen zurückzubleiben. Unsicherheit besteht aber hinsichtlich des Schadensersatzanspruchs aus § 21 Abs. 2 S. 2 AGG. Für Rechtssicherheit sorgen würde hier die Entscheidung des Gesetzgebers dahingehend, dass der Entlastungsbeweis nach § 21 Abs. 2 S. 1 AGG ausscheidet, wenn die Verletzung des Benachteiligungsverbots auf einer algorithmenbasierten Entscheidung beruht. Die Konformität einer solchen Änderung des AGG zu den Richtlinien wäre unproblematisch, weil diese nur Mindestanforderungen stellen.

E. Konkrete Betrachtung rechtspolitischer Handlungsoptionen für personalisierte Newsfeeds, personalisierte Werbung und personalisierte Preise

Gemäß dem Arbeitsauftrag sollen nunmehr die eingangs dargestellten Fallkonstellationen algorithmenbasierter Big Data-Anwendungen untersucht werden.

I. Personalisierte Newsfeeds

1. Chancen algorithmenbasierter personalisierter Suchfunktionen und „Newsfeeds“ in digitalen Plattformen

Personalisierte Suchfunktionen und Newsfeeds können Nutzern - natürlich in Abhängigkeit von der Qualität des verwendeten Algorithmus und der ihm zur Verfügung stehenden Nutzerdaten - einen komfortablen Zugang zu Informationen, die ihren Interessen und ihrem Informationsbedarf entsprechen, ermöglichen.[219] Gerade bei Internetsuchmaschinen kann die Personalisierung der Suchergebnisse dazu beitragen, die Recherche stärker an dem persönlichen Nutzerinteresse auszurichten und damit in zeitsparender Weise die Qualität der Rechercheergebnisse aus Nutzersicht zu verbessern. Damit wird die zeiteffiziente und kostengünstige Verfügbarkeit für den Nutzer relevanter Informationen aus einer aus menschlicher Sicht unüberschaubaren Datenmenge erheblich erleichtert. Dies kommt mangels Entgeltlichkeit der personalisierten Suchangebote weiten Teilen der Bevölkerung zugute („Demokratisierung“).[220] Bei Newsfeeds kann eine stärkere Personalisierung die Nützlichkeit einer digitalen Plattform für den Nutzer erhöhen, da ihm – wie es z.B. bei einer Sortierung der sogenannten „Timeline“ nach Maßgabe der chronologischen Reihenfolge der Veröffentlichung der Fall wäre - anstelle einer ungefilterten großen Datenmenge mit zahlreichen potentiell für ihn persönlich nicht relevanten Informationen primär die Informationen angezeigt werden, die potentiell für ihn persönlich interessant und relevant sind. Sowohl bei Suchmaschinen als auch bei digitalen Plattformen mit Newsfeed-Funktion kann eine stärkere Personalisierung der Informationsangebote mittels Algorithmen dazu beitragen, dass die Nutzer über die sie interessierenden Themengebiete umfassender und qualitativ besser informiert werden.[221] Will der Nutzer mittels Suchmaschinen erzielte

[219] *Lischka/Klingel*, Neun Chancen, neun Risiken algorithmischer Entscheidungsfindung, abrufbar unter: https://algorithmenethik.de/2017/06/09/neun-chancen-neun-risiken-algorithmischer-entscheidungsfindung/ (letzter Abruf: 25.8.2018).
[220] *Lischka/Klingel*, Neun Chancen, neun Risiken algorithmischer Entscheidungsfindung, abrufbar unter: https://algorithmenethik.de/2017/06/09/neun-chancen-neun-risiken-algorithmischer-entscheidungsfindung/ (letzter Abruf: 25.8.2018).
[221] *Lischka/Stöcker*, Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier, *Gütersloh* 2017, S. 18, abrufbar unter: https://www.bertelsmann-

Rechercheergebnisse oder Informationen aus Newsfeeds zur Grundlage von Entscheidungen machen, so kann eine durch Personalisierung erhöhte persönliche Relevanz der dem Nutzer angezeigten Informationen eine breitere Informationsgrundlage für Entscheidungen des Nutzers zur Folge haben.[222]

2. Risiken algorithmenbasierter personalisierter Suchfunktionen und „Newsfeeds“ in digitalen Plattformen

Algorithmisch gesteuerte personalisierte Newsfeeds führen zur Informationseinblendung unter Relevanzgesichtspunkten, wobei sich die Relevanz – in der Gewichtung natürlich in Abhängigkeit vom jeweiligen Algorithmus – auch nach personenbezogenen Interessen oder Vorlieben und/oder der Interaktion „befreundeter“ Nutzer mit geposteten Beiträgen bemisst. Damit wird die Relevanz angezeigter Inhalte nicht nach deren tagespolitischer oder zeitgeschichtlicher Bedeutung oder sonstigen in der Presse geltenden qualitativen Kriterien bemessen, was zu einer großen Diskrepanz zwischen allgemeiner Nachrichtenlage und den Informationen im Newsfeed und damit tendenziell zu unvollständiger Information der Intermediärnutzer führen kann.[223] Das Ausmaß der durch Personalisierung von Newsfeeds potentiell herbeigeführten „Unterversorgung“ der Nutzer mit objektiv relevanten Informationen hängt dabei neben der Gewichtung der Personalisierung im jeweiligen Algorithmus und den persönlichen Interessen des Nutzers auch davon ab, ob und in welchem Ausmaß sich der betroffene Nutzer zusätzlich auch aus anderen Quellen (wie z.B. Tagespresse, Rundfunk etc.) informiert. Allerdings kann die andersartige Zusammensetzung personalisierter Newsfeeds oder Trefferlisten in Online-Suchmaschinen gegenüber der allgemeinen Rundfunk- und Presseberichterstattung bei Nutzern, die sich der Folgen der Personalisierung des digital-algorithmisch sortierten Informationsangebots nicht bewusst sind, auch zur Folge haben, dass das Misstrauen der Nutzer gegenüber der Objektivität der Rundfunk- und Presseberichterstattung wächst. Umgekehrt kann diese Diskrepanz bei Nutzern dazu führen, dass sie nicht zuletzt auch wegen des Gefühls, bei Internetmedien den Folgen als intransparent empfundener algorithmischer Vorsortierung ausgeliefert zu sein, die Nutzung des Internets zunehmend meiden oder einschränken.[224] Ferner kann mit der Personalisierung

---

stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digitale_Oeffentlichkeit_final.pdf (letzter Abruf: 25.8.2018).

[222] Vgl. *Ernst*, Algorithmische Entscheidungsfindung und personenbezogene Daten**,** JZ 2017, 1026 (1029).

[223] *Lischka/Stöcker*, Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier, Gütersloh 2017, S. 11, abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/Digitale_Oeffentlichkeit_final.pdf (letzter Abruf: 25.8.2018).

[224] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 73 f, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018).

von Newsfeeds und Rechercheergebnissen im Internet auch das Risiko sogenannter „Filterblasen-“ oder „Echokammereffekte“[225] verbunden sein. Damit ist die auf personalisierte Algorithmensortierung zurückgeführte Verengung der Nachrichtenlage und Meinungsvielfalt auf dem Weltbild und den Interessen des Nutzers entsprechende Beiträge und Informationen gemeint, die den Nutzer wiederum in seiner Auffassung bestärken.[226] Auch wenn zu diesem Effekt zunehmend kritische Stimmen zu vernehmen sind, die unter Bezugnahme auf vergleichbare milieubezogene Phänomene in der analogen Welt[227] oder auf empirische Untersuchungen zum Grad der Personalisierung der Informationsangebote bestimmter Intermediäre (wie z.B. die Internetsuchmaschine Google[228]) den Filterblaseneffekt verneinen oder relativieren, ist jedenfalls zu konstatieren, dass er eintreten könnte, wenn der seitens des genutzten Intermediärs verwendete Algorithmus hinreichend stark personalisiert ausgerichtet wird.

3. Stellungnahme

Die jederzeitige und ubiquitäre Verfügbarkeit unzähliger Nachrichten und sonstiger Informationen darf wohl als der wesentliche Fortschritt angesehen werden, den das Internet ermöglicht hat. Aber erst durch zahlenmäßige Begrenzung, mithin eine Vorauswahl wird die sonst unüberschaubare Menge von Netzinformationen für den Menschen handhabbar und damit sinnvoll. Die Notwendigkeit solcher Vorauswahl impliziert zum einen, dass dafür aus zeitlichen und ökonomischen Gründen Algorithmen eingesetzt werden, und zum anderen den Verlust von Objektivität. Eine algorithmische Vorauswahl ist – ebenso wenig wie eine menschliche es sein könnte – nicht objektiv, sondern wertet nach den implementierten Kriterien. Das Forschungsprojekt „#Datenspende: Google und die Bundestagswahl 2017“ hat für die dort untersuchten Fragen – aufgrund seines Setups mit freiwilliger Teilnahme von

---

[225] Grundlegend hierzu: *Pariser*, The filter bubble. What the internet is hiding from you, 2011.

[226] *Von Gehlen*, Welt ohne Gegenmeinung, abrufbar unter: http://www.sueddeutsche.de/digital/wie-google-und-co-uns-andere-standpunkte-vorenthalten-welt-ohne-gegenmeinung-1.1112983 (letzter Abruf: 25.8.2018); *Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen - Eine Herausforderung für das Recht, AöR 142 (2017), 1 (12 f).

[227] *Fischer*, Filterblase?, abrufbar unter: http://www.zeit.de/2017/34/algorithmen-filterblase-meinungen-selbstbetrug (letzter Abruf: 25.8.2018).

[228] *Weisberg*, Bubble trouble. Is Web personalization turning us into solipsistic twins?, abrufbar unter: http://www.slate.com/articles/news_and_politics/the_big_idea/2011/06/bubble_trouble.html (letzter Abruf: 25.8.2018); *Krafft/Gamer/Laessing/Zweig*, Filterblase geplatzt? Kaum Raum für Personalisierung bei Google-Suche zur Bundestagswahl 2017, abrufbar unter: https://algorithmwatch.org/wp-content/uploads/2017/09/1_Zwischenbericht__final.pdf (letzter Abruf: 25.8.2018).

Datenspendern allerdings nicht notwendigerweise repräsentativ – nur wenige Anzeichen für Personalisierung gefunden.[229] Das kann man unter dem Gesichtspunkt der Gleichbehandlung und des Schutzes vor „Filterblasen“ begrüßen, aber auch kritisch sehen. Denn wenn die Kriterien des Auswahlalgorithmus bei allen Nutzern zu denselben Ergebnissen führen, sie also mit anderen Worten nicht personalisiert sind, ist ihr Einfluss deshalb nicht gering. Er ist vielmehr insofern sehr groß, als nicht nur bei einigen oder vielen, sondern bei allen Nutzern dieselben Netzinformationen auf vordere Plätze der Auswahl und damit in den Fokus gerückt werden, während andere Informationen ebenfalls allen vorenthalten werden, weil sie es in der Auswahl nicht auf die vorderen, von den Nutzern wahrgenommenen Plätze schaffen. Daher ist die Personalierung von Suchmaschinenergebnissen und Newsfeeds durchaus zu begrüßen, jedenfalls nicht prinzipiell abzulehnen. Den damit verbundenen Risiken – Unterversorgung mit objektiv relevanten Nachrichten, objektiv unbegründetes Misstrauen gegenüber klassischen Medien, generelles Meiden der Internetnutzung – wäre aber nach Möglichkeit zu begegnen. Dabei liegt auf der Hand, dass sich gerade in dem hier betroffenen Schutzbereich von Art. 5 Abs. 1 GG staatliche Einflussnahme auf die in den Auswahlalgorithmen für die Personalisierung von Suchfunktionen und Newsfeeds implementierten Kriterien von vornherein verbietet. „Filterblasen“- und „Echokammereffekte“ mag man beklagen – rechtlich steht außer Frage, dass Ausfluss der Informations- und der allgemeinen Handlungsfreiheit und, zivilrechtlich gewendet, der Privatautonomie auch die Freiheit ist, sich nicht, nur aus einem verengten Blickwinkel oder auch bewusst nur in der Absicht zu informieren, das eigene Weltbild und die eigenen Auffassungen zu bestätigen, statt sie kritisch zu hinterfragen. Schon aus diesem Grund hilft der Einbau eines „Zufallelements“, durch das die Nutzer gelegentlich mit einer Nachricht konfrontiert werden, die nicht ihrem üblichen Präferenzprofil entspricht,[230] nicht weiter. Zivilrechtlich kann es nur darum gehen zu gewährleisten, dass der Nutzer über sein – regelmäßig durch Nutzung entsprechender Angebote schlüssig erklärtes – Einverständnis mit dem „Wie“ der Personalisierung von Suchmaschinenergebnissen und Newsfeeds eigenverantwortlich entscheiden kann. Diese Eigenverantwortlichkeit ist umso eher gegeben, je genauer sich der Nutzer über die von dem Auswahlalgorithmus genutzten Kriterien, insbesondere über die Hauptparameter des Rankings informieren kann. Der Vorschlag einer Kennzeichnung von ADM-Prozessen mit eingängigen Symbolen[231] dürfte eine solch genaue Information nicht ersetzen, sondern allenfalls im Sinne eines groben Überblicks ergänzen können.

[229] Der Abschlussbericht vom Juni 2018 kann unter https://www.blm.de/files/pdf2/bericht-datenspende---wer-sieht-was-auf-google.pdf abgerufen werden (letzter Abruf: 25.8.2018).
[230] Vgl. Algorithmic accountability, Gutachten der Abida-Assessing Big Data, S. 62, abrufbar unter: http://www.abida.de/de/blog-item/gutachten-algorithmic-accountability (letzter Abruf: 25.8.2018).
[231] A.a.O. (vorige Fn.), S. 59.

Entsprechende Transparenzforderungen enthalten die Vorschläge der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates vom 11. April 2018 (COM [2018] 185 final) für Online-Marktplätze[232] und vom 26. April 2018 (COM [2018] 238 final) für gewerbliche Nutzer von Online-Vermittlungsdiensten[233], wobei in letzterem statt von „Hauptparametern für das Ranking" von den „wichtigsten, das Ranking bestimmenden Parametern" die Rede ist. Diese Forderungen werden von der Arbeitsgruppe geteilt. Es wäre – ungeachtet des Umstands, dass sie wohl zum Teil schon heute erfüllt werden[234] – zu begrüßen, wenn sie ausgedehnt würden auf Auswahlalgorithmen von Suchmaschinenergebnissen und Newsfeeds für Verbraucher.

II. Personalisierte Werbung

1. Chancen algorithmenbasierter personalisierter Werbung

Aus Unternehmenssicht ermöglicht die algorithmische Auswertung personenbezogener Nutzerdaten (wie z.B. Facebook-Likes) die Bildung von Kundenzielgruppen, denen auf die jeweilige Zielgruppe zugeschnittene Werbung gezielt eingeblendet werden kann.[235] Online-Werbung kann dadurch zielgenauer platziert werden; Unternehmen, die nur gezielte Kundengruppen ansprechen möchten, können auf Werbeangebote für die breite Masse der Internetnutzer verzichten und dadurch ihren Werbeetat von überflüssigen Ausgaben für nicht relevante Werbeadressaten einsparen. Eine auf Personendaten (wie z.B. Facebook-Likes) beruhende personalisierte Werbung kann nachweislich den Werbeerfolg einer Online - Werbekampagne steigern.[236] Für spezialisierte kleine und mittelständische Unternehmen, die Marktnischen besetzen, verbessert personalisierte Werbung die Chancen, aus der großen Zahl der Nutzer eines bestimmten Internetdienstes relevante Kundengruppen herauszufiltern und zu erreichen, die man sonst allenfalls durch Annoncen in themenspezifischen Printmedien (wie z.B. Fachzeitschriften) erreichen könnte. Als Beispiel für die Chancen personalisierter Werbung im Internet wird in Medienberichten ein

[232] Art. 2 Nr. 4 sieht die Einfügung eines entsprechenden Art. 6a in die Richtlinie 2011/83/EU vor (S. 40 des Vorschlags der Kommission).
[233] Art. 5 (S. 25 des Vorschlags der Kommission).
[234] Z. B. erklärt Google die Funktionsweise seiner Suchmaschine auf der Seite https://www.google.com/intl/de/search/howsearchworks/ (letzter Abruf: 25.8.2018).
[235] *Matz/Kosinski/Nave/Stillwell*, Psychological targeting as an effective approach to digital mass persuasion, abrufbar unter: http://www.pnas.org/content/114/48/12714.full (letzter Abruf: 25.8.2018).
[236] *Matz/Kosinski/Nave/Stillwell*, Psychological targeting as an effective approach to digital mass persuasion, abrufbar unter: http://www.pnas.org/content/114/48/12714.full (letzter Abruf: 25.8.2018).

Panamahutmacher angeführt, der mittels GoogleAds in der Lage sei, 84 Auslandsmärkte zu beliefern.[237]

Aus Sicht der Adressaten von Onlinewerbung bietet die Berücksichtigung personenbezogener Daten bei der Auswahl von Werbeinhalten, die dem Nutzer angezeigt werden, die Chance, dass die tatsächlichen Interessen und Bedürfnisse des Nutzers hinsichtlich der im Rahmen der Internetnutzung eingeblendeten Werbung berücksichtigt werden. Dies eröffnet dem Nutzer die Möglichkeit, von potentiell für ihn interessanten Werbeannoncen mit weniger Rechercheaufwand (vertieft) Kenntnis zu erhalten und dadurch seine Konsumbedürfnisse komfortabler befriedigen zu können.[238] Dies kann auch unter Teilhabegesichtspunkten für die Internutzer förderlich sein, weil es Nutzern die Möglichkeit des Zugangs zu „Angeboten" ermöglicht, die ihnen zuvor mangels diesbezüglicher auf ihre persönlichen Interessen zugeschnittenen Recherche- oder Auswahlmöglichkeiten verschlossen waren.[239] Dies kann den Wettbewerbsdruck auf die jeweils relevanten Märkte zu Gunsten der Nutzer mit der Folge erhöhen, dass sie die Chance der Kenntniserlangung von alternativen Angeboten zu marktstarken Anbietern mit großen Werbeetats erhalten und dadurch ggf. passgenauere, günstigere oder qualitativ bessere Produkte finden oder Einsparungen erzielen können. Zugleich bietet eine stärkere Personalisierung der Werbung für den einzelnen Nutzer die Chance einer größeren Werbevielfalt zu Lasten einförmiger Werbeangebote finanzstarker Unternehmen in den Massenmedien, die ggf. an den speziellen Bedürfnissen und Interessen einzelner Nutzer oder Nutzergruppen vorbei gehen können.

2. Risiken algorithmenbasierter personalisierter Werbung

Da personalisierte Werbung auf der Erhebung und algorithmischen Auswertung personenbezogener Informationen des Nutzers (z.B. aus seinem bisherigen Surf- und Kaufverhalten; anhand des benutzten Endgeräts oder seinem Wohnort etc.) beruht, macht sie sich eine informationsbasierte Machtasymmetrie zwischen Unternehmen und Werbeadressaten zunutze, die auf der Einschätzung gründet, der Algorithmus könne bei hinreichender Datenlage die Interessen und Kaufabsichten des Nutzers besser vorhersehen als dieser selbst.[240] Hieran

---

[237] *Schneider*, Personalisierte Werbung: Durchs Netz verfolgt, abrufbar unter: http://www.tagesspiegel.de/wirtschaft/streitthema-tracking-personalisierte-werbung-durchs-netz-verfolgt-/6445032.html (letzter Abruf: 25.8.2018).

[238] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017.

[239] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[240] *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018); Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter:

anknüpfend könnte mit personalisierter Werbung die Gefahr der Verhaltensmanipulation der Werbeadressaten[241] z.B. durch „unbewusste Verhaltensanreize“[242] einhergehen sowie ferner die Problematik, dass Werbeinhalte passgenau auf die mittels Facebook-Likes algorithmisch ausgewertete Persönlichkeitsstruktur einzelner Benutzergruppen zugeschnitten werden.[243] Ferner könnte man gegen personalisierte Werbung anführen, dass weniger in ihr selbst als in der ihr notwendig vorgelagerten Datensammlung der Unternehmen über Nutzer, die in Nutzerprofilen verwaltet werden, ein Problem liege. Wenn man dies bejaht, so könnte man dies letztlich auch als Nachteil personalisierter Werbung bewerten, da sie einen erheblichen wirtschaftlichen Anreiz und teilweise auch das ausschlaggebende Motiv für die Datenerhebung und -speicherung der Unternehmen ist.[244] Damit könnte auch die personalisierte Werbung, insbesondere wenn sie mit früheren Suchanfragen korrespondiert, bei kritischen Nutzern das Gefühl der „Überwachung“ oder des „Verfolgtseins“ auslösen[245] und dadurch tendenziell in Teilen der Bevölkerung die Bereitschaft zur Nutzung des Internets schwächen.[246]

3. Stellungnahme

Wie oben (Kapitel 1, B. II. 2.) angekündigt, sollen, obwohl der Schwerpunkt der Bearbeitung nach der Zielsetzung der Arbeitsgruppe im Zivilrecht liegt, hier zunächst die datenschutzrechtlichen Probleme erörtert werden (a-c), da die aktuelle Diskussion um personalisierte Werbung nahezu ausschließlich im Bereich des Datenschutzrechts geführt wird. Die DS-GVO trifft keine

---

https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[241] *Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen - Eine Herausforderung für das Recht, AöR 142 (2017), 1 (5); vgl. auch *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1018) und *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 69, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf 25.8.2018) mit dem Beispiel der gezielten Werbeeinblendung bei Onlinespielern in besonders emotionalen Spielmomenten.

[242] *Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen - Eine Herausforderung für das Recht, AöR 142 (2017), 1 (13); Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter:. https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[243] So etwa in der Studie von *Matz/Kosinski/Nave/Stillwel*l, Psychological targeting as an effective approach to digital mass persuasion, abrufbar unter: http://www.pnas.org/content/114/48/12714.full (letzter Abruf: 25.8.2018).

[244] *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (abgerufen am 22.1.2018); *Schneider*, http://www.tagesspiegel.de/wirtschaft/streitthema-tracking-personalisierte-werbung-durchs-netz-verfolgt-/6445032.html (letzter Abruf: 25.8.2018).

[245] *Martin*i, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1018);

[246] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 73 f, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018).

spezifischen Regelungen hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten für Werbezwecke.[247] Datenschutzrechtlich werden als maßgebliche Regelungen für die Zulässigkeit personenbezogener Werbung zwei Tatbestände diskutiert, nämlich die Datenverarbeitung aufgrund einer Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO, vgl. dazu sogleich unter a.) und die Datenverarbeitung zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 Buchst. f DS-GVO, vgl. dazu sogleich unter b.). Im Zusammenhang mit der Frage der Freiwilligkeit einer Einwilligung wird zudem die Frage diskutiert, welche Folgen das Koppelungsverbot (Art. 7 Abs. 4 DS-GVO) für die personalisierte Werbung hat.[248] Auf das Sonderproblem der Werbung im Zusammenhang mit der Bereitstellung vernetzter Gebrauchsgegenstände wird in der Folge kurz unter c. eingegangen. Unter d. werden sodann die zivilrechtlichen Aspekte der personalisierten Werbung erörtert.

a. Zulässigkeit einer Datenverarbeitung zu Werbezwecken aufgrund von Einwilligung

Die Zulässigkeit einer Datenverarbeitung aufgrund von Einwilligung ist in Art 6 Abs. 1 Buchst. a DS-GVO geregelt. Die konkreten Anforderungen an die Einwilligung ergeben sich aus Art. 4 Nr. 11 und Art. 7 DS-GVO. Zu den generellen Voraussetzungen von Einwilligungen wird zunächst auf die Ausführungen unter C. II. 1. c. Bezug genommen.

Die Einwilligung kann in elektronischer Form und auch konkludent erfolgen, allerdings wird bezweifelt, dass unter Geltung der DS-GVO bereits in der fortgesetzten Nutzung einer Internetseite, nachdem in einem Banner auf die Nutzung von Cookies oder Fingerprinting-Verfahren hingewiesen wurde, eine (konkludente) Einwilligung gesehen werden kann, da nach Erwägungsgrund 32 die Einwilligung „durch eine eindeutige bestätigende Handlung“ erfolgen und die betroffene Person „in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten signalisiert“

[247] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1861).
[248] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1861 ff.); *Gierschmann*, Gestaltungsmöglichkeiten bei Verwendung personenbezogener Daten in der Werbung Auslegung des Art.6 Abs. 1 lit. f DS-GVO und Lösungsvorschläge; MMR 2018, 7 (7 ff.); *Golland*, Das Koppelungsverbot in der Datenschutz-Grundverordnung; Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag, MMR 2018, 130 (130 ff.).

haben muss. Daher wird empfohlen, eine aktive Einwilligung des Nutzers, etwa durch Ankreuzen eines Kästchens, einzuholen.[249]

In der Praxis scheint es allerdings verbreitet auch nach Geltungsbeginn der DS-GVO üblich zu sein, einen bloßen Hinweis auf die Verwendung von Cookies in einem Banner mitzuteilen und sodann von einer konkludenten Einwilligung ausgehen zu wollen.[250] Ob dies bei einer Überprüfung durch den Europäischen Gerichtshof Bestand haben wird, bleibt abzuwarten. Zudem wird im Hinblick auf die gem. Art. 4 Nr. 11 DS-GVO ausdrücklich vorausgesetzte Freiwilligkeit der Einwilligung vertreten, dass diese im Rahmen von sozialen Netzwerken fehlen dürfte, da der einzelne Nutzer bei einem Anbieterwechsel einen Großteil seiner virtuellen Verbindungen zu seinen Kontakten verlieren würde, so dass von einem „Take-it-or-leave-it" Szenario gesprochen werden könne.[251] Des Weiteren bleibt abzuwarten, welche Vorgaben und Klärungen insoweit durch die E-Privacy-Verordnung für elektronische Kommunikationsdienste erfolgen werden.

Möglicherweise von gravierender Auswirkung ist im Zusammenhang mit Einwilligungen in die Datenverarbeitung zwecks personalisierter Werbung zudem das sogenannte „Koppelungsverbot" des Art. 7 Abs. 4 DS-GVO. Diese Vorschrift ordnet an, dass bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Maße Rechnung getragen werden muss, ob unter anderem die Erfüllung eines Vertrages einschließlich der Erbringung einer Dienstleistung von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich sind. Im Erwägungsgrund 42 wird in Satz 5 hierzu ausgeführt, dass von Freiwilligkeit nur ausgegangen werden sollte, wenn die betroffene Person eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Vor diesem Hintergrund wird vertreten, dass das Geschäftsmodell „Bezahlung mit Daten", also die kostenlose Bereitstellung eines Internetdienstes im Austausch für die Einwilligung des Nutzers zur Verarbeitung seiner Daten möglicherweise vor dem Aus stehen könnte.[252] Als unzulässig wird es angesehen, dahingehende Einwilligungen im Wege des „Take-it-or-leave-it" einzuholen und auf der Grundlage umfassender Einwilligungsklauseln vermeintlich „kostenlose" Leistungen zu präsentieren. Der Tausch Leistung gegen Daten müsse transparent

[249] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1862) unter Verweis auf Erwägungsgrund 32 der DS-GVO.
[250] Eigene Praxiswahrnehmung aus der Arbeitsgemeinschaft.
[251] *Golland*, Das Koppelungsverbot in der Datenschutz-Grundverordnung; Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag, MMR 2018, 130 (130/131).
[252] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1859).

gemacht werden.[253] Von besonderer Bedeutung für die Frage der Zulässigkeit personalisierter Werbung ist insoweit die Frage, ob und gegebenenfalls in welchen Fällen den Nutzern ein anderer Zugang zu gleichwertigen vertraglichen Leistungen in zumutbarer Weise möglich sein muss. Anders als in dem früheren Koppelungsverbot des § 28 Abs. 3b BDSG a. F. ist eine derartige Einschränkung in Art. 7 Abs. 4 DS-GVO zwar nicht mehr ausdrücklich normiert, jedoch wird vertreten, dass dieser Aspekt in die Gesamtbetrachtung nach Art. 7 Ab. 4 DSVGO einfließen sollte, da Sinn und Zweck des Freiwilligkeitsgebots sei, den Einzelnen davor zu schützen, dass er allein deshalb in eine Datenverarbeitung einwilligen müsse, weil er ansonsten ein bestimmtes Leistungsangebot nicht in Anspruch nehmen könne.[254] Gerade wenn die Marktanteile anderer Anbieter deutlich niedriger seien und daher nur ein Bruchteil der Endkunden mit dem Angebot erreicht werden könne, sei die Gleichwertigkeit alternativer Angebote zweifelhaft. Daher gelte bei Diensten mit Netzwerkeffekten allgemein besondere Vorsicht. Könnten etwa bestimmte Personen nur erreicht werden, wenn ein bestimmter Anbieter gewählt werde – etwa die anderen Nutzer eines sozialen Netzwerkes wie Facebook – sei eine Alternative schon deshalb kaum zumutbar, weil und wenn diese von den relevanten Nutzern nicht verwendet werde.[255]

Vor diesem Hintergrund wird in der Literatur den Diensteanbietern angeraten, wenigstens zwei im Leistungsumfang gleichwertige Zugänge zu den Leistungen des angebotenen Dienstes bereitzustellen, von denen wenigstens einer unabhängig von der in die Verarbeitung von Nutzungsdaten zu kommerziellen Zwecken erteilenden Einwilligung sei. Künftige Geschäftsmodelle würden sich am Konzept des gleichwertigen Alternativzugangs orientieren müssen.[256] Andere halten es angesichts des Wortlauts von Art. 7 Abs. 4 DS-GVO für zweifelhaft, ob die Rechtsprechung wie bisher eine marktbeherrschende Stellung des jeweiligen Anbieters für die Feststellung der Freiwilligkeit berücksichtigen wird.[257]

Allerdings wird auch vertreten, dass in den Fällen, in denen für den Nutzer „entgeltfreie“ weil werbefinanzierte Inhalte und Dienstleistungen Vertragsgegenstand sind, nicht vom Vorliegen des Koppelungsverbot auszugehen sei, wenn hinreichend transparent gemacht werde, dass der angebotene Dienst nur unter dieser Voraussetzung wirtschaftlich angeboten werden könne.[258]

---

[253] *Kühling/Buchner* DS-GVO Kommentar, 2017, Art. 7 Rn 50 und 51.
[254] *Kühling/Buchner* DS-GVO Kommentar, 2017, Art. 7 Rn 52.
[255] *Kühling/Buchner* DS-GVO Kommentar, 2017, Art. 7 Rn 53.
[256] *Golland*, Das Koppelungsverbot in der Datenschutz-Grundverordnung; Anwendungsbereich, ökonomische Auswirkungen auf Web 2.0-Dienste und Lösungsvorschlag, MMR 2018, 130 (134).
[257] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1859).
[258] Gola/*Schulz*, DS-GVO Kommentar 2017, Art. 7 Rn 27.

Gerade bezüglich des Koppelungsverbotes sind damit noch grundlegende Fragen bezüglich der Reichweite und der Auslegung offen und es bleibt abzuwarten, wie sich die Rechtsprechung, insbesondere der Europäische Gerichtshof, hierzu positioniert.

b. Zulässigkeit einer Datenverarbeitung zu Werbezwecken zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten

Eine Datenverarbeitung zur Wahrung der berechtigten Interessen nach Art. 6 Abs. 1 Buchst. f DS-GVO ist zulässig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich (ist), sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt". Hinsichtlich der Einzelheiten zu dieser Frage wird zunächst wiederum Bezug auf die Ausführungen unter C. II. 1. b. genommen. Bei diesem Tatbestand ist eine Interessenabwägung mit den Interessen des Betroffenen vorzunehmen.

Im Rahmen der Interessenabwägung wird für Fälle der Datenverarbeitung zu Werbezwecken in der Literatur auf mehrere zueinander in einem Spannungsverhältnis stehende Erwägungsgründe verwiesen:

Insoweit wird auf Erwägungsgrund 47 hingewiesen, wonach die Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung gerade als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann. Auf der anderen Seite wird darauf hingewiesen, dass die Erstellung von Nutzungsprofilen als Profiling im Sinne der Definition in Art. 4 Nr. 4 DS-GVO einzuordnen ist, wonach Profiling vorliegt, wenn eine Datenauswertung darin besteht, bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten und dass die DS-GVO in verschiedenen Erwägungsgründen (etwa 60, 63, 70, 71 und insbesondere 72) zum Ausdruck bringt, dass das Profiling eine erhöhte Gefahr für die Rechte der Betroffenen bedeuten kann.[259] In diesem Zusammenhang wird vertreten, dass ein sachgerechter Ausgleich auch unter Geltung der DS-GVO der bisherigen Lösung in § 15 Abs. 3 des Telemediengesetzes entsprechen dürfte, wonach die Erstellung von Nutzungsprofilen und nachfolgende Werbemaßnahmen auf Basis pseudonymisierter Daten ohne Einwilligung des Betroffenen zulässig sind.[260]

[259] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1862).
[260] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1862).

Von anderen wird ein umfangreiches Prüfraster vorgeschlagen („berechtigtes Interesse“ als Eingangsschwelle, „Erforderlichkeit“, „Kein Überwiegen entgegenstehender Grundrechte oder Grundfreiheiten des Betroffenen“ sowie „Ausgewogenheit“) und prognostiziert, dass unter Geltung der DS-GVO die Verarbeitung von personenbezogenen Daten basierend auf „berechtigtem Interesse“ zukünftig in größerem Umfang möglich sein dürfte, als nach alter Rechtslage.[261]

Allerdings besteht bei der Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f DS-GVO eine gravierende Einschränkung, wenn sie personalisierte Werbung in Form von Direktwerbung rechtfertigen soll. Art 21 Abs. 2 DS-GVO normiert ein Widerspruchsrecht des Betroffenen für den Fall der Direktwerbung. Direktwerbung ist die unmittelbare Ansprache der betroffenen Person etwa durch Zusendung von Briefen oder Prospekten, durch Telefonanrufe, E-Mails oder Übermittlung von SMS.[262] Wird dieses Widerspruchrecht ausgeübt, kommt eine Interessenabwägung nach Art. 6 Abs. 1 Buchst. f DS-GVO von vornherein nicht mehr in Betracht. Gleiches muss gelten, wenn die betroffene Person nicht oder nicht ordnungsgemäß auf ihr Widerspruchsrecht nach Art. 21 Abs. 4 DS-GVO hingewiesen worden ist.[263]

Zudem besteht ein Widerspruchsrecht auch im Hinblick auf „Profiling“; dies allerdings nur bei Vorliegen von Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben (Art. 21 Abs. 1 DS-GVO). Profiling wird in Art. 4 Nr. 4 DS-GVO definiert als jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorauszusagen. Damit wird die Datenverarbeitung zwecks Erstellung von Persönlichkeitsprofilen für Werbezwecke („persönliche Vorlieben“, „Interessen“) eindeutig von Art. 21 Abs. 1 DS-GVO erfasst. So wird in Art. 21 Abs. 1 DS-GVO auch ausdrücklich Profiling erwähnt, das mit Direktwerbung in Zusammenhang steht.

Art. 21 Abs. 1 DS-GVO setzt allerdings anders als Absatz 2 die Geltendmachung von Gründen voraus, die sich aus der besonderen Situation des Betroffenen ergeben. Der Widerspruch muss daher damit begründet werden, dass im Fall der

---

[261] Vgl. sehr ausführlich *Gierschmann*, Gestaltungsmöglichkeiten bei Verwendung personenbezogener Daten in der Werbung Auslegung des Art.6 Abs. 1 Buchst. f DS-GVO und Lösungsvorschläge; MMR 2018, 7 (9-11).

[262] Vgl. Kühling/Buchner/*Herbst*, DS-GVO Kommentar, 2017, Art. 21 Rn 26.

[263] Kühling/Buchner/ *Petri*, DS-GVO Kommentar, 2017, Art. 6 Rn 176, vgl. auch bei Art. 21 Rn 32, 33.

konkreten Person eine atypische Konstellation vorliegt, die ihren Interessen besonderes Gewicht verleiht, wobei es sich insbesondere um Gründe handeln kann, von denen anzunehmen ist, dass sie dem Verantwortlichen nicht bekannt sind und die er bei seiner pauschalierenden Abwägung daher nicht berücksichtigen konnte.[264]

Der Tatbestand der Wahrung der berechtigten Interessen des Verantwortlichen gem. Art. 6 Abs. 1 Buchst. f DS-GVO ist damit für diejenigen, die Geschäftsmodelle betreiben, die auf der Verarbeitung personenbezogener Daten zu Werbezwecken beruhen, bereits aus diesem Grund mit nicht unerheblichen Unsicherheiten belastet. Auch hier bleibt zudem (wie bereits unter C. II. 1. b. ausgeführt) abzuwarten, welche konkretisierenden Vorgaben künftig der Europäische Gerichtshof im Hinblick auf die Durchführung der Abwägung bei Art. 6 Abs. 1 Buchst. f DS-GVO machen wird.

Ob die Belästigung durch personalisierte Werbung auch von Art. 22 DS-GVO erfasst wird (automatisierte Entscheidungen im Einzelfall einschließlich Profiling) ist umstritten. Gegen die Einbeziehung personalisierter Werbung in den Anwendungsbereich von Art. 22 DS-GVO spricht ein Umkehrschluss aus Art. 21 Abs. 2 DS-GVO, der dem Betroffenen ein Widerspruchsrecht gegen Direktwerbung einräumt und dementsprechend von einem an sich rechtmäßigen Verarbeitungsvorgang ausgeht. Erforderlich ist vielmehr eine „rechtliche Wirkung“, wovon immer dann die Rede sein kann, wenn sich durch die Entscheidung die Rechtsposition des Betroffenen ändert.[265] Hieran dürfte es bei personalisierter Werbung fehlen. Es ist daher davon auszugehen, dass Art. 22 DS-GVO bei personalisierter Werbung nicht eingreift.

c. Werbung im Zusammenhang mit der Bereitstellung vernetzter Gebrauchsgegenstände

Die im Zusammenhang mit der Nutzung vernetzter Gebrauchsgegenstände („Internet of Things“, etwa Fernseher, Haushaltsgeräte, Fitnessarmbänder („Wearables“) oder autonomes Fahren) anfallenden Daten sind für Werbezwecke besonders attraktiv, da sich aus ihnen, gegebenenfalls in Kombination mit weiteren Daten, aussagekräftige Profile der Nutzer erstellen lassen und auch das Offline-Verhalten im Alltag systematisch erfasst und für Werbezwecke ausgewertet werden kann.[266] Auch zu dieser Problematik enthält die DS-GVO

[264] Kühling/Buchner/*Herbst*, DS-GVO Kommentar, 2017, Art. 21 Rn 15.
[265] Vgl. zum Streitstand
http://www.abida.de/sites/default/files/ABIDA%20Gutachten%20Algorithmic%20Accountability.pdf.
Dort Seite 33 (Ziffer 2.1.1.1.1.3 am Ende) mwN in Fn 114 und 115 sowie in Fn 111 (letzter Abruf: 25.8.2018).
[266] *Weidert, Klar*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858 (1863).

keine speziellen Regelungen, so dass als Rechtfertigung die oben (unter a. und b.) beschriebenen Tatbestände der Einwilligung und der Wahrung berechtigter Interessen in Betracht kommen. Auch hier ist noch offen, wie die Rechtsprechung diese Fälle beurteilen wird und es bleibt abzuwarten, welche konkreteren Vorgaben die E-Privacy-Verordnung insoweit möglicherweise machen wird.

d. Zivilrechtliche Aspekte der personalisierten Werbung

Wie bereits oben dargestellt, wird die Problematik der personalisierten Werbung in erster Linie unter dem Gesichtspunkt des Datenschutzrechts diskutiert und zivilrechtliche Aspekte werden nur ganz vereinzelt angesprochen. So wird als Grenze der Zulässigkeit der Erstellung von Nutzerprofilen und ihrer Zusammenführung mit Bestandsdaten für personalisierte Werbung das Transparenzgebot für Allgemeine Geschäftsbedingungen (AGB) gesehen. Dabei wird darauf hingewiesen, dass es sich bei der Frage, ob das Einholen der entsprechenden Einwilligung für eine umfangreiche Datennutzung intransparent i.S.v. § 305 BGB ist, um eine Wertungsfrage handelt, die für jeden Einzelfall beurteilt werden müsse. Das Transparenzgebot sei verletzt, wenn Klauseln verwendet würden, die in ihrem Kernbereich oder für einen rechtlich nicht vorgebildeten Durchschnittsbürger unklar seien.[267]

Bei der Frage, ob vorgefertigte Vereinbarungen und (Einverständnis-) Erklärungen betreffend die Datenverarbeitung zu Werbezwecken überhaupt an den §§ 305 ff. BGB gemessen werden können, ist nunmehr die Datenschutz-Grundverordnung als höherrangiges Recht zu berücksichtigen.

Allerdings verweist die DS-GVO in Erwägungsgrund 42 auf die RL 93/13/EWG (Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen), so dass Einwilligungen in die Allgemeinen Geschäftsbedingungen der AGB-Kontrolle unterliegen und insbesondere nicht überraschend (§ 305c BGB) sein dürfen, wobei der objektive Maßstab der vernünftigen Erwartungshaltung einer durchschnittlich betroffenen Person zu berücksichtigen ist. Der Verweis auf die RL 93/13/EWG eröffnet Raum für eine inhaltliche Prüfung der Angemessenheit der Einwilligung im jeweiligen Verarbeitungskontext.[268] Eine zivilrechtliche AGB-Kontrolle ist daher auch neben der datenschutzrechtlichen Prüfung weiter möglich und erforderlich und kann zur zivilrechtlichen Unwirksamkeit der Einverständniserklärung führen.

---

[267] *Bauer*, Personalisierte Werbung auf Social Community Websites Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen, MMR 2008, 435 (437).

[268] Gola/*Schulz*, DS-GVO Kommentar 2017, Art. 7 Rn 42.

Auch zivilrechtlich ist in erster Linie von Interesse, auf welchem Rechtsgrund die Sammlung und Verarbeitung der Nutzerdaten zwecks Profilbildung und Schaltung personalisierter Werbung erfolgt; insbesondere ob ein wirksamer Vertrag hierüber zwischen dem Diensteanbieter und dem Nutzer zustande gekommen ist. Mit diesen Fragen hat sich die Arbeitsgruppe „Digitaler Neustart" im Hinblick auf soziale Netzwerke bereits ausführlich beschäftigt.[269] Dabei ist die Arbeitsgruppe bereits zu dem Schluss gekommen, dass als Leistung des Nutzers die datenschutzrechtliche Einwilligung in die kommerzielle Verwertung seiner Daten, z.B. zum Schalten personenspezifischer Werbung und zur Profilbildung zu sehen ist. Im ersten Abschlussbericht der Arbeitsgruppe sind auch die Themenkreise der zivilrechtlichen Relevanz des Rechts auf Widerruf der datenschutzrechtlichen Einwilligung und die Rechte der Parteien bei Vertragsbeendigung bei zivilrechtlichem Widerruf, die Einordnung der Hauptleistung des Nutzers (als synallagmatische, den Typus des Vertragsverhältnisses nicht prägende Gegenleistung), der Inhalt der vom Nutzer geschuldeten Gegenleistung (Datenqualität), die Zulässigkeit und Grenzen einer formularmäßigen Vereinbarung der Hauptleistung des Nutzers, sowie die Frage etwaigen Regelungsbedarfs ausführlich behandelt worden.[270] Die Arbeitsgruppe hat insoweit hinsichtlich einzelner Aspekte Regelungsbedarf ausgemacht und etwa vorgeschlagen, eine „Button-Lösung" für das Bezahlen mit Daten einzuführen.[271] Auf diese Ausführungen, an denen die Arbeitsgruppe weiter festhält, wird Bezug genommen. Im Hinblick auf die zivilrechtlichen Fragestellungen bezüglich des Zustandekommens eines Vertrages spielt die Frage der algorithmischen Auswertung rechtlich keine Rolle. Allen Vertragsparteien dürfte in der heutigen Zeit ohne weiteres bewusst sein, dass eine Datenerhebung und Profilbildung zum Zwecke der Schaltung personalisierter Werbung lediglich unter Verwendung von Algorithmen durchgeführt werden kann.

e. Schaltung/Einblendung der personalisierten Werbung

Bei der später geschalteten personalisierten Werbung handelt es sich um ein sogenanntes „invitatio ad offerendum", also die Aufforderung, ein Angebot zum Abschluss eines Vertrages abzugeben. Sie bewegt sich damit im Bereich der Anbahnung eines Vertragsschlusses und die Eingriffsintensität ist in der Regel eher gering. Zivilrechtliche Folgen (im engeren Sinne, also Folgen im Sinne des Bürgerlichen Gesetzbuchs) hat sie unmittelbar nicht.

[269] Bericht der Arbeitsgruppe „Digitaler Neustart" vom 15. Mai 2017, Kapitel 2 G. I. – III. (S.199 bis 225).
[270] Bericht der Arbeitsgruppe „Digitaler Neustart" vom 15. Mai 2017, Kapitel 2 G. II. 2. bis 8. (S.203 ff.)
[271] Bericht der Arbeitsgruppe „Digitaler Neustart" vom 15. Mai 2017, Kapitel 2 G. IV. (S. 225).

Hier können sich aber wettbewerbsrechtliche Fragen stellen, insbesondere wenn der Empfänger der personalisierten Werbung diese nicht erhalten möchte und Maßnahmen (z.B. Einsatz von Werbeblockern) ergreift, um die Werbung nicht wahrnehmen zu müssen.

Wettbewerbsrechtlich kann Werbung als unzumutbare Belästigung unzulässig sein (§ 7 Abs. 1, 2 des Gesetzes gegen den unlauteren Wettbewerb). In der Vorschrift sind verschiedene Fälle unzulässiger Arten von Werbung aufgeführt. Daneben kann unerwünschte Werbung im Einzelfall auch eine Verletzung des allgemeinen Persönlichkeitsrechts oder des Rechts am eingerichteten und ausgeübten Gewerbebetrieb begründen.[272] In den hier interessierenden Fällen wird dies nur in Ausnahmefällen in Betracht kommen, da der Adressat der Werbung regelmäßig die datenschutzrechtliche Einwilligung in die kommerzielle Nutzung seiner Daten als Gegenleistung für das genutzte Angebot gerade auch zu Werbezwecken erteilt hat.[273]

Wenn der Adressat diese Werbung, die ihn nicht in Grundrechten verletzt und auch nicht wettbewerbswidrig ist (also dem Normalfall einer personalisierten Werbung, die auf die datenschutzrechtliche Einwilligung in die kommerzielle Nutzung der Daten beruht), aber nicht wahrnehmen möchte, stellt sich die Frage, ob er sich – seinerseits nun mit Hilfe von Algorithmen – durch den Einsatz von speziellen Computerprogrammen (Werbeblockern) der Wahrnehmung der Werbung entziehen kann.

In der Literatur wird insoweit ausgeführt, dass es – jenseits etwaiger individualvertraglicher Vereinbarungen – in der Privatrechtsordnung keinen Anspruch gebe, dass ein Umworbener die Werbebotschaft auch zur Kenntnis nehmen müsse. Ein Anspruch auf Rezeption der Werbung bestehe nicht. Der Adressat könne sich demgegenüber auf ein rechtlich anerkanntes Interesse berufen, wenn er Schutzvorkehrungen gegen legale, von ihm aber trotzdem nicht gewünschte Werbung treffe. So umfasse Art. 5 Abs. 1 S. 1. Hs. 1 GG auch die negative Informationsfreiheit, denn ein Zwang zur Aufnahme bestimmter Information sei mit einem freien öffentlichen Kommunikationsprozess unvereinbar. Folglich nehme der Adressat eine grundrechtlich verbürgte Freiheit

[272] Vgl. zum Allgemeinen Persönlichkeitsrecht ausführlich: *Gomille*, Die Verteidigung gegen unerwünschte Werbung, GRUR 2017, 241 (242 ff.); zum eingerichteten und ausgeübten Gewerbebetrieb *Köhler/Bornkamm/Feddersen*, UWG Kommentar, 36. Aufl. 2018, Einleitung Rn 7.38 mwN.

[273] Eine unzumutbare Belästigung iSv § 7 UWG könnte hier im Ausnahmefall dennoch zu bejahen sein, etwa wenn die personalisierte Werbung in einem Umfang erfolgt (etwa durch die Zusendung von Werbe-Emails in außerordentlich großem Umfang), die die Kommunikation des Betroffenen ernsthaft beeinträchtigt.

in Anspruch, wenn er während der Werbeinsel im TV manuell den Sender wechsele, ein Pop-up-Fenster wegklicke oder einen abonnierten Newsletter ungesehen lösche. Nichts anderes gelte, wenn er sich technischer Lösungen bediene, die ihn bei dieser Informationsauslese unterstützten.[274] So hat auch der Bundesgerichtshof mit Urteil vom 19. April 2018 das Angebot des Werbeblockers AdBlockPlus für grundsätzlich zulässig erklärt und auch in dem Vertrieb dieses Programms keinen Wettbewerbsverstoß gesehen.[275] Wenn ein Nutzer ein werbefinanziertes Medium mit aktiviertem Werbeblocker ansteuert, ist der Medienbetreiber allerdings berechtigt, ihn von dem weiteren Medienkonsum auszuschließen, was auch technisch möglich ist und praktiziert wird.[276]

Das Schalten der personalisierten Werbung ist damit als solches zivilrechtlich kaum von Bedeutung. Wettbewerbsrechtlich ist es zulässig. Die Verhinderung der Rezeption mittels Algorithmen durch Werbeblocker ist ebenso zulässig – der Anbieter ist in diesem Fall aber berechtigt, den Kunden von dem werbefinanzierten Angebot auszuschließen. Dies ist auch folgerichtig, da die datenschutzrechtliche Einwilligung in die Verwendung der Nutzerdaten auch zu Werbezwecken gerade Gegenleistung des Nutzers ist und der Zweck dieser Gegenleistung durch Blockieren der Werbung vereitelt würde.

f. Facebook Datenskandal und Problematik des Einsatzes persönlicher Daten zu Zwecken von (ggf. verdeckter) Wahlwerbung

Die algorithmische Auswertung von Nutzerverhalten und die Erstellung von Profilen ist in der jüngsten Vergangenheit insbesondere im Hinblick auf den sog. Facebook-Datenskandal diskutiert worden.

Dabei hatte der Entwickler einer Umfrage-App Informationen von Nutzern an die Analysefirma Cambridge Analytica weitergereicht. Die Firma hatte unter anderem für das Wahlkampfteam von US-Präsident Donald Trump gearbeitet. Inzwischen ist von rund 310.000 betroffenen Nutzern in Deutschland die Rede; Facebook hat erklärt, dass weltweit Informationen von bis zu 87 Mio. Mitgliedern unrechtmäßig an die Analysefirma gelangt sein könnten. An der Umfrage

[274] *Gomille*, Die Verteidigung gegen unerwünschte Werbung, GRUR 2017, 241 (245 mwN) – im Jahr 2000 hatte das LG Berlin das für den Vertrieb eines Zusatzgeräts zur automatischen Ausblendung von Fernsehwerbung nach anders beurteilt (LG Berlin ZUM-RD, 144 (146)), was aber durch die jüngste Rechtsprechung des Bundesgerichtshofs zu Werbeblockern überholt sein dürfte.

[275] BGH, Urt. v. 19. 4. 2018, Az I RZ 154/16 (derzeit nur als Pressemitteilung verfügbar) (die vorangegangenen Instanzen – LG und OLG Köln – hatten indes bereits wegen besonderer Umstände einzelne Aspekte für wettbewerbswidrig erklärt (vgl. OLG-Köln GRUR 2016, 1082); ebenso auch *Gomille*, Die Verteidigung gegen unerwünschte Werbung, GRUR 2017, 241 (247/248).

[276] *Gomille*, Die Verteidigung gegen unerwünschte Werbung, GRUR 2017, 241 (247 mwN).

teilgenommen hatten zwar nur 65 Nutzer in Deutschland (weltweit 270.000), allerdings wurden insoweit auch die Daten von deren Facebook-Freunden weitergegeben. Von 2010 bis 2015 hatte Facebook es den Entwicklern derartiger Apps erlaubt, auch die persönlichen Daten von Nutzern zu erfassen, die diese Apps gar nicht selbst nutzten.[277] Der Skandal führte dazu, dass die Analysefirma Cambridge Analytica ihr Geschäft einstellte und Insolvenz anmeldete[278] und der Aktienkurs von Facebook nach Bekanntwerden des Skandals um sieben Prozent fiel (was 35 Milliarden US-Dollar entspricht).[279]

Eine Weitergabe und Auswertung der Nutzerdaten wie sie in dem Datenskandal stattgefunden hatte, wäre unter Geltung der DS-GVO mangels Eingreifens jeglichen Rechtfertigungsgrundes gem. Art. 6 Abs. 1 DS-GVO für die Datenverarbeitung rechtswidrig. Es bestünden die Ansprüche nach Art. 12 ff. und 82 DS-GVO (etwa Information, Auskunft, Löschung und Schadensersatz), sowie die Möglichkeit der Verhängung eines Bußgeldes in Höhe von bis zu 20 Mio. Euro oder 4 % des weltweit erzielten Jahresumsatzes durch die Datenschutz-Aufsichtsbehörde (Art. 83 Abs. 5 DS-GVO). Auch nach zuvor geltendem deutschen Datenschutzrecht war der Vorgang rechtswidrig (§§ 4 ff. BDSG a. F. vor dem 25. Mai 2018). Auch das Bundesdatenschutzgesetz sah vor Geltung der DS-GVO bereits Ansprüche des Betroffenen vor (Auskunft, § 19, 35 BDSG, Berichtigung, Löschung und Sperrung, §§ 20, 35 BDSG, Schadensersatz §§ 7, 8 BDSG) und auch die Verhängung eines Bußgeldes war möglich (§ 43 BDSG). Da allerdings Facebook seinen Sitz in Irland hat und in Deutschland keine Niederlassung unterhält, war irisches Recht maßgebend.[280] Seit dem 25. Mai 2018 ist aber die DS-GVO aufgrund des Marktortprinzips auch auf Facebook anzuwenden (vgl. zum räumlichen Anwendungsbereich Art. 3 DS-GVO).

Ein besonderes Problem, auf das die Öffentlichkeit insbesondere im Zusammenhang mit dem Facebook-Datenskandal aufmerksam geworden ist, stellt (gegebenenfalls verdeckte) Wahlwerbung dar. Cambridge Analytica erstellte im US-Wahlkampf, etwa anhand persönlichkeitsrelevanter Daten,

---

[277] Vgl. etwa http://www.spiegel.de/netzwelt/web/datenskandal-bei-facebook-310-000-deutsche-koennten-betroffen-sein-a-1201310.html (letzter Abruf: 25.8.2018) sowie https://www.sueddeutsche.de/digital/datenmissbrauch-was-ist-eigentlich-gerade-bei-facebook-los-1.3932349 (letzter Abruf: 25.8.2018).

[278] Vgl. https://www.heise.de/newsticker/meldung/Facebook-Datenskandal-Cambridge-Analytica-macht-angeblich-dicht-4039494.html (letzter Abruf 25.8.2018); wobei allerdings offenbar in der Folge von deren Managern sogleich eine Firma mit neuem Namen aber gleichem Konzept gegründet wurde vgl. https://www.tagesspiegel.de/wirtschaft/nach-facebook-datenskandal-war-die-insolvenz-von-cambridge-analytica-nur-ein-manoever/21237184.html (letzter Abruf 25.8.2018).

[279] Vgl. https://www.bayern3.de/facebook-datenskandal-cambridge-analytica-kurs-aktie-tipps-sicherheit-datenschutz-was-tun (letzter Abruf: 25.8.2018).

[280] § 1 Abs. 5 BDSG, vgl. dazu etwa auch aus der Presse: http://www.fr.de/politik/facebook-kann-ich-klagen-a-1482884; https://www.berliner-zeitung.de/politik/datenskandal--koennen-betroffene-in-deutschland-facebook-verklagen--29989272 (letzter Abruf: 25.8.2018).

individualisierte Wahlwerbung für Donald Trump im amerikanischen Präsidentschaftswahlkampf und dabei insgesamt 175.000 verschiedene (jeweils auf bestimmte Personengruppen individuell angepasste) Versionen.[281]

Bei einem Einsatz von Algorithmen, die dafür konzipiert sind, Persönlichkeitsanalysen vorzunehmen, um auf diese Weise psychologisch optimiert Personen zu einem bestimmten Wahlverhalten zu bewegen (bis hin dazu, Wähler, die mit Sicherheit nicht den eigenen Kandidaten wählen werden, nach Möglichkeit von der Wahl abzuhalten),[282] könnte eine Gefahr für die freie politische Willensbildung bestehen.

Soweit – wie oben dargestellt – unberechtigt auf die Daten von Facebook-Freunden zugegriffen wird, stellt sich dieses Verhalten ohne weiteres als rechtswidrig dar und die DS-GVO bietet hinreichende Reaktions- und Sanktionsmöglichkeiten.

Allerdings werden Daten vielfach aufgrund einer Einwilligung des Betroffenen gesammelt. Insoweit stellt sich die Frage, inwieweit die über den Einzelnen gesammelten Daten, aufgrund von Art. 6 Abs. 1 Buchst. a oder Buchst. f DS-GVO derzeit zulässigerweise auch für Wahlwerbezwecke genutzt werden dürften und ob die DS-GVO insoweit bereits hinreichenden Schutz bietet.

In diesem Zusammenhang sind die Anforderungen zu berücksichtigen, die die DS-GVO an eine wirksame Einwilligung stellt. Diese setzt zum einen Informiertheit voraus (Erwägungsgrund 32), so dass die Einwilligung für den konkreten Fall und in Kenntnis der Sachlage abgegeben werden muss. Die betreffende Person muss wissen, was mit den Daten geschehen soll. Unspezifische Pauschal- oder Blankoeinwilligungen sind nicht statthaft.[283] Soll sich die Erklärung auf mehrere werbende Unternehmen erstrecken, sind diese gesondert aufzuführen, wobei die Angabe der Kategorie von Empfängern (z.B. Dienstleister aus der Gartenbaubranche) zureichend ist.[284] Zudem setzt eine wirksame Einwilligung voraus, dass die Einwilligung hinreichend bestimmt ist. Personenbezogene Daten dürfen danach stets nur für festgelegte eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Zweckbestimmung muss im Zuge der Einwilligungserteilung grundsätzlich so präzise wie möglich erfolgen, um sicherzustellen, dass personenbezogene Daten nicht für Zwecke verarbeitet werden, mit denen die betroffene Person bei der Erhebung nicht gerechnet hat. Auch bezüglich dieses Erfordernisses gilt, dass eine pauschale

[281] www.dasmagazin.ch vom 12.3.2016 „Ich habe nur gezeigt, dass es die Bombe gibt“ und Süddeutsche Zeitung vom 3./4.3.2018, S. 51 „Der Vermesser der Seele“.
[282] Vgl. www.dasmagazin.ch vom 12.3.2016 „Ich habe nur gezeigt, dass es die Bombe gibt“ unter der Zwischenüberschrift „Wie man Clinton-Wähler von der Urne fernhält“.
[283] Gola/*Schulz*, DS-GVO Kommentar 2017, Art. 7 Rn 31.
[284] Gola/*Schulz*, DS-GVO Kommentar 2017, Art. 7 Rn 34.

Einwilligungsklausel, die sich nicht auf bestimmte Datenverarbeitungszwecke beschränkt, stets unwirksam ist.[285]

Aus all dem ergibt sich, dass eine Verwendung von personenbezogenen Daten zwecks Profilbildung zu Wahlwerbezwecken nur zulässig wäre, wenn explizit in Wahlwerbung eingewilligt wurde. Zudem dürfte, damit auch eine Wahlwerbung, die nicht explizit als solche gekennzeichnet ist, zulässig ist, auch auf diesen Umstand im Rahmen der Einholung der Einwilligung explizit gesondert hinzuweisen sein, wobei insoweit fraglich ist, ob eine derartige verdeckte Einflussnahme überhaupt einen eindeutigen und legitimen Zweck darstellen und zulässig sein kann.

g. Gesetzgeberischer Handlungsbedarf

Im Hinblick auf personalisierte Werbung besteht der Handlungsbedarf, den die Arbeitsgruppe bereits als Ergebnis ihrer ersten Arbeitsphase für das Bezahlen mit Daten ausgemacht hat, weiter fort. Personalisierte Werbung ist ein besonders häufiger und wichtiger Anwendungsfall des Bezahlens mit Daten. Insoweit bleibt es bei folgenden Empfehlungen der Arbeitsgruppe aus dem ersten Abschlussbericht:

> „Die Möglichkeiten des zivilrechtlichen Widerrufs und der Beendigung eines Vertrags, der ein „Bezahlen mit Daten“ vorsieht, erfordern keine grundlegenden Rechtsänderungen.
>
> Mit Blick auf § 357 Abs. 9 BGB, mit welchem Art. 14 Abs. 4 lit. b. der Verbraucherrechterichtlinie umgesetzt worden ist, sollte erwogen werden, für Widerrufsfälle ausdrücklich zu regeln, dass (auch) den Anbieter keine Wertersatzpflicht trifft.
>
> Es könnte sich empfehlen und sollte deshalb erwogen werden, im allgemeinen Schuldrecht allgemein klarzustellen, dass ein Entgelt auch in der Erteilung einer Einwilligung in die Verarbeitung personenbezogener Daten für kommerzielle Zwecke des Vertragspartners bestehen kann.
>
> Mit Blick auf das Erfordernis der Freiwilligkeit einer datenschutzrechtlichen Einwilligung sollte bestimmt werden, dass ein zivilrechtlicher Anspruch auf Erteilung einer solchen Einwilligung nicht klagbar ist und dass aus der Nichterfüllung eines auf Erteilung einer

[285] *Kühling/Buchner*, DS-GVO Kommentar, 2017, Art. 7 Rn 61/62.

> datenschutzrechtlichen Einwilligung gerichteten Anspruchs keine anderweitigen Ansprüche hergeleitet werden können.
>
> Zum Schutz von Verbrauchern empfiehlt sich für das „Bezahlen mit Daten“ eine „Button-Lösung“. Mit einer entsprechenden Ergänzung von § 312j Abs. 3 BGB sollte eine Ergänzung von § 312a Abs. 3 BGB einhergehen. Des Weiteren sollte eine Ergänzung von § 312j Abs. 4 BGB in dem Sinne erwogen werden, dass ein Verstoß gegen den neu gefassten § 312j Abs. 3 BGB, soweit er einen Fall des „Bezahlens mit Daten“ betrifft, nicht das Zustandekommen des Vertrags hindert, sondern lediglich zur Folge hat, dass der Verbraucher an den Vertrag nicht gebunden ist.
>
> Es sollte in Betracht gezogen werden, gesetzlich zu bestimmen, dass es nicht zu Lasten einer Vertragspartei zu werten ist, wenn die von ihr zu erbringende Gegenleistung nicht in einer Geldzahlung, sondern in ihrer Einwilligung in die Nutzung personenbezogener Daten besteht.“[286]

Hinsichtlich der Einblendungen der Werbung selbst führen die geltenden wettbewerbsrechtlichen Vorschriften und die Rechtsprechung hierzu zu angemessenen Ergebnissen. Gesetzgeberischer Handlungsbedarf besteht insoweit nicht.

Bezüglich der datenschutzrechtlichen Regelungen der DS-GVO besteht zwar noch bei zahlreichen Fragen Rechtsunsicherheit. Hier bleibt allerdings zunächst die Rechtsprechung zur Auslegung der DS-GVO abzuwarten, bis abschließend beurteilt werden kann, ob und ggf. inwiefern gesetzgeberisch ergänzender Handlungsbedarf besteht. Insoweit ist allerdings zu beachten, dass den Mitgliedstaaten für Fälle der Datenverarbeitung nach Art. 6 Abs. 1 Buchst. f DS-GVO keine Befugnis zum Erlass spezifischer Bestimmungen eingeräumt ist (vgl. Art. 6 Abs. 2 und 3, die nur auf Art. 6 Abs. 1 Buchst. c und e DS-GVO Bezug nehmen). Entsprechender Rechtsetzungsbedarf wäre mithin auf der Ebene des Unionsrechts zu verwirklichen.

Aus Sicht der Nutzer erschiene es wünschenswert, wenn das Koppelungsverbot gem. Art. 7 Abs. 4 DS-GVO in der Weise ausgelegt würde, dass (jedenfalls in Fällen, in denen ein Anbieter eine marktbeherrschende Stellung innehat) ein alternativer (entgeltlicher) Zugang zu dem Angebot bereitgehalten werden muss. Dies würde auch denjenigen Nutzern, die bereit sind, einen gewissen Betrag für die Inanspruchnahme der Leistung zu bezahlen, aber ihre persönlichen Daten nicht gegenüber Dritten freigeben möchten, die Nutzung der entsprechenden

[286] Bericht der Arbeitsgruppe „Digitaler Neustart“ vom 15. Mai 2017, Kapitel 2 G. IV. (S. 225).

Angebote ermöglichen. Insoweit bliebe auch abzuwarten, wie hoch die Netzwerkbetreiber diesen Betrag ansetzen würden und ob gegebenenfalls ein entsprechend hoher Betrag von der Rechtsprechung als nicht hinreichend angesehen würde, um dem Koppelungsverbot Genüge zu tun. Die Einwilligung in die algorithmenbasierte Erstellung und Verwendung von Persönlichkeitsprofilen wäre nicht mehr Voraussetzung, um überhaupt an den größten sozialen Netzwerken teilnehmen zu können. Insoweit bleibt aber zunächst die Entwicklung der Rechtsprechung zu dieser Frage abzuwarten, bevor gegebenenfalls gesetzgeberischer Handlungsbedarf (soweit die DS-GVO überhaupt noch nationale Regelungen zulässt) erörtert werden kann.

Im Hinblick auf den Facebook-Datenskandal gilt, dass aufgrund derartiger Vorgänge nicht unerhebliche Gefahren für die Freiheit des Einzelnen und die Gesellschaft insgesamt drohen. Insoweit ist zu berücksichtigen, dass zum einen aufgrund der oben beschriebenen Datensammelmethoden über das Setzen von Cookies über sehr lange Zeiträume detaillierte Informationen in erheblichem Umfang über den einzelnen Nutzer gesammelt werden können. Zudem ist zu berücksichtigen, dass verhältnismäßig wenige Informationen bereits sehr weitgehende Rückschlüsse über die Persönlichkeit und damit das potenzielle Verhalten des Einzelnen ermöglichen, da es – wie bereits oben unter Kapitel 1 B. II. 2. dargestellt - Algorithmen gibt, die die Persönlichkeit von Menschen anhand von verhältnismäßig wenigen Facebook-Likes sehr genau einschätzen können. Der Psychologe Kosinski, der einen derartigen Algorithmus programmiert hatte, hatte eine Mitarbeit bei Cambridge Analytica zwar abgelehnt. Dort hatte man aber in der Folge vergleichbare Algorithmen entwickelt.[287]

Angesichts des Umstandes, dass – wie oben dargestellt – die Datensammlung mittels Cookies auch vor zehn Jahren schon in der juristischen Fachliteratur diskutiert wurde, dürften über zahlreiche Internetnutzer bereits ganz erhebliche Datenmengen vorliegen, die zur Erstellung von detaillierten Persönlichkeitsprofilen genutzt werden können.

Die Schaltung von Wirtschaftswerbung erscheint aber auch unter Berücksichtigung dieses Umstandes tendenziell als unproblematisch, da es sich bei der Werbung für Produkte um einen gesellschaftlich unproblematischeren Vorgang handelt und heutzutage die Rezeption auch personalisierter Produktwerbung zum Alltag der meisten Menschen gehört. Zudem wird auch personalisierte Produktwerbung als Werbung wahrgenommen, so dass die Beeinflussung sich insoweit in Grenzen hält.

Ausdifferenzierte politische Einflussnahme aufgrund von mittels umfangreicher gesammelter Daten erstellten Persönlichkeitsprofilen stellt sich aber als problematischer dar als bloße Produktwerbung. Diese Art von Einflussnahme

[287] Vgl. Süddeutsche Zeitung vom 3./4.3.2018, S. 51 „Der Vermesser der Seele“.

unterscheidet sich auch dadurch von der Schaltung herkömmlicher Wirtschaftswerbung, als sie nicht notwendigerweise klar als Wahlwerbung zu erkennen ist. So ist etwa die Übermittlung von Informationen, die potenzielle Wähler eines anderen Lagers von der Wahl abhalten sollen, für den Betroffenen nicht in gleicher Weise als Wahlwerbung zu erkennen, wie herkömmliche Werbung.

Allerdings handelt es sich bei der Vorgehensweise im Facebook-Datenskandal gerade nach dem jetzt geltenden und auf Facebook anzuwendenden EU-Recht (DS-GVO) um rechtswidrige Datenverarbeitung, so dass bei einem etwaigen künftigen vergleichbaren Skandal die Sanktionsmöglichkeiten und Ansprüche aus der DS-GVO eingreifen würden. Bezüglich der Verwendung von auf diese Art und Weise (unrechtmäßig) erlangter Daten enthält die DS-GVO hinreichende Sanktionsmöglichkeiten, so dass insoweit kein gesetzgeberischer Handlungsbedarf besteht.

Vor dem Hintergrund, dass die DS-GVO für eine wirksame Einwilligung in die Verwendung zu Wahlwerbezwecken eine speziell hierauf bezogene Aufklärung und Einwilligungserklärung verlangt und so durch konkrete Informationserfordernisse Schutz bietet und (soweit überhaupt zulässig) es zudem wohl gebietet, auch gesondert eine explizite Einwilligung für die Übersendung von Wahlwerbung, die nicht explizit als solche gekennzeichnet ist, einzuholen (s.o. unter Kapitel 1 C. II. 2.), besteht auch jedenfalls derzeit kein akuter gesetzgeberischer Handlungsbedarf. Insoweit sollte aber die Auslegung der DS-GVO durch die Gerichte, insbesondere den EuGH intensiv beobachtet werden.

III. Personalisierte Preise

1. Chancen personalisierter Preise im Online-Handel

Aus Unternehmenssicht sollen personalisierte Preise darauf abzielen, mittels Algorithmen, die z.B. das Surfverhalten und die bisherige (Online-)Kaufhistorie auswerten, die Zahlungsbereitschaft des Kunden für ein Produkt einzuschätzen, um auf diese Weise die maximale Zahlungsbereitschaft des Kunden und damit verbundene Mehrerlöse gegenüber dem gegenwärtigen Einheitspreissystem realisieren zu können.[288] Ob sich diese Zielsetzung derzeit jedenfalls in Märkten mit intaktem Wettbewerb realisieren ließe, ist angesichts der – im Onlinebereich nicht zuletzt durch Preisvergleichsportalen gesteigerten –

[288] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 6, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

Preisvergleichsmöglichkeiten der Kunden und der Notwendigkeit der Anbieter, ihre personalisierten Preisofferten auch auf die sonstigen Vertriebswege (z.B. stationärer Handel) zu erstrecken,[289] umstritten.[290] Personalisierte Preise können aus Unternehmenssicht auch umgekehrt dazu eingesetzt werden, Kunden durch für sie besonders attraktive Offerten zu einem Anbieter- oder Markenwechsel (sogenanntes „Brand- oder Storeswitching") zu bewegen, in der Erwartung, eine längerfristige Kundenbeziehung bzw. Kaufgewohnheit des Kunden zu etablieren, die bei im Zeitverlauf abnehmender Preissensibilität des Kunden dem Anbieter oder dem Produkt gegenüber die Chance zu Mehrerlösen bietet.[291]

Aus Kundensicht könnten personalisierte Preise auch dazu führen, dass weniger zahlungskräftigen Kunden mit geringerer Zahlungsbereitschaft niedrigere Preise angeboten werden, die durch die Mehrerlöse der Kunden, die mehr als den bisherigen Einheitspreis zahlen, mitgetragen werden.[292] Ebenso wie die Chance der Erlösung der Maximalpreise bei zahlungskräftigen Kunden ist die Realisierbarkeit dieses möglichen „Wohlfahrtseffekts" personalisierter Preise indes umstritten, da in Frage gestellt wird, dass Unternehmen dazu motiviert sein

---

[289] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 12, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[290] Skeptisch insoweit etwa: *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 12, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018); bejahend dagegen: *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018); ebenso jedenfalls für Kunden mit geringer Wechselbereitschaft gegenüber ihrem Vertragspartner: Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 5, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[291] *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 5, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018).

[292] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 5, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018); *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 4, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018); *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 8, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

könnten, geringen Zahlungsbereitschaften bei der Preisbildung Rechnung zu tragen.[293] Zumindest in der Konstellation, dass ein Anbieter temporär durch offensive Preispolitik seine Marktanteile auszuweiten versucht, dürfte indes auch die Berücksichtigung unterdurchschnittlicher Zahlungsbereitschaften unternehmerseitig ernsthaft in Betracht kommen.

2. Risiken personalisierter Preise im Online-Handel

Aus Unternehmenssicht wird das Risiko diskutiert, dass mangels hinreichender diesbezüglicher Kompetenz auf Anbieterseite und/oder mangels hinreichend leistungsfähiger Algorithmen Zahlungsbereitschaften falsch eingeschätzt werden und dadurch entweder Kunden verprellt oder Mindererlöse gegenüber dem Einheitspreismodell erzielt werden können.[294] Ferner wird aus Unternehmenssicht das Risiko gesehen, dass bei fehlender Konsistenz personalisierter Preise über alle Vertriebswege eines Unternehmens hinweg „Verwirrung" und Verdruss auf Verbraucherseite erzeugt werden kann und Kundenbeziehungen verloren gehen können.[295] Überdies wird aus Unternehmerperspektive das Szenario beschrieben, dass jedenfalls onlineaffine Kunden in zunehmendem Maße Strategien entwickeln könnten, um personalisierte Preise zu unterlaufen, indem sie z.B. die Datenerhebungen der

---

[293] Während dies einerseits für möglich erachtet wird: *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 8, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018), sind andere Stimmen in der Literatur skeptisch: Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 5, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018); *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 4, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018); *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018).

[294] S*chleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 11 f., abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[295] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel". Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 12., abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018); *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 6, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018).

Unternehmen technisch unterbinden, mittels Software die Übertragung falscher preisrelevanter Daten veranlassen, unter Fake-Accounts einkaufen oder dritte Personen mit „günstigeren“ Profileigenschaften mit dem Einkauf beauftragen.[296] Des Weiteren ist es sowohl für die Kaufentscheidung[297] als auch für die Kundenbindung wichtig, dass der Kunde die vereinbarten und gezahlten Preise als „fair“ empfindet. Gewinnt der Kunde dagegen – entweder mangels Transparenz der Preispersonalisierung oder im Wege des Austauschs mit anderen Kunden – den Eindruck, unfair behandelt worden zu sein, kann dies für die betroffenen Unternehmen zum Verlust von Kundenbeziehungen und Imageproblemen führen.[298] Aus Unternehmersicht könnten auch in wettbewerblicher Hinsicht insoweit durch Preispersonalisierung falsche Anreize gesetzt werden, dass Unternehmen, die sich gegen Datenerhebung bzw. –kauf zum Zwecke der Preispersonalisierung entscheiden, Wettbewerbsnachteile erleiden könnten.[299] Allerdings wird die Bedeutung dieses Aspekts stark davon abhängen, ob die Preispersonalisierung künftig eine stärkere Nutzerakzeptanz erfährt, da bei mangelnder Nutzerakzeptanz der garantierte Verzicht eines Unternehmens auf Datenerhebung- und/oder –kauf sowie Preispersonalisierung auch gezielt als Werbeargument und Wettbewerbsvorteil eingesetzt werden könnte. Schließlich zeigen aus Unternehmenssicht Versuche, personalisierte Preise durchzusetzen, dass diese vielfach – jedenfalls wenn sie nicht als transparent und „fair“ empfunden werden[300] oder wenn der Kunde nicht die

---

[296] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 14 f., abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[297] *Richards/Liaukonyte/Streletskaya*, Personaliced pricing and Price fairness, Ithaka/New York, September 2015, S. 32, abrufbar unter: https://courses.cit.cornell.edu/jl2545/papers/personalized_Pricing_IJIO.pdf, (letzter Abruf: 25.8.2018).

[298] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 13 f., abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018).

[299] *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 4, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018).

[300] *Schleusener/Hosell*, Expertise zum Thema „Personalisierte Preisdifferenzierung im Online-Handel“. Untersuchung und Ausarbeitung für den Sachverständigenrat für Verbraucherfragen beim Bundesminister für Justiz und für Verbraucherschutz, Oktober 2015, S. 14, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/eWeb-Research-Center_Preisdifferenzierung-im-Onlinehandel.pdf (letzter Abruf: 25.8.2018); *Richards/Liaukonyte/Streletskaya*, Personaliced pricing and Price fairness, Ithaka/New York, September 2015, S. 1, abrufbar unter: https://courses.cit.cornell.edu/jl2545/papers/personalized_Pricing_IJIO.pdf (letzter Abruf: 25.8.2018).

Möglichkeit hatte, auf sie Einfluss zu nehmen[301] - bei Kunden auf Ablehnung stoßen, was wiederum zu Imageproblemen bei den betroffenen Unternehmen führen kann.[302]

Schließlich bergen personalisierte Preise das Risiko, dass marktstarke Plattformen diese dazu nutzen, systematisch Konkurrenten zu verdrängen oder die Etablierung etwaiger künftiger Konkurrenten (z.B. auch durch ihr größeres Datenreservoir an Kundendaten) zu erschweren.[303]

Aus Kundensicht sind personalisierte Preise bei fehlendem Preisvergleich mangels Transparenz und Kenntnis der Preispersonalisierung mit der Gefahr überhöhter Preiszahlung verbunden. Ferner besteht das Risiko, auf Grund fehlerhafter (z.B. veralteter oder fehlerhaft aufgezeichneter) Daten oder auf Grund von Falschzuordnungen durch den Algorithmus[304] individuell überhöhten, „ungerechten" Preisen ausgesetzt zu werden.[305] Überdies besteht auch die Gefahr, dass Kunden, die mit hohen Sicherheitseinstellungen surfen und auch ansonsten auf Grund ihres restriktiven Umgangs mit der Offenbarung personenbezogener Daten im Internet, keine ausreichende Datenbasis zur Bildung algorithmenbasierter persönlicher Preise „bereitstellen", von der Teilnahme am Onlinemarkt verkäuferseitig ausgeschlossen werden könnten.[306] Auch könnten bei der Preisbildung berücksichtigte persönliche Daten diskriminierend wirken, wenn ein Unternehmen etwa Geschlecht, Religionszugehörigkeit oder Alter des Kunden bei der Preisbildung berücksichtigen würde,[307] was nicht von vorneherein undenkbar ist, weil man z.B. aus dem Alter eines Kunden durchaus ggf. auf die

---

[301] *Richards/Liaukonyte/Streletskaya*, Personaliced pricing and Price fairness, Ithaka/New York, September 2015, S. 1, abrufbar unter: https://courses.cit.cornell.edu/jl2545/papers/personalized_Pricing_IJIO.pdf (letzter Abruf: 25.8.2018).

[302] *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 6, abrufbar unter: http://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_WP02_Personalisierte-Preise.pdf (letzter Abruf: 25.8.2018); *Zander-Hayat/Reisch/Steffen*, VuR 2016, 403, 406; Müller, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018).

[303] *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017.

[304] Z.B. Student wohnt in kleiner Dachstube in als „kaufkräftig" klassifiziertem Stadtviertel oder bestellt mit einem leihweise überlassenen hochpreisigen Endgerät seines Onkels.

[305] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 71, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018); *Martini*, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017 (1018).

[306] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 72, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018).

[307] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 71, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018); Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

Zahlungsbereitschaft des Kunden für bestimmte Produkte Rückschlüsse ziehen könnte. Als bedeutsames Bedenken gegenüber personalisierten Preisen wird aus Kundensicht ins Feld geführt, dass auf Grund des mit der Datenerhebung und -aufbereitung einhergehenden zunehmenden Informationsvorsprungs der Anbieterseite das Marktgleichgewicht im Vergleich zur analogen Welt einseitig stark zu Gunsten der Anbieterseite verschoben werde.[308] Dabei bewirke die Möglichkeit, mit Hilfe von Algorithmen aufgrund erhobener Daten das Käuferverhalten bis zu einem gewissen Grad vorhersehen zu können, dass die Anbieterseite bildlich gesprochen im Rahmen der Vertragsanbahnung die Gedanken der Kundenseite lesen könne,[309] was sich spezifisch für den digitalen Bereich zu einem dauerhaften strukturellen Machtgefälle verfestigen könnte.[310] Diese Problematik könnte aus Kundensicht noch dadurch verschärft werden, dass die bei der Preispersonalisierung verwendeten Kundendaten (teilweise) möglicherweise auch nicht aus dem aktuellen Surfvorgang und der bisherigen Kundenbeziehung zu dem Anbieter, sondern auch von Drittanbietern stammen können, so dass Daten zur Verwendung kommen können, mit deren Verwendung der Kunde im aktuellen Erwerbsvorgang gar nicht rechnet.[311]

Schließlich lassen die erhobenen personenbezogenen Daten den Rückschluss auf eine Notlage des Kunden z.B. aus medizinischer Sicht zu - so könnten Unternehmen personalisierte Preise für hiermit im Zusammenhang stehende Produkte (wie z.B. Medikamente oder Heil- und Hilfsmittel) sich diese Notlage missbräuchlich zunutze machen.[312]

---

[308] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 71, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018); Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[309] *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018).

[310] *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018); *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 71, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018); Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018).

[311] *Christl*, Kommerzielle Digitale Überwachung im Alltag, S. 71, abrufbar unter: http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf (letzter Abruf: 25.8.2018).

[312] Verbraucherzentrale Bundesverband e.V., Algorithmenbasierte Entscheidungsprozesse. Thesenpapier des vzbv, S. 7, abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2018/05/22/dm_17-12-07_vzbv_thesenpapier_algorithmen.pdf (letzter Abruf: 25.8.2018); *Müller*, Personalisierte Preise brauchen Regeln, abrufbar unter: http://dasnetz.online/personalisierte-preise-brauchen-regeln/ (letzter Abruf: 25.8.2018).

Ein weiterer Nachteil personalisierter Preise ist die deutliche Beschränkung der Möglichkeit des Preisvergleichs, was sich zu Lasten des freien Wettbewerbs, der auf Preistransparenz angewiesen ist, auswirken könnte.[313] Der Bedeutung des Preisvergleichs wird mit dem Preisauszeichnungsrecht Rechnung getragen. In der Preisauszeichnungsverordnung vom 18. September 1969 ist in der Gesetzesbegründung ausgeführt: „Die Preisauszeichnung dient der Preisklarheit und Preiswahrheit und sichert die Möglichkeit des Preisvergleichs. In der heutigen Zeit eines reichlichen und stark differenzierten Warenangebot kommt ihr für den Verbraucher besondere Bedeutung zu, da erst eine deutliche Preisauszeichnung dem Verbraucher die schnelle und zuverlässige Information über das preisgünstigste Angebot ermöglicht. Aber auch die gesamtwirtschaftliche Bedeutung der Preisauszeichnung kann gar nicht hoch genug veranschlagt werden. Nur der informierte Verbraucher ist in der Lage, der ihm zukommenden volkswirtschaftlichen Funktion voll gerecht zu werden und durch seine Entscheidung zur Stabilität des Preisniveaus beizutragen.“[314] Die Kriterien der Preiswahrheit und Preisklarheit werden noch heute im Preisauszeichnungsrecht in ständiger Rechtsprechung betont.[315] Auch auf europäischer Ebene wurde zuletzt durch die Richtlinie 98/6/EG zum Schutz der Verbraucher bei der Angabe der Preise der ihnen angebotenen Erzeugnisse festgelegt, dass der Verkaufspreis und der Preis je Maßeinheit anzugeben ist. Die Vorgabe trage merklich zur Verbesserung der Verbraucherinformation bei, da dies den Verbrauchern auf einfachste Weise optimale Möglichkeiten biete, die Preise von Erzeugnissen zu beurteilen und miteinander zu vergleichen und somit anhand einfacher Vergleiche fundierte Entscheidungen zu treffen.[316]

3. Stellungnahme

a. Zulässigkeit personalisierter Preise nach bisheriger Rechtslage

Grundsätzlich steht es einem Unternehmen im Rahmen einer marktwirtschaftlich orientierten Wirtschaftsordnung frei, seine Preisgestaltung in eigener Verantwortung vorzunehmen.[317] Danach ist der Einsatz personalisierter Preise als Ausdruck der Vertragsfreiheit bisher grundsätzlich erlaubt.

---

[313] *Zander-Hayat/Domurath/Groß*, Personalisierte Preise. SVRV Working Paper Nr. 2 August 2016, S. 7, abrufbar unter: http://www.svr-verbraucherfragen.de/dokumente/working-paper-personalisierte-preise/ (letzter Abruf: 25.8.2018).
[314] BAnz. 1969 Nr. 178, S. 3.
[315] Vgl. u.a. BGH, Urt. v. 4.10.2007 - I ZR 143/04, NJW 2008, 1384.
[316] Richtlinie 98/6/EG des Europäischen Parlaments und des Rates vom 16.02.1998 über den Schutz der Verbraucher bei der Angabe der Preise der ihnen angebotenen Erzeugnisse: Erwägungsgrund 6.
[317] BGH, Urt. v. 18.4.1958 – I ZR 158/56, GRUR 1958, 487 (489).

Soweit bei der Preisbildung personenbezogene Daten einbezogen werden, gelten die Anforderungen der Datenschutz-Grundverordnung einschließlich der Transparenzpflichten der Art. 13, 14 DS-GVO (s.o. unter C II).

Personalisierte Preise sind dann de lege lata verboten, wenn der Preisbildung Kriterien im Sinne des § 19 AGG zugrundeliegen. Nach dieser Norm sind, wie bereits dargestellt, unter anderem Benachteiligungen aus Gründen der Rasse, der ethnischen Herkunft, des Geschlechts oder des Alters verboten.

Ein weiteres Verbot enthält § 5 der Verordnung über Informationspflichten für Dienstleistungserbringer (DL-InfoV). Danach darf ein Dienstleistungserbringer keine Bedingungen für den Zugang zu einer Dienstleistung bekannt machen, die auf der Staatsangehörigkeit oder dem Wohnsitz des Dienstleistungsempfängers beruhende diskriminierende Bestimmungen enthalten, es sei denn, die Unterschiede bei den Zugangsbedingungen sind unmittelbar durch objektive Kriterien gerechtfertigt.[318]

Sowohl ein Verstoß gegen die Benachteiligungsverbote der §§ 19, 20 AGG als auch gegen § 5 DL-InfoV stellt darüber hinaus in Verbindung mit § 3a UWG einen wettbewerbsrechtlichen Rechtsbruch dar.[319] Personalisierte Preise sind daneben auch dann am Kartellrecht und dabei insbesondere an § 19 Abs. 2 Nr. 2 GWB zu messen, wenn sie aus einer marktbeherrschenden Stellung heraus aufgestellt werden und von denjenigen abweichen, die sich bei wirksamem Wettbewerb nach hoher Wahrscheinlichkeit ergeben würden.

b. Gesetzgeberischer Handlungsbedarf

Neben den dargelegten gesetzlichen Regelungen scheint es erwägenswert, insbesondere im Hinblick auf die Begründungen aus dem Preisauszeichnungsrecht, weiteren gesetzlichen Handlungsbedarf in Betracht zu ziehen. Dem Verbraucher sollte es auf einfache Weise möglich sein, die Preise von Erzeugnissen zu beurteilen, miteinander zu vergleichen und anhand dieses Vergleichs fundierte Entscheidungen zu treffen. Personalisierte Preise behindern diese Vergleichsmöglichkeit, insbesondere solange der Verbraucher mit ihnen nicht rechnet, und schaffen eine große Intransparenz. Sie vergrößern das Ungleichgewicht zwischen Verbrauchern und Unternehmen und öffnen der missbräuchlichen Ausnutzung von Notlagen Tür und Tor. Der bestehende Rechtsrahmen hindert dieses Ungleichgewicht nicht. Dies dürfte auch für die Datenschutz-Grundverordnung gelten. Zum einen ist diese lediglich bei der

[318] Einen Verstoß gegen dieses Verbot hat die EU-Kommission im Jahr 2014 im Hinblick auf sechs Autovermietungsfirmen festgestellt, bei denen durch automatisches Rerouting unterschiedliche Preise aufgrund des Wohnortes erhoben wurden. Die betroffenen Firmen haben ihre Preispolitik inzwischen abgeändert, vgl. Pressemitteilung der Europäischen Kommission vom 28.10.2014, „Kommission begrüßt Verbesserung für Kunden von Autovermietungsfirmen“, abrufbar unter www://europa.eu/rapid/press-release_IP-14-1209_de.htm (letzter Abruf: 25.8.2018).

[319] *Köhler*/Bornkamp/Feddersen, UWG, § 3a, Rn. 1.294.

Verarbeitung personenbezogener Daten anwendbar (s.o. unter C.II), zum anderen hat sich der datenschutzrechtliche Individualrechtsschutz bisher als lediglich begrenzt effektiv erwiesen.[320]

Als Reaktion auf dieses Ungleichgewicht hatte die 12. Verbraucherschutzministerkonferenz am 22. April 2016 in Düsseldorf beschlossen, dass allen Kunden im Onlinehandel von demselben Anbieter auch ein- und derselbe Referenzpreis angezeigt und angeboten werden sollte. Soweit Anbieter von diesem Referenzpreis abweichten, sollten Sie verpflichtet werden, Verbraucherinnen und Verbraucher über die Bedingungen für eine Abweichung vom Referenzpreis in einer nachvollziehbaren und transparenten Weise zu informieren.[321]

Dieser Vorschlag legislativen Handels erscheint jedoch zu weitgehend. Er stellt einen erheblichen Eingriff in die Vertragsfreiheit dar. Als milderes Mittel aus dem oben dargestellten Katalog der Gestaltungsmittel (s. o. Kapitel 1 D. II. 1.) kommt die Einführung einer Transparenzpflicht – in Form eines „transparenten Preisschildes“ - in Betracht. Diese verhindert nicht den Einsatz personalisierter Preise, sensibilisiert jedoch die Verbraucher im Hinblick auf bestimmte Verhaltensweisen. Die Verbraucher könnten den Kauf zum Beispiel nochmals über ein anderes Endgerät versuchen oder bei einem anderen Anbieter die Ware aufrufen. Auch steht zu erwarten, dass Verbraucher ihrerseits Technologien nutzen werden, um die für sie jeweils günstigsten erreichbaren Preise zu realisieren. Denkbar ist, dass die Verbraucher bei nutzungsdatenbasierten, individuellen Preisen ihrerseits ihre gesendeten Profildaten mithilfe von Standardsoftware manipulieren können oder die Kaufentscheidung für einen bestimmten Händler einem Agenten („Shop-Bot“) übertragen.[322] Bis die Verbraucher jedoch diesen Schritt nachvollzogen haben, wird noch Zeit vergehen. Gerade in der Zeit des technischen Übergangs ist daher eine entsprechende Transparenzpflicht angebracht. Der Eingriff ist grundrechtsschonend, wenn die Transparenzpflicht keine Details der Preisbildung umfasst.

Konkret betrachtet könnte der Gesetzgeber eine gesetzliche Verpflichtung, vorrangig auf europäischer Ebene, schaffen, wonach individualisierte Preise auf

---

[320] *Busch*, Algorithmic Accountability, S. 51, abrufbar unter http://www.abida.de/en/node/397 (letzter Abruf: 25.8.2018).

[321] Beschluss der Verbraucherschutzministerkonferenz abrufbar unter https://www.verbraucherschutzministerkonferenz.de/Beschluesse.html (letzter Abruf: 25.8.2018).

[322] *Schleusener*, Dynamisch und personalisiert: Wie entwickelt sich die Preissetzung im Online-Handel? Aus Zeitgespräch, 96. Jahrgang, Heft 12, S. 863-882, abrufbar unter www://archiv.wirtschftsdienst.eu/jahr/2016/12/dynamische-preissetzung-wer-profitiert (letzter Abruf: 25.8.2018).

allgemein zugänglichen Internet-Verkaufsseiten als solche gekennzeichnet werden müssten. Es wäre dabei ausreichend, zunächst neben dem angezeigten Preis den Hinweis „personalisierter Preis“ einzublenden. Nicht erforderlich wäre, die genauen Einzelheiten der Preisbildung darzulegen. Die gesetzliche Regelung müsste dabei einen weiten Begriff des individualisierten Preises zugrunde legen. Eine spätere Evaluierung könnte zeigen, inwieweit diese Maßnahme bereits ausreichend ist, das erkannte Gefahrenpotential personalisierter Preise einzugrenzen.

Es sollte erwogen werden, eine Missachtung der Kennzeichnungspflicht in Form des „transparenten Preisschilds“ mit Bußgeld zu bewehren.

In der Praxis könnte eine sinnvolle Verknüpfung zwischen diesen Anforderungen und den datenschutzrechtlichen Anforderungen dergestalt hergestellt werden, dass ein Button „personalisierter Preis“ verwendet wird und beim Anklicken die datenschutzrechtlichen Erläuterungen nach Art. 13, 14 DS-GVO hinterlegt sind.

F. Ergebnis

Der Einsatz algorithmischer Entscheidungsfindung darf nicht zu Erleichterungen im Rahmen des Entlastungsbeweises nach § 21 Abs. 2 S. 2 AGG führen.

Bei der Erstellung personalisierter Trefferlisten im Internet sollten die wesentlichen Kriterien des Sortieralgorithmusses offengelegt werden.

Bei der Verwendung personalisierter Preise im Rahmen von Vertragsbeziehungen im Internet sollten die Unternehmen verpflichtet werden, dem Verbraucher gegenüber die Tatsache des Einsatzes algorithmischer Entscheidungssysteme zur personalisierten Preisbildung offenzulegen, ohne weitere Details der Preisfindung preisgeben zu müssen („transparentes Preisschild“).

Kapitel 2: Gesundheitsdatenschutz

A. Vorbemerkung

Ein Blick nach China scheint wie Science Fiction. Das chinesische Start-up iCarbon sammelt Gesundheitsdaten seiner Nutzer und verspricht damit das Leid der Menschen zu reduzieren. Nach den Erkenntnissen der Biotechnik und Genetik werden Gesundheitsdaten bis hin zu DNA permanent mittels künstlicher Intelligenz ausgewertet und dem Kunden individuelle Vorschläge zu gesundheitsförderndem Verhalten gemacht. Die Daten werden direkt in den Wohnungen der Kunden erhoben, etwa durch eine Toilette mit ausfahrbarem Löffel, die Urinproben sammelt.[323]

Die technischen Möglichkeiten zur Ermittlung individueller Gesundheitsrisiken sind längst gegeben, so dass es auch in Europa einer grundsätzlichen Auseinandersetzung mit dem Thema bedarf.

In jüngster Vergangenheit ist auf dem deutschen Versicherungsmarkt zu beobachten, dass Versicherungstarife angeboten werden, bei denen der Tarif unter anderem dadurch beeinflusst werden kann, dass die Versicherten Gesundheitsdaten über Trainingseinheiten, die sie mit Fitness-Trackern aufzeichnen, per App an ein Partnerunternehmen der Versicherer übermitteln.[324] Auch durch das Erreichen von seitens des Versicherers nach durchgeführtem Gesundheitstest vorgeschlagenen Zielen kann der Tarif beeinflusst werden.[325] Bei derartigen Vertragskonstellationen können im Laufe der Zeit große Mengen an sensiblen Gesundheitsdaten übertragen und gespeichert werden. Derartige Datenübermittlungen gehen über die Erhebung von Gesundheitsdaten, die für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht erforderlich sind (§§ 19, 31, 213 VVG), weit hinaus.

Aktuell betrifft dies noch nicht Krankenversicherungen, wohl aber Risikolebens-, Unfall- und Erwerbsunfähigkeitsversicherungen sowie private Rentenversicherungen.[326] Auch eine Ausweitung auf private

[323] Handelsblatt vom 1.-3.6.2018, S. 61: Wang will's wissen – alles.
[324] Vgl. unter: https://www.generalivitality.de/vmp/aktiv_leben/fitness-tracker (letzter Abruf: 25.8.2018), daneben kann der Tarif vom Versicherten etwa auch durch Teilnahme an diversen Gesundheitschecks und -tests, Vorsorgeuntersuchungen, Impfungen sowie durch Fitness, Teilnahme an Sportveranstaltungen, gesunde Ernährung, das Erreichen vorgeschlagener Ziele und ähnlichem positiv beeinflusst werden, vgl. unter https://www.generalivitality.de/vmp/punkte_und_status/tipps_zum_punktesammeln (letzter Abruf: 25.8.2018).
[325] Vgl. unter https://www.generalivitality.de/vmp/aktiv_leben/ziele (letzter Abruf: 25.8.2018).
[326] Vgl. https://www.generali.de/vitality (letzter Abruf: 25.8.2018).

Krankenversicherungen wird aber geprüft und könnte in naher Zukunft umgesetzt werden.[327]

Während derartige Vertragsgestaltungen im Bereich der gesetzlichen Krankenversicherungen ohnehin nicht in Betracht kommen dürften,[328] wären nach derzeitiger Rechtslage im Bereich der privaten Krankenversicherung und bei sonstigen Versicherungen solche Vertragsgestaltungen (bei Einwilligung des Versicherten in die Datennutzung) grundsätzlich möglich.[329] Derartige Vertragsgestaltungen bergen aber diverse Risiken für die Gemeinschaft der Versicherten. Insbesondere könnte ein mittelbarer Zwang für alle Versicherten entstehen, hochsensible Gesundheitsdaten zu ermitteln und zu übertragen.

B. Begriffsbestimmungen

Da für die hier interessierenden Fragestellungen immer wieder die Begriffe der Gesundheitsdaten und der Fitness-Tracker bzw. „Wearables“ eine wesentliche Rolle spielen, sollen vorab diese Begrifflichkeiten geklärt werden:

I. Definition „Fitness-Tracker“

Bei Wikipedia findet sich für Fitness-Tracker folgende Definition:

„Ein Activity Tracker (auch Fitness- bzw. Gesundheits-Armband, Smart Band oder Fitness Tracker) ist ein tragbares elektronisches Gerät („Wearable“) bzw. eine Applikation zur Aufzeichnung und Versendung fitness- und gesundheitsrelevanter Daten wie etwa Laufstrecken, Energieumsatz und in manchen Fällen auch Herzschlagfrequenz oder Schlafqualität. Die Bezeichnung wird hauptsächlich für am Körper tragbare elektronische Überwachungsgeräte

---

[327] Vgl. http://versicherungsmonitor.de/2018/01/generali-mit-vitality-krankenversicherung/ sowie https://www.aerztezeitung.de/praxis_wirtschaft/w_specials/special-versicherungen/article/955825/praevention-generali-weitet-programm-vitality-pkv.html (letzter Abruf: 25.8.2018). Eine Ausweitung ist danach zum Ende des Jahres 2018 oder Anfang des Jahres 2019 beabsichtigt, wobei es aber (anders als bei der Berufsunfähigkeits- oder Risikolebensversicherung) keine Preisnachlässe für gesundheitsbewusstes Verhalten geben soll.

[328] Vgl. zu den dort vorhandenen (gesetzlich geregelten) Möglichkeiten im Einzelnen unten unter B. II.

[329] Vgl. etwa *Ortner/Daubenbüchel*, Medizinprodukte 4.0 – Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918 (2920); zu den (derzeit aber nicht überschrittenen) verfassungsrechtlich durch das informationelle Selbstbestimmungsrecht und die Menschenwürde gezogenen grundlegenden Grenzen (bei deren Überschreitung den Gesetzgeber sogar eine Pflicht zum Tätigwerden treffen würde) vgl. ausführlich *Rudkowski, Lena*, Grundrechte als Grenze von Self-Tracking-Tarifen in der Privatversicherung, in Festschrift „Der Forschung – der Lehre – der Bildung, 100 Jahre Hamburger Seminar für Versicherungswissenschaft und Versicherungswissenschaftlicher Verein in Hamburg e. V.“, 661 ff.

verwendet, welche (in vielen Fällen drahtlos) mit einem Computer oder Smartphone für die Datenerfassung über einen längeren Zeitraum synchronisiert werden. Abgesehen von diesen tragbaren Geräten gibt es auch vergleichbare Applikationen für Smartphones."[330]

Auch in der juristischen Fachliteratur wird sich dem Begriff in ähnlicher Weise genähert. Fitness-Tracker bzw. „Wearables" sammeln danach je nach Modell unterschiedliche Daten. Neben dem klassischen Schrittzähler erfassen viele Modelle die Herzfrequenz, Schlafzeit und die verbrannten Kalorien der Träger. Moderne Sportuhren verfügen über GPS-Sender; so messen sie die gelaufenen, gefahrenen oder geschwommenen Kilometer und erheben Daten über die Schrittlänge und –höhe, Bodenkontaktzeit und vieles mehr. Je nach Modell werden diese Daten automatisch oder manuell auf die Server der Anbieter geladen und dort aufbereitet. In aller Regel geben die Nutzer zudem persönliche Informationen preis wie Alter, Geschlecht, Körpergröße und Gewicht.[331] In der juristischen Fachliteratur, die sich mit dem Phänomen des „self-tracking" mittels Sportuhren und Fitness-Trackern befasst, wird konstatiert, dass es sich dabei um einen Trend handelt, der nicht nur Sportler, sondern inzwischen auch breite Gesellschaftsschichten erfasst hat.[332] Bei dem Versicherungsunternehmen Generali, das mit dem Vitality-Tarif eine Tarifstruktur anbietet, mit dem durch gesundheitsbewusstes Verhalten die Verringerung des Versicherungstarifs erreicht werden kann, werden etwa auf der Homepage diverse konkrete Apps und Tracker aufgeführt, die mit Vitality verknüpfbar sind.[333]

Vor dem Hintergrund der unterschiedlichen Funktionalitäten ist für Fitness-Tracker bzw. „Wearables" eine umfassende, wirklich einheitliche Definition daher nicht möglich. Die in Wikipedia enthaltene Beschreibung, die sich mit der Verwendung des Begriffs auch in der juristischen Literatur deckt, umreisst das Phänomen aber hinreichend klar.

---

[330] https://de.wikipedia.org/wiki/Activity_Tracker (letzter Abruf: 25.8.2018).

[331] *Dregelies, Max*, Wohin laufen meine Daten? – Datenschutz bei Sportuhren und Fitnesstrackern, VuR 2017, 256 (256); konkret nach dem einzelnen Anbietern von „Wearables" ausdifferenziert: Eberbach, Wolfram, Personalisierte Prävention: Wirkungen und Auswirkungen – Zugleich ein Plädoyer für die Solidarität mit dem Selbstbestimmungsrecht, MedR 2014, 449 (460/ 461); ähnlich: *Kopp, Reinhold/ Sokoll, Karen*, Wearables am Arbeitsplatz – Einfallstor für die Alltagsüberwachung?, NZA 2015, 1352 (1352)

[332] *Dregelies, Max*, Wohin laufen meine Daten? – Datenschutz bei Sportuhren und Fitnesstrackern, VuR 2017, 256 (256 mwN)

[333] Vgl. unter: https://www.generalivitality.de/vmp/aktiv_leben/fitness-tracker (letzter Abruf: 25.8.2018); der Erwerb mancher Geräte wird danach mit einem (derzeit) 40%igen Rabatt unterstützt.

II. Definition „Gesundheitsdaten“

Hinsichtlich des Begriffs der „Gesundheitsdaten“ enthält die Datenschutz-Grundverordnung (DS-GVO) für das Datenschutzrecht eine Legaldefinition. Danach sind „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DS-GVO). Diese Definition wird für ausfüllungsbedürftig gehalten und dabei vertreten, dass man vom Grundsatz her von einem weiten Verständnis von Gesundheitsdaten werde ausgehen müssen. Bereits die regelmäßige Ermittlung der Schrittzahl in Verbindung mit den allgemeinen Körperdaten (Alter, Größe, Gewicht) ermögliche eindeutige Rückschlüsse auf den Gesundheitszustand einer Person. Daten über Körper und Bewegung einer Person seien somit Gesundheitsdaten, so dass ein Großteil der von Sportuhren und Fitness-Trackern erhobenen Daten unter diese Definition falle.[334]

Das Versicherungsvertragsgesetz (VVG) enthält keine Legaldefinition von Gesundheitsdaten. In § 213 VVG (Erhebung personenbezogener Gesundheitsdaten bei Dritten) wird dieser Begriff aber verwendet.

In der Kommentarliteratur zum VVG wird zum Teil hinsichtlich der Definition von Gesundheitsdaten auf das Datenschutzrecht Bezug genommen.[335] Andere definieren personenbezogene Gesundheitsdaten als Informationen über Krankheiten, Beschwerden oder Störungen oder aus solchem Anlass erfolgte Behandlungen, Untersuchungen und Beratungen einschließlich ihres Ablaufs und ihres Ergebnisses, darüber hinaus aber auch Umstände, die auf ein physisches oder psychisches Leiden oder sein Fehlen schließen lassen.[336]

Vorzugswürdig erscheint es für die Zwecke des vorliegenden Berichts, eine einheitliche weite Definition von Gesundheitsdaten zu Grunde zu legen, die der in der DS-GVO enthaltenen entspricht. Soweit Vorgaben der DS-GVO zu beachten sind, ist ohnehin die dort enthaltene Legaldefinition maßgeblich. Der in der versicherungsvertragsrechtlichen Literatur zum Teil vorgenommene Verweis auf die datenschutzrechtliche Definition verhindert, dass derselbe Begriff datenschutzrechtlich und versicherungsvertragsrechtlich unterschiedlich beurteilt

---

[334] *Dregelies, Max*, Wohin laufen meine Daten? – Datenschutz bei Sportuhren und Fitnesstrackern, VuR 2017, 256 (258/259).

[335] Etwa: Bach/Moser/*Kalis*, Private Krankenversicherung, 5. Aufl. 2015, § 213 VVG Rn 40, 41 (mit zusätzlichem Hinweis darauf, dass es sich um Informationen handeln müsse, die sich auf einzelne Personen beziehen).

[336] *Langheid/Rixecker/ Rixecker*, Versicherungsvertragsgesetz, 5. Aufl. 2016, § 213 VVG Rn 9.

werden müsste, was insbesondere wegen der Überschneidungen der beiden Materien misslich wäre.

Für die hier in Rede stehenden Übertragungen von Messdaten durch Fitness-Armbänder bzw. „Wearables“ (wie etwa Herzfrequenz, Schlafzeit, verbrannten Kalorien, im Training zurückgelegte Kilometer) bedeutet dies, dass ohne weiteres umfassend von Gesundheitsdaten auszugehen ist. Gerade weil diese Daten einen Rückschluss auf den Trainingstand, die Fitness und damit die körperliche Verfassung zulassen, sind sie ja für die Versicherer von Interesse. Für diesen Bericht wird daher, soweit von Gesundheitsdaten die Rede ist, die Legaldefinition des Art. 4 Nr. 15 DS-GVO zu Grunde gelegt.

C. Stand der Diskussion in Literatur und Rechtsprechung

I. Diskussionsstand im Hinblick auf private Versicherungen

In der Literatur wird die Frage aufgeworfen, ob mit der Zurverfügungstellung individueller Gesundheitsdaten zwecks Tarifersparnis das Grundprinzip von Versicherungen als eine Institution zur Übernahme von Risiken des Lebens durch einen Ausgleich im Versicherungskollektiv und das gegenseitige Solidarprinzip in Frage gestellt wird. Schließlich erfolge diese neue Tarifkalkulation überwiegend auf der Basis rein individuellen Verhaltens. Daher stelle sich die Frage, ob künftig Versicherungen zu akzeptablen Preisen nur noch für diejenigen möglich sein werden, die Kontrollprozeduren für sich akzeptierten, während die anderen, die dazu nicht bereit seien, deshalb auf kaum bezahlbare Tarife verwiesen würden oder gar keine Risikodeckung mehr erhalten würden. Hohe Schadensquoten seien schließlich für Unternehmen auf lange Sicht unwirtschaftlich und schon aus marktwirtschaftlichen Erwägungen würden immer mehr Unternehmen dazu übergehen, vermeintlich risikobehaftete Kunden auszusortieren. Insoweit wird davor gewarnt, dass die Individualisierung von Versicherungsprodukten zu einer Erosion des Versicherungssolidarprinzips führen würde.[337] Bei der Jahrestagung des Deutschen Ethikrates im Jahr 2015 wurde insoweit bereits prägnant formuliert: „Was der Prämienvorteil für den einen ist, ist der Präminennachteil für den anderen“.[338]

Aus verfassungsrechtlicher Sicht wird darauf hingewiesen, dass Versicherungsverträge, die Prämien (auch) anhand von Self-Tracking-Daten berechnen, sowohl die Grundrechte der Versicherungsnehmer und Vertragsinteressenten berühren, die das Self-Tracking oder die Preisgabe von

[337] *Heinz,* Digitaler „Datenstriptease“ – Die Erhebung von Kundendaten darf Solidarprinzip der Versicherungen nicht verletzen, VW 10/2016, 14.
[338] Zitiert in Sonja *Schulz,* Der Mensch im Datenstrom, zm 105 vom 1.7.2015, 1488 (1492), zitierte Äußerung von Christiane Woppen vom Deutschen Ethikrat.

Self-Tracking-Daten ganz oder wenigstens in einem bestimmten Umfang ablehnen, als auch die derjenigen Versicherungsnehmer, die in eine Verwendung von Self-Tracking-Daten für Zwecke der Versicherung vollumfänglich einwilligen möchten.[339] Hinsichtlich der zum Self-Tracking bereiten Versicherungsnehmer wird dabei wegen der erfolgten Einwilligung eine Verletzung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) nicht gesehen. Die Grenze für Einwilligungen stellt danach die Verletzung der Menschenwürde (Art. 1 Abs. 1 GG) dar, da die Menschenwürde für den Einzelnen unverzichtbar und zudem objektiv zu bestimmen ist. Insoweit wird vertreten, dass sich eine Verletzung der Menschenwürde durch Herabwürdigung des Versicherungsnehmers zum bloßen Objekt daraus ergeben könnte, dass der Umfang der zu offenbarenden Daten so groß sei, dass sie nur durch eine Totalüberwachung generiert werden könnten. Der Versicherungsnehmer werde dann – sei es auch mit seinem Einverständnis – zum entmenschlichten „Datenlieferanten“. Eine Totalüberwachung rund um die Uhr wird daher, auch wenn sie nur auf einzelne Vital- oder Verhaltensdaten bezogen sei, als unzulässig angesehen, ebenso wie das Recht des Versicherers, nach Belieben „Stichproben“ beim Versicherungsnehmer zu nehmen, weil letzteres faktisch auch eine nahezu lückenlose Überwachung ermögliche. Zudem müsse der Versicherungsnehmer frei über die Durchführung der einzelnen Datenerhebungen und -übertragungen entscheiden können; verdeckte Überwachungen seien daher unzulässig. Zudem wird eine Verletzung der Menschenwürde in Fällen angenommen, in denen über das Self-Tracking in größerem Umfang Einfluss auf sein persönliches Verhalten genommen wird. Die Auferlegung von Verhaltenspflichten (etwa um die Aussagekraft der Self-Tracking-Daten zu erhöhen) müsse die Ausnahme sein, der Versicherungsnehmer dürfe nicht zur „Marionette“ des Versicherers werden. Erst recht könne Verhaltensoptimierung nicht Gegenstand des Versicherungsvertrages sein, bereits die Pflicht des Versicherungsnehmers zur Information des Versicherers, ob einer Empfehlung gefolgt wurde, müsse unzulässig sein.[340]

Diejenigen Versicherungsnehmer, die nicht zum Self-Tracking bereit sind, werden grundsätzlich als durch das im Datenschutzrecht vorgesehene Einwilligungserfordernis ausreichend geschützt angesehen. Eine Betroffenheit im allgemeinen Persönlichkeitsrecht wird aber angenommen, wenn der Grundrechtsträger vor der Wahl stehe, auf die Inanspruchnahme der gewünschten Leistung zu verzichten oder seine personenbezogenen Daten preiszugeben. Ein

[339] *Rudkowski*, Grundrechte als Grenze von Self-Tracking-Tarifen in der Privatversicherung, in Festschrift „Der Forschung – der Lehre – der Bildung, 100 Jahre Hamburger Seminar für Versicherungswissenschaft und Versicherungswissenschaftlicher Verein in Hamburg e. V.“, 661 (662).

[340] *Rudkowski*, Grundrechte als Grenze von Self-Tracking-Tarifen in der Privatversicherung, in Festschrift „Der Forschung – der Lehre – der Bildung, 100 Jahre Hamburger Seminar für Versicherungswissenschaft und Versicherungswissenschaftlicher Verein in Hamburg e. V.“, 661 (663 bis 669).

solcher Druck könne insbesondere wirtschaftlicher Natur sein, etwa wenn die Prämiendifferenz zwischen Tarifen mit und ohne Self-Tracking so groß wäre, dass es bei wirtschaftlicher Betrachtung grob unvernünftig wäre, keinen Self-Tracking-Tarif zu wählen oder auch wenn die Prämie im herkömmlichen Tarif von einem Durchschnittsverdienst nicht mehr in vertretbarer Weise bestritten werden könne. Die Entscheidung zur Offenlegung personenbezogener Daten sei in einem solchen Fall keine freie mehr. Als Voraussetzung für den Eintritt einer solchen Konstellation wird indes eine Durchdringung des Marktes mit Self-Tracking-Tarifen angesehen, bei der Personen mit „guten" Risiken vorwiegend Self-Tracking-Tarife wählten, so dass in den übrigen Tarifen Personen mit ungünstigen Risiken zurückblieben, die dann höhere Prämien zu zahlen hätten. Eine solche Marktlage sei aber derzeit nicht gegeben.[341] Insoweit wird vertreten, dass bei Eintreten einer solchen Konstellation Pflichten des Staates zum Schutz des Rechts auf informationelle Selbstbestimmung eingreifen würden, die es dem Gesetzgeber und den Gerichten gebieten würden, dafür Sorge zu tragen, dass die Gewährleistung des informationellen Selbstschutzes gewahrt bleibe. Für eine verhältnismäßige und damit interessengerechte Regelung hätte der Gesetzgeber zu berücksichtigen, dass die risikogerechte Kalkulation nach dem Gesetz der großen Zahl charakteristisch für die Privatversicherung sei und eine Abkopplung des Versicherungsschutzes vom Risiko sich nur rechtfertigen lasse, wenn ein existentielles Interesse der Begünstigten am Zugang zur Versicherungsleistung vorliege. Insoweit sei aber auch in eine Abwägung einzubeziehen, dass auch bei Einschränkung der Verwertung von Self-Tracking-Daten risikoadäquate Kalkulation nicht unmöglich werde (da bereits vor dem Aufkommen von Self-Tracking risikogerecht kalkuliert wurde) und dass Personen, die sich weigerten, am Self-Tracking teilzunehmen, im Ergebnis letztlich der Zugang zum Versicherungsmarkt verschlossen bleibe. Diesem faktischen Ausschluss müssten nicht einmal zwingend schlechte Risiken zugrunde liegen, sondern gegebenenfalls lediglich der Wunsch, ihre personenbezogenen Daten vertraulich halten zu wollen.[342]

Im Hinblick auf Selbstüberwachung und genormtem Präventionsverhalten mittels Fitness-Trackern bzw. Wearables wird zudem darauf hingewiesen, dass sich immer wieder auch hochgelobte, wissenschaftlich fundierte Standards später als zweifelhaft oder sogar als falsch erwiesen, wenn noch neuere Erkenntnisse ihnen

[341] *Rudkowski*, Grundrechte als Grenze von Self-Tracking-Tarifen in der Privatversicherung, in Festschrift „Der Forschung – der Lehre – der Bildung, 100 Jahre Hamburger Seminar für Versicherungswissenschaft und Versicherungswissenschaftlicher Verein in Hamburg e. V.", 661 (669 bis 670).

[342] *Rudkowski*, Grundrechte als Grenze von Self-Tracking-Tarifen in der Privatversicherung, in Festschrift „Der Forschung – der Lehre – der Bildung, 100 Jahre Hamburger Seminar für Versicherungswissenschaft und Versicherungswissenschaftlicher Verein in Hamburg e. V.", 661 (671 bis 672).

widersprächen.[343] Zudem wird darauf hingewiesen, dass das informationelle Selbstbestimmungsrecht aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG das Recht umfasse, Lebensziele, auch soweit sie die Gesundheit berührten, selbst zu bestimmen und danach zu leben; ein Druck, die Lebensführung nach Gesundheitsnormen – nach Bauchumfang, Kalorienzahl und täglich gelaufenen Metern – zu richten, sei damit unvereinbar.[344]

Aus dem Blickwinkel des Datenschutzrechts wird darauf hingewiesen, dass je nach Art und Umfang der Anwendung die Gefahr des Kontrollverlusts des Einzelnen über seine personenbezogenen Daten bestehe.[345]

Allgemein wird im Hinblick auf Big Data-Auswertungen im Gesundheitswesen angemahnt, neben den positiven Möglichkeiten auch die damit einhergehenden Gefahren zu berücksichtigen, da es auch handfeste wirtschaftliche Interessen an Gesundheitsdaten gebe. Wie viel Alkohol getrunken, wie viele Zigaretten am Tag geraucht werden oder ob und wie Sport getrieben werde, sei nicht nur für den Hausarzt von Interesse, sondern wecke auch Begehrlichkeiten bei der Versicherungswirtschaft. Diese könnten die Höhe der Versicherungsprämie an einen anhand der Gesundheitsdaten errechneten Score knüpfen. Bisher werde zwar nur der umgekehrte Weg beschritten, indem Bonuspunkte oder Beitragsreduktionen für in den Bonusprogrammen genanntes Verhalten angeboten werde. Vor dem Hintergrund der wirtschaftlichen Interessen und der Möglichkeiten von Big Data-Analysen bestehe jedoch eine Diskriminierungsgefahr.[346]

Es wird im Hinblick auf das Sammeln von Gesundheitsdaten mit Fitness-Trackern und die Möglichkeit der Einführung von Tarifen, die ein gesundheitsbewusstes Verhalten belohnen, aber auch auf die Chancen und Vorteile hingewiesen. Insoweit wird darauf verwiesen, dass der „Lifestyle“ ein großer Kostentreiber im deutschen Gesundheitswesen sei und dramatische Auswirkungen auf chronische Erkrankungen wie Diabetes mellitus Typ II, Adipositas oder Herz-Kreislauf-Erkrankungen habe – Ziel der Krankenversicherer müsse es sein, den Versicherten zu einer nachhaltigen Verhaltensänderung und damit einem gesünderen Lebensstil zu motivieren.[347] Aber auch diejenigen, die diese

---

[343] *Eberbach, Wolfram*, Personalisierte Prävention: Wirkungen und Auswirkungen – Zugleich ein Plädoyer für die Solidarität mit dem Selbstbestimmungsrecht, MedR 2014, 449 (461 mit diversen Beispielen auf Seiten 461-463).
[344] *Eberbach, Wolfram*, Personalisierte Prävention: Wirkungen und Auswirkungen – Zugleich ein Plädoyer für die Solidarität mit dem Selbstbestimmungsrecht, MedR 2014, 449 (464).
[345] *Kopp, Reinhold/ Sokoll, Karen*, Wearables am Arbeitsplatz – Einfallstor für die Alltagsüberwachung?, NZA 2015, 1352 (1353).
[346] *Becker/Schwab*, Big Data im Gesundheitswesen – Datenschutzrechtliche Zulässigkeit und Lösungsansätze, ZD 2015, 151 (152).
[347] *Braun, Michael*; Nürnberg, Volker; Verhaltensbedingte Versicherungstarife – innovative E-Health-Initiative oder Ausstieg aus der Solidargemeinschaft?, G + S 1/2015, 70 (72).

Möglichkeiten und Chancen betonen, verweisen auf die Gefahr der Selektion von Versichertenbeständen, wenn alle Versicherten, die laut Fitness-Tracker gesundheitsbewusst leben, aus der Grundgesamtheit selektiert würden und einen separaten Tarif erhielten.[348] Zudem warnen auch sie vor dem Risiko, dass Daten in die falschen Hände geraten könnten und davor, dass die sensiblen Daten in Ländern gespeichert werden könnten, wo weniger strenge Datenschutzrichtlinien gelten würden als in Europa (wie etwa in den USA).[349] Aber auch die Krankenversicherer müssten vor möglichem Missbrauch geschützt werden, etwa wenn das Armband an einen (sportlicheren) Dritten gegeben werde.[350]

II. Diskussionsstand/ übertragbare Argumentationen im Hinblick auf gesetzliche Krankenversicherungen

Für die gesetzliche Krankenversicherung existiert bereits seit längerem eine konkrete gesetzliche Regelung zur Frage der Berücksichtigung von gesundheitsbewusstem Verhalten. Wegen der Nähe zu den hier interessierenden privaten Versicherungen erscheint es sinnvoll, die bestehenden Regelungen zur gesetzlichen Krankenversicherung kurz zu analysieren. Die am 1. Januar 2000 in Kraft getretene und mit Wirkung vom 25. Juli 2015 neu gefasste[351] Vorschrift des § 65a des Fünften Buchs Sozialgesetzbuch (SGB V) regelt, wann ein Bonus für gesundheitsbewusstes Verhalten gewährt werden kann. Die Vorschrift lautet:

„(1) Die Krankenkasse soll in ihrer Satzung bestimmen, unter welchen Voraussetzungen Versicherte, die

1. regelmäßig Leistungen zur Erfassung von gesundheitlichen Risiken und Früherkennung von Krankheiten nach den §§ 25 und 26 in Anspruch nehmen,
2. Leistungen für Schutzimpfungen nach § 20i in Anspruch nehmen oder
3. regelmäßig Leistungen der Krankenkassen zur verhaltensbezogenen Prävention nach § 20 Absatz 5 in Anspruch nehmen oder an vergleichbaren, qualitätsgesicherten Angeboten zur Förderung eines gesundheitsbewussten Verhaltens teilnehmen,

Anspruch auf einen Bonus haben, der zusätzlich zu der in § 62 Absatz 1 Satz 2 genannten abgesenkten Belastungsgrenze zu gewähren ist.

---

[348] *Braun, Michael*; Nürnberg, Volker; Verhaltensbedingte Versicherungstarife – innovative E-Health-Initiative oder Ausstieg aus der Solidargemeinschaft?, G + S 1/2015, 70 (73).
[349] *Braun, Michael*; Nürnberg, Volker; Verhaltensbedingte Versicherungstarife – innovative E-Health-Initiative oder Ausstieg aus der Solidargemeinschaft?, G + S 1/2015, 70 (74).
[350] *Braun, Michael*, Nürnberg, Volker; Verhaltensbedingte Versicherungstarife – innovative E-Health-Initiative oder Ausstieg aus der Solidargemeinschaft?, G + S 1/2015, 70 (74/75).
[351] Bei der Neufassung wurden insbesondere die Kann-Regelungen durch Soll-Regelungen ersetzt (vgl. dazu etwa juris-PK-SGB V/*Koch*, § 65a Rn 1).

(2) Die Krankenkasse soll in ihrer Satzung auch vorsehen, dass bei Maßnahmen zur betrieblichen Gesundheitsförderung durch Arbeitgeber sowohl der Arbeitgeber als auch die teilnehmenden Versicherten einen Bonus erhalten.

(3) Die Aufwendungen für Maßnahmen nach Absatz 1 müssen mittelfristig aus Einsparungen und Effizienzsteigerungen, die durch diese Maßnahmen erzielt werden, finanziert werden. Die Krankenkassen haben regelmäßig, mindestens alle drei Jahre, über diese Einsparungen gegenüber der zuständigen Aufsichtsbehörde Rechenschaft abzulegen. Werden keine Einsparungen erzielt, dürfen keine Boni für die entsprechenden Versorgungsformen gewährt werden."

Zweck der in Absatz 1 dieser Norm enthaltenen Ermächtigung an die gesetzlichen Krankenkassen ist es, ökonomische Anreize zu gesundheitsbewusstem Verhalten zu schaffen, aber auch, die Wirtschaftlichkeit der gesetzlichen Krankenversicherungen durch Einsparungen und Effizienzsteigerungen zu fördern (Umsetzung des Wirtschaftlichkeitsgebots des § 12 SGB V).[352] § 65a Abs. 1 SGB V enthält die Ermächtigung und Verpflichtung der gesetzlichen Krankenkassen, in der Satzung zu bestimmen, unter welchen Voraussetzungen Versicherte einen Anspruch auf einen Bonus haben.[353] Die Bonusgewährung muss an die Inanspruchnahme von Leistungen zur Früherkennung bereits eingetretener Krankheiten (Gesundheitscheck, Krebsvorsorgeuntersuchungen, Mammographie-Screening, Kinder- und Jungenduntersuchungen, zahnärztliche Vorsorgeuntersuchungen), welche der Sekundärprävention zuzuordnen sind oder an Leistungen zur primären verhaltensbezogenen Prävention (Verhinderung und Verminderung von Krankheitsrisiken, § 20 Abs. 1 S. 1 SGB V) anknüpfen. Letztere sollen gem. § 20 Abs. 1 S. 2 SGB V insbesondere einen Beitrag zur Verminderung sozial bedingter sowie geschlechtsbezogener Ungleichheit von Gesundheitschancen leisten. Gleichgestellt werden vergleichbare qualitätsgesicherte Angebote zur Förderung eines gesundheitsbewussten Verhaltens (etwa Erreichung des Deutschen Sportabzeichens oder qualitätsgesicherte Bewegungsangebote in Sport- oder Fitnessstudios mit qualifizierten Trainern).

Ob damit auch die Nutzung von sog. Fitness-Apps erfasst ist, lässt die Gesetzesbegründung offen.[354] Vom Bundesversicherungsamt wurde dies mit der

[352] Hauck-Noftz/*Leopold*, SGB V, § 65a Rn 8; Kasseler Kommentar Sozialversicherungsrecht/ *Roters*, SGB V § 65a Rn 2; BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 1; juris-PK-SGB V/*Koch*, § 65a Rn 14.
[353] Kasseler Kommentar Sozialversicherungsrecht/*Roters*, SGB V § 65a Rn 3.
[354] BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 3; vgl. auch Hauck-Noftz/*Leopold*, SGB V, § 65a Rn 13-15.

Begründung verneint, dass sportliche Betätigungen nur dann als qualitätsgesicherte Maßnahmen eingestuft werden können, wenn diese nachweisbar unter fachlicher Anleitung erfolgten, woran es bei der Sammlung von Daten durch Fitness-Apps fehle. Das Bundesversicherungsamt verweist zudem auf das Missbrauchsrisiko, das mangels Kontrolle, ob die sportlichen Aktivitäten vom Versicherten tatsächlich selbst erbracht wurden, bestehe, sowie auf erhebliche datenschutzrechtliche Bedenken.[355] Auch in der Literatur wird es überwiegend unter Verweis auf die Argumentation des Bundesversicherungsamtes abgelehnt, Fitness-Apps unter § 65a SGB V zu subsummieren.[356] Vereinzelt wird in der Literatur die Aufnahme von Fitness-Apps bei den Bonusprogrammen gesetzlicher Krankenversicherer nach teleologischer Auslegung von § 65a SGB V hingegen für zulässig gehalten, da, wenn nicht auch Daten über die private Lebensgestaltung des Versicherten erhoben und verarbeitet werden dürften, die Erreichung des Ziels von Bonusprogrammen, eine effektive Prävention zu leisten, unmöglich gemacht werde.[357] In der Praxis hat allerdings die Barmer GEK ein entsprechendes Programm beendet.[358] Auch ganz allgemein wird in der Kommentarliteratur ausgeführt, dass die Bonusgewährung zur Vermeidung von Missbrauch von der Vorlage eines kontrollierbaren Nachweises über die regelmäßige Teilnahme abhängig gemacht werden muss, während andererseits keine weitergehenden Daten, etwa über die private Lebensführung des Versicherten, erhoben werden dürfen.[359] Dies spricht deutlich dagegen, dass die Datenübertragung mittels Fitness-Apps im Rahmen von Bonusprogrammen gem. § 65a SGB V in der gesetzlichen Krankenkasse zulässig ist. Insgesamt wird man daher festhalten können, dass derartige Konzepte nach der derzeitigen Rechtslage bei gesetzlichen Krankenkassen nicht möglich sind und auch praktisch keine Rolle spielen.

Welche Art von Bonus oder Gutschrift die Satzung vorsieht, steht im Ermessen der Krankenkassen. Diese dürfen aber die Boni weder entgegen der gesetzlichen Zielrichtung der Gesundheitsförderung als bloße Werbemaßnahme ausgestalten, noch diese mit zweckwidrigen Auflagen und Voraussetzungen versehen. Möglich sind Sach- oder Geldprämien wie auch die Befreiung von gesetzlichen

---

[355] www.bundesversicherungsamt.de, Tätigkeitsbericht 2014 S. 22,23; dieser Kritik zustimmend: BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 3; ebenfalls kritisch: Kasseler Kommentar Sozialversicherungsrecht/*Roters*, SGB V § 65a Rn 4.

[356] BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 3; ebenfalls kritisch: Kasseler Kommentar Sozialversicherungsrecht/*Roters*, SGB V § 65a Rn 4.

[357] *Brönneke, Jan Benedikt/Kipker, Dennis-Kenji*, Fitness-Apps in Bonusprogrammen gesetzlicher Krankenversicherungen – Sozial- und datenschutzrechtliche Anforderungen, Gesundheitsrecht 4/2015, 211 (214 und 215/216 (Fazit und Ausblick)).

[358] Vgl. BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 3 mwN.

[359] BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 4 unter Verweis auf die Gesetzesbegründung (BT-Drs. 15/1525, 95).

Zuzahlungen.[360] Zweifelhaft ist hingegen, ob auch ein Bonus in Form eines Beitragsnachlasses vorgesehen werden könnte, schon da ein Beitragsnachlass grundsätzlich nur für diejenigen Versicherten in Betracht käme, die Beiträge zu entrichten hätten, also die Mitglieder der Krankenkasse, so dass damit alle übrigen Versicherten (etwa Familienversicherte nach § 10 SGB V) ausgeschlossen wären.[361] Bei der Nutzung von Gesundheitsdaten für Bonusprogramme muss aber in jedem Fall das Solidarprinzip der gesetzlichen Krankenversicherung berücksichtigt werden; Personen, die aus medizinischen Gründen nicht in gleichem Maß an gesundheitsförderlichen Aktivitäten teilnehmen können, dürfen keinen Nachteil haben, es muss stets der Grundsatz der Gleichbehandlung gelten.[362]

Wegen dieses Solidarprinzips der gesetzlichen Krankenversicherung dürfte dort, selbst für den Fall, dass man Beitragsnachlässe unter § 65a SGB V subsummieren würde, kein mittelbarer Zwang drohen, da Ausgestaltungen, die einen derartigen Zwang begründen könnten (gravierende Tarifvergünstigungen für Gesundheitsbewusste, die bereit sind, ihre Trainingsdaten zu übertragen) bereits gegen das Solidarprinzip (das in § 1 S. 1 SGB V verankert ist[363]), verstoßen würde.

Nach alldem besteht im Rahmen der gesetzlichen Krankenversicherung bereits seit längerem ein gesetzlich geregeltes System, mit dem gesundheitsbewusstes Verhalten gefördert wird, ohne dass massenhaft sensible Gesundheitsdaten über Fitness-Armbänder übertragen würden oder der Versicherungstarif selbst zur Disposition stehen und eine Benachteiligung Dritter drohen würde. Bonusprogramme werden im Übrigen bereits derzeit auch von privaten Krankenversicherungen angeboten.[364]

III. Zu berücksichtigende bzw. übertragbare Rechtsprechung des Bundesverfassungsgerichts

Bezüglich Vertragsgestaltungen, bei denen Versicherte sich verpflichten, persönliche Daten an den Versicherer zu übermitteln, stellt sich insbesondere die

---

[360] Kasseler Kommentar Sozialversicherungsrecht/*Roters*, SGB V § 65a Rn 6; BeckOK Sozialrecht/*Scholz*, SGB V § 65a Rn 5; Hauck-Noftz/*Leopold*, SGB V, § 65a Rn 21.

[361] Insoweit zweifelnd: Hauck-Noftz/*Leopold*, SGB V, § 65a Rn 23 mwN, der dies i. E. zwar für möglich hält, aber wegen der Bedenken hiervon abrät.

[362] *Braun, Michael; Nürnberg, Volker*; Verhaltensbedingte Versicherungstarife – innovative E-Health-Initiative oder Ausstieg aus der Solidargemeinschaft?, G + S 1/2015, 70 (73).

[363] Vgl. hierzu ausführlich Hauck-Noftz/*Noftz*, SGB V, § 1 Rn 36 ff.

[364] Vgl. T*öpfer, Armin/Opitz, Frank*, Bedeutung und Einfluss von Bonusprogrammen, Welt der Krankenversicherung 5/2017, 110 (111), wonach in aller Regel alle Kassen ihren Versicherten inzwischen Bonusprogramme anbieten.

Frage nach einer möglichen Verletzung des informationellen Selbstbestimmungsrechts. Nach der Rechtsprechung des Bundesverfassungsgerichts gibt das Recht auf informationelle Selbstbestimmung dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Es flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt. Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann.[365] Die mit dem Recht auf informationelle Selbstbestimmung abzuwehrenden Persönlichkeitsgefährdungen ergeben sich aus den vielfältigen Möglichkeiten des Staates und gegebenenfalls auch privater Akteure zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Vor allem mittels elektronischer Datenverarbeitung können aus solchen Informationen weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können.[366]

Das Bundesverfassungsgericht hat sich bereits in diversen Fällen mit der Wirksamkeit von Klauseln in Versicherungsverträgen auseinandergesetzt, die Auswirkungen auf das informationelle Selbstbestimmungsrecht haben. Die tragenden Grundsätze dieser Entscheidungen enthalten grundsätzliche Wertungen, die auch für die Frage der Übertragung von Gesundheitsdaten zu Zwecken der Tarifbestimmung relevant sind.

Das Bundesverfassungsgericht führt insoweit in ständiger Rechtsprechung aus, dass es zwar dem Einzelnen frei stehe, Daten anderen gegenüber zu offenbaren. Sei jedoch ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht habe, dass er den Vertragsinhalt faktisch einseitig bestimmen könne, sei es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehre. Eine solche einseitige Bestimmungsmacht eines Vertragspartners könne sich auch daraus ergeben, dass die von dem überlegenen Vertragspartner angebotene Leistung für den anderen Partner zur Sicherung seiner persönlichen Lebensverhältnisse von so erheblicher Bedeutung sei, dass die denkbare Alternative, zur Vermeidung einer zu weitgehenden Preisgabe persönlicher Informationen von einem Vertragsschluss

[365] BVerfG, Urt. v. 27.2.2008 (Online-Durchsuchung) - 1 BvR 370/07; 1 BvR 595/07, Juris Rn 198 mwN; BVerfG, Beschl. v. 24.1.2012 - Az. 1 BvR 1299/05, Juris Rn 122.
[366] BVerfG, Urt. v. 27.2.2008 (Online-Durchsuchung) - Az. 1 BvR 370/07; 1 BvR 595/07, Juris Rn 199 mwN.

ganz abzusehen, für ihn unzumutbar sei. Seien in einem solchen Fall die Vertragsbedingungen in dem Punkt, der für die Gewährleistung informationellen Selbstschutzes von Bedeutung sei, zugleich praktisch nicht verhandelbar, so verlange die aus dem allgemeinen Persönlichkeitsrecht folgende Schutzpflicht eine gerichtliche Überprüfung, ob das Geheimhaltungsinteresse des unterlegenen Teils dem Offenbarungsinteresse des überlegenen Teils angemessen zugeordnet wurde. Dazu seien die gegenläufigen Belange einander im Rahmen einer umfassenden Abwägung gegenüberzustellen.[367] In diesem Zusammenhang hat das Bundesverfassungsgericht auch wiederholt betont, dass die Vertragsbedingungen der Versicherer praktisch nicht verhandelbar sind.[368]

Unter Anwendung dieser Grundsätze hat das Bundesverfassungsgericht verschiedene klagabweisende Urteile, die gegenüber Versicherungsnehmern ergangen waren, welche sich etwa geweigert hatten, umfangreiche Schweigepflichtentbindungserklärungen abzugeben, aufgehoben. Es hat die Verfahren an die Instanzgerichte zurückverwiesen und zum Teil auch dem Gesetzgeber aufgegeben, Regelungen zu treffen, um den Schutz der Betroffenen zu gewährleisten. Dies betraf etwa vorgedruckte Schweigepflichtentbindungserklärungen im Rahmen einer Berufsunfähigkeitsversicherung[369] sowie im Rahmen eines Lebensversicherungsvertrages mit Berufsunfähigkeitszusatzversicherung[370] und die Berechnung des Schlussüberschusses bei kapitalbildenden Lebensversicherungen.[371]

Aus diesen Rechtsprechungsgrundsätzen des Bundesverfassungsgerichts lässt sich für die hier in Rede stehenden Sachverhalte schließen, dass es Versicherten in Bereichen, in denen sie zur Sicherung ihrer persönlichen Lebensverhältnisse auf eine Versicherung angewiesen sind, möglich sein muss, Versicherungen zu tragbaren Konditionen abzuschließen, ohne dass sie sich verpflichten müssen, dauerhaft hochsensible Gesundheitsdaten über ihren Fitnesszustand zu ermitteln und einem Partnerunternehmen des Versicherers zu übermitteln. Für den Bereich der Krankenversicherung, auf die wegen ihrer elementaren Bedeutung jedermann in ganz besonderer Weise angewiesen ist, dürfte die Prämisse des Bundesverfassungsgerichts, dass es unzumutbar für einen Versicherungsnehmer wäre, zur Vermeidung einer zu weitgehenden Preisgabe persönlicher

[367] BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn 30-32 (juris); BVerfG Beschl. v. 17.7.2013 - 1 BvR 3167/08, Rn 20, 21 (juris); vgl. auch BVerfG, Urt. v. 26.7.2005 - 1 BvR 80/95 Rn 61, 62 (juris).
[368] BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn 36 mwN (juris); BVerfG, Urt. v. 26.7.2005 - 1 BvR 80/95 Rn 77 (juris); BVerfG, Beschl. v. 17.7.2013 - 1 BvR 3167/08, Rn 25 – bezüglich datenschutzrechtlicher Konditionen – (juris).
[369] BVerfG, Beschl. v. 17.7.2013 - 1 BvR 3167/08, Rn 2, 4, 31 (juris).
[370] BVerfG, Beschl. v. 23.10.2006 - 1 BvR 2027/02, Rn 2, 8; 59 (juris).
[371] BVerfG, Urt. v. 26.7.2005 - 1 BvR 80/95 Leitsatz und Rn 2ff., 98, 99 (juris).

Informationen von einem Vertragsschluss ganz abzusehen, in ganz besonderer Weise gelten.

Würden also Versicherungstarife bei der privaten Krankenversicherung eingeführt, bei denen die Beitragshöhe erheblich davon beeinflusst wird, dass in großem Umfang sensible Gesundheitsdaten übermittelt werden (und damit auch der aktuelle Fitnessstand und gegebenenfalls das Erreichen von Fitnesszielen belegt wird), und würden sich diese Tarife durchsetzen, so dass sich der Abschluss einer Krankenversicherung ohne Übernahme der Verpflichtung der Übertragung von Gesundheitsdaten als unverhältnismäßig teuer darstellen würde, so dürfte angesichts der bestehenden Rechtsprechung des Bundesverfassungsgerichts hier eine Schutzpflicht des Staates eingreifen, damit kein faktischer Zwang zur Preisgabe dieser sensiblen Daten entsteht. In der derzeitigen Situation entspringt hieraus keine Handlungspflicht des Staates, da derartige Tarife bei der Krankenversicherung (noch) nicht angeboten werden und daher unmittelbar auch keine Auswirkungen für Versicherungsnehmer drohen, die den oben dargestellten entsprechen würden.

IV. Europarechtliche Zulässigkeit einschränkender Regelungen im Hinblick auf die Datenschutz-Grundverordnung

Würde man, etwa im Versicherungsvertragsgesetz, Regelungen treffen, die zum Schutz der Betroffenen Vertragsgestaltungen einschränken oder untersagen, bei denen sich der Versicherte verpflichtet, permanent Gesundheitsdaten an ein Partnerunternehmen des Versicherers zu übermitteln, stellt sich die Frage, ob dies im Hinblick auf die Datenschutz-Grundverordnung zulässig ist. Schließlich würde hier eine Regelung getroffen, die eine vertragliche Vereinbarung über die Weitergabe personenbezogener Daten betrifft, also in den Anwendungsbereich der DS-GVO fällt, die diese Fragen grundsätzlich abschließend regelt. Modifikationen der durch die DS-GVO vorgegebenen Regelungen durch die einzelnen Mitgliedstaaten sind grundsätzlich untersagt.[372] Eigenständige nationale Regelungen sind indes zulässig, sofern die DS-GVO dies in Öffnungsklauseln vorsieht. Eine derartige allgemeine Öffnungsklausel ist aber in Art. 9 Abs. 4 DS-GVO enthalten[373], die lautet:

„Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist."

[372] Gola, Peter/*Gola*, DS-GVO Kommentar, 2017, Einleitung Rn 15.
[373] Vgl. dazu auch Gola, Peter/*Schulz*, DS-GVO Kommentar, 2017, Art. 9 Rn 37.

Da vorliegend gerade die Verarbeitung von Gesundheitsdaten in Rede steht, greift die Öffnungsklausel des Art. 9 Abs. 4 DS-GVO ein und eine beschränkende Regelung im VVG wäre möglich.

D. Stellungnahme

In der gegenwärtigen Situation dürfte keine akute Pflicht des Staates zum Eingreifen anzunehmen sein. Im Hinblick auf das informationelle Selbstbestimmungsrecht der Versicherungsnehmer, die ihre Gesundheitsdaten nicht preisgeben wollen, gilt, dass entsprechende Vertragsgestaltungen noch die Ausnahme sind und bei der besonders wichtigen Krankenversicherung überhaupt noch nicht angeboten werden. Daher existieren problemlos Alternativen und ein mittelbarer Zwang zur Preisgabe derartiger Daten besteht derzeit nicht.

Soweit in der Literatur zum Teil vertreten wird, dass eine Verletzung der Menschenwürde vorliege, wenn Daten in einem so großen Umfang zu offenbaren seien, dass sie nur durch eine Totalüberwachung generiert werden könnten, so dass der Versicherungsnehmer zu einem entmenschlichten „Datenlieferanten" werde,[374] vermag sich hieraus jedenfalls derzeit ebenfalls keine Handlungspflicht des Staates abzuleiten. Eine derartige Totalüberwachung wird nach den derzeit auf dem Markt befindlichen Angeboten von den Kunden gerade nicht verlangt, vielmehr können die Teilnehmer lediglich täglich Punkte für Trainingseinheiten erhalten, die sie mit einem Fitness-Tracker oder einer App der Partner des Versicherers erfassen.[375] Zudem betrifft dies lediglich einen besonders gelagerten Ausnahmefall und nicht die generelle Problematik der Übertagung von Gesundheitsdaten.

Weiter ist zu berücksichtigen, dass Tarifen, die die Umsetzung von Gesundheitszielen und den Nachweis von Trainingseinheiten mittels Fitness-Trackern finanziell begünstigen, gesundheitsbewusstes Verhalten fördern und damit insoweit ein gesamtgesellschaftlich sinnvolles Ziel verfolgen. Auf der anderen Seite bestehen aber auch erhebliche Risiken im Hinblick auf das informationelle Selbstbestimmungsrecht hinsichtlich besonders sensibler Daten sowie bezüglich möglicher Diskriminierungen.

---

[374] *Rudkowski*, Grundrechte als Grenze von Self-Tracking-Tarifen in der Privatversicherung, in Festschrift „Der Forschung – der Lehre – der Bildung, 100 Jahre Hamburger Seminar für Versicherungswissenschaft und Versicherungswissenschaftlicher Verein in Hamburg e. V." 661 (663 bis 669).

[375] https://www.generalivitality.de/vmp/aktiv_leben/fitness-tracker (letzter Abruf: 25.08.2018).

Nach der oben unter C. III. dargestellten Rechtsprechung des Bundesverfassungsgerichts dürfte eine Pflicht zum Eingreifen des Staates daher – trotz dieses an sich sinnvollen Ziels – zum Schutz des informationellen Selbstbestimmungsrechts entstehen, wenn Tarife, bei denen die Beitragshöhe durch Übermittlung von Gesundheitsdaten über Trainingseinheiten und das Erreichen von Fitnesszielen maßgeblich beeinflusst werden könnten, auch in der für alle Versicherungsnehmer besonders wichtige Krankenversicherung angeboten würden und sich solche Tarife auf dem Markt durchsetzen würden. Dies hätte zur Folge, dass ein mittelbarer Zwang zur Preisgabe dieser sensiblen Daten auch für die Versicherungsnehmer entstehen könnte, die diese Daten nicht übertragen wollen. Eine Krankenversicherung ist für alle von herausragender Bedeutung, zudem ist hier die weitgehende Versicherungspflicht zu beachten.[376]

Wenn sich derartige Konzepte auch für die besonders wichtige private Krankenversicherung auf dem Markt durchsetzen würden, wäre ein staatlicher Eingriff, der Versicherungsmodelle untersagt oder einschränkt (was verfassungsrechtlich dann allerdings geboten sein dürfte), für alle Betroffenen weitaus schwerwiegender, als wenn bereits zum gegenwärtigen Zeitpunkt eine klare Regelung jedenfalls für die privaten Krankenversicherungen (im VVG) getroffen würde. Derzeit würde durch ein solches Vorgehen noch kein status quo verändert. Es würde kein Versicherungsmodell, das bereits in der Praxis verbreitet ist und auf das sich Versicherer und Versicherte eingestellt haben, nachträglich untersagt. Der faktische Eingriff mit einer Regelung zur Zulässigkeit derartiger Tarife wäre im jetzigen Zeitpunkt weitaus geringer, als nach einer möglichen Marktdurchdringung.

Insoweit ist auch zu beachten dass der Trend zur verstärkten Messung und Speicherung von Gesundheitsdaten mittels Fitness-Trackern bzw. „Wearables“ sowie Apps unübersehbar ist. Angesichts der hier beschriebenen bereits aufkommenden ersten Ansätze in der Versicherungswirtschaft, derartige Daten zu erhalten und diese Übertragung zum Gegenstand der Tarifstruktur zu machen, könnten sich derartige Tarife in naher Zukunft auch schnell stärker auf dem Markt durchsetzen, wodurch legislative Maßnahmen zu größeren Einschnitten führen würden, als es jetzt der Fall wäre.

Vor diesem Hintergrund erscheint es sinnvoll, bereits jetzt legislative Maßnahmen zum Schutz der besonders sensiblen Gesundheitsdaten in Betracht zu ziehen. Dies vor allem, weil die Gefahrenpotentiale im Hinblick auf Verletzungen des

[376] § 193 Abs. 3 VVG bei der privaten Krankenversicherung sowie § 5 SGB V bei der gesetzlichen Krankenversicherung.

informationellen Selbstbestimmungsrechts und verschiedenartige Diskriminierungen, die diesen Konzepten innewohnen, erheblich sind:

Zum einen drohen die bereits ausführlich dargestellten Gefahren für das informationelle Selbstbestimmungsrecht derjenigen, die ihre sensiblen Gesundheitsdaten nicht übertragen wollen, wenn sich entsprechende Tarife durchsetzen sollten. Wird dauerhaft Kunden, die bereit sind, ihre hochsensiblen Gesundheitsdaten preiszugeben, ein günstigerer Tarif angeboten und wird dies von zahlreichen Kunden auch genutzt, wird dies langfristig zu einem Ansteigen der Versicherungsprämien der anderen Versicherten führen. Insoweit besteht die nicht fernliegende Gefahr, dass künftig ein erheblicher Druck entstehen wird, Gesundheitsdaten preiszugeben, um nicht wirtschaftliche Nachteile durch teurere Tarife zu erleiden.

Dieser Gefahr kann auch nicht mit dem Hinweis auf eine mögliche Rückkehr in die gesetzliche Krankenversicherung begegnet werden, in der diese Gefahren nicht in gleicher Weise bestehen. Eine Rückkehr in die gesetzliche Krankenversicherung, in der sich – wie oben dargestellt – diese Probleme nicht stellen, durch Versicherte, die sich privat versichert haben, ist in vielen Fällen nur schwierig oder überhaupt nicht möglich (Voraussetzungen: Tätigkeit in einem Angestelltenverhältnis mit weniger als 59.400 Euro jährlichem Bruttoeinkommen (für das Jahr 2018, im Jahr 2017: 57.600 Euro) sowie i.d.R. das Nichtüberschreiten der Altersgrenze von 55 Jahren gem. § 6 Abs. 3a SGB V).[377] Diese Rückkehr stellt mithin keine Option dar, die die Problematik umfassend entschärfen würde.

Hinzu kommt die Gefahr weiterer erheblicher Diskriminierungen durch derartige Versicherungstarifmodelle:

Menschen, die nicht in der Lage sind, die körperliche Fitness zu leisten, die ihnen die Teilnahme an günstigeren Tarifen ermöglicht (etwa ältere Menschen, chronisch Kranke oder Menschen mit körperlichen Behinderungen) würden benachteiligt. Sie wären regelmäßig von der Möglichkeit, günstige Tarife durch körperliche Fitness und den Beleg derselben mittels Datenübertragungen zu erhalten, von vornherein ausgeschlossen. Das damit einhergehende Diskriminierungspotenzial ist erheblich. Es droht darüber hinaus, dass das

[377] Vgl. zu den Details ausführlich etwa: BeckOK Sozialrecht/*Ulmer*, SGB V, § 6 Rn 1, 2, 3, 12-14, 40-42 (dort noch die Einkommensgrenze von 57.600 für 2017); Kasseler Kommentar Sozialversicherungsrecht/ *Peters*, SGB V § 6 Rn2, 10 ff., 57 ff; https://www.krankenversicherung.net/rueckkehr-gesetzliche; http://www.finanztip.de/pkv-rueckkehr-gkv/ (letzter Abruf: 25.8.2018).

Grundprinzip von Versicherungen als eine Institution zur Übernahme von Risiken des Lebens durch einen Ausgleich im Versichertenkollektiv in Frage gestellt wird.[378]

Hinzu kommt, dass gerade weniger wohlhabende Menschen sich veranlasst sehen könnten, ihre Gesundheitsdaten zu offenbaren, wenn sie eine private Versicherung abschließen wollen, da die Einsparungsmöglichkeiten sich für sie als wesentlich darstellen, während es sich Besserverdienende leisten könnten, diese intimen Informationen für sich zu behalten. In der Literatur wird darüber hinaus (wie oben unter Kapitel 2 B. I. ausführlich dargestellt) sogar die Befürchtung geäußert, dass künftig Versicherungen zu akzeptablen Preisen nur noch denjenigen möglich sein könnten, die Kontrollprozeduren für sich akzeptieren, während die anderen auf kaum mehr bezahlbare Tarife verwiesen werden könnten oder sogar gar keine Risikodeckung mehr erhalten könnten.[379] Die Preisgabe von sensiblen und sehr persönlichen Gesundheitsdaten sollte nicht von der wirtschaftlichen Situation des Betroffenen abhängen. Angesichts des eingeschränkten Leistungsumfangs und der nicht uneingeschränken persönlichen Anwendbarkeit des Basistarifs gem. § 152 VVG kann die Problematik auch durch einen Verweis auf den Basistarif des VVG nicht gelöst werden. Auch vor diesem Hintergrund gilt es einer solchen Entwicklung entgegenzuwirken.

Schließlich sind auch die Gefahren zu berücksichtigen, die für denjenigen entstehen, der einen derartigen Tarif freiwillig abschließt. Insoweit besteht etwa im Fall des Datendiebstahls ein nicht zu vernachlässigendes Risiko, da für dieses Geschäftsmodell hochsensible Daten in großer Menge personalisiert gespeichert werden müssen.[380] Auch droht jedem Einzelnen für den Fall der Änderung seines persönlichen Gesundheits- und Fitnessverhaltens (auch in Konstellationen, in denen dies für ihn gar nicht zu beeinflussen ist, etwa im Fall von Unfällen, schwerer Krankheit oder sonstiger auftretender körperlicher Einschränkungen), eine Verschlechterung des Versicherungstarifs.[381]

---

[378] So auch *Heinz*, Digitaler „Datenstriptease" – Die Erhebung von Kundendaten darf Solidarprinzip der Versicherungen nicht verletzen, VW 10/2016, 14.

[379] Vgl. *Heinz*, Digitaler „Datenstriptease" – Die Erhebung von Kundendaten darf Solidarprinzip der Versicherungen nicht verletzen, VW 10/2016, 14.

[380] Auch ohne Datendiebstahl droht bei Nutzung von Fitness-Trackern, dass in nicht unerheblichem Umfang private Daten öffentlich werden können. Bei der Nutzung des Fitnesstrackers von Strava wurde etwa entdeckt, dass auch US-Soldaten im Auslandseinsatz in Afghanistan damit ihre Joggingrouten (sowie z. T. sogar Versorgungsrouten) öffentlich gemacht hatten, mit der Folge eines gesteigerten Anschlagsrisikos, vgl. https://www.heise.de/newsticker/meldung/Fitnesstracker-Strava-Aktivitaetenkarte-legt-Militaerbasen-und-Soldaten-Infos-in-aller-Welt-offen-3952875.html (letzter Abruf: 25.8.2018).

[381] Derzeit droht allerdings keine stärkere Verschlechterung als der Rückfall zu dem Einstiegstarif.

Der sinnvolle Effekt, Versicherten Anreize zu einem gesundheitsbewussten Verhalten geben, ließe sich auch in anderer Weise realisieren als durch massenhafte Weitergabe hochsensibler Gesundheitsdaten mit negativen Auswirkungen auf das Gesamtsystem der Versicherungen.

Auch wenn das Angebot eines günstigeren Versicherungstarifs die stärkste Anreizwirkung haben dürfte, ist aber gleichwohl durch Bonusprogramme entsprechend solchen im Sinne des § 65a SGB V (also unter Wahrung des Solidarprinzips) eine Anreizwirkung zu erzielen, der nicht die Gefahr einer Diskriminierung Dritter innewohnt, die diese Daten nicht preisgeben möchten. Solche Bonusprogramme werden bereits derzeit von privaten wie gesetzlichen Versicherern angeboten und werden von den Versicherten auch sehr positiv bewertet.[382] Ein sinnvolles Setzen von Anreizen für gesundheitsbewusstes Verhalten kann damit auch in anderer Weise erfolgen, als durch potentiell Dritte diskriminierende Tarifgestaltungen, die mit der massenhaften Preisgabe hochsensibler Gesundheitsdaten verknüpft sind.

Der zusätzliche (möglicherweise noch stärkere) Anreiz zu gesundheitsbewusstem Verhalten, der durch das Angebot günstigerer Versicherungstarife bei Übertragung von Gesundheitsdaten einhergehen würde, stünde jedenfalls bei Versicherungen, bei denen der Nichtabschluss keine Alternative darstellt, in keinem Verhältnis zu dem Risiko für das informationelle Selbstbestimmungsrecht aller Versicherten, die sich faktisch gezwungen sehen könnten, ihre Gesundheitsdaten zu übermitteln sowie zu dem Risiko erheblicher weiterer Diskriminierungen.

Vor diesem Hintergrund kommt die Arbeitsgruppe zu dem Schluss, dass der Bundesgesetzgeber, in dem speziellen, besonders sensible Daten betreffenden und für den Einzelnen besonders wichtigen Bereich der privaten Krankenversicherung regulativ tätig werden sollte – gerade um zu verhindern, dass durch die Etablierung neuer Geschäftsmodelle Fakten geschaffen werden, die schwer umkehrbar wären. Dies gilt umso mehr, als es durchaus denkbar erscheint, dass

[382] Vgl. *Töpfer, Armin/ Opitz, Frank*, Bedeutung und Einfluss von Bonusprogrammen, Welt der Krankenversicherung 5/2017, 110 (111), wonach in aller Regel private wie gesetzliche Krankenkassen ihren Versicherten inzwischen Bonusprogramme anbieten und diese im Bereich der gesetzlichen Krankenversicherung inzwischen auch gesetzlich vorgeschrieben sind. Nach diesem Aufsatz, der sich mit einer Befragung von über 1.000 repräsentativ Befragten aus privater und gesetzlicher Krankenversicherung befasst (M+M Versicherungsbarometer 2017) sind 48,1 % der Befragten zufrieden und 32,7 % der Befragten sogar sehr zufrieden mit dem Bonusprogramm ihrer Versicherung (zusammen also: 80,8 %), Abb. 2 auf S. 111.

derartige Gesundheitsdaten künftig (wiederum mit entsprechender Einwilligung) mit anderen Daten kombiniert werden könnten und so immer weitergehend versucht werden könnte, Einfluss auf das Leben des Einzelnen zu nehmen. Dies könnte etwa durch Kombination der Gesundheitsdaten mit Informationen aus Pay-back-Daten bei Einkäufen geschehen, die über die gekauften Produkte Rückschlüsse über die (gesunde oder ungesunde) Ernährungsweise und den Alkohol- und Zigarettenkonsum zulassen. Eine Kombination mit DNA-Daten würde noch weitergehende Rückschlüsse über jeden Einzelnen zulassen (etwa die Ermittlung der Wahrscheinlichkeit des Ausbrechens schwerer Krankheiten), so dass bereits die genetische Veranlagung zum Gegenstand von Krankenversicherungstarifen würde.

Um derartigen Entwicklungen frühzeitig effektiv entgegenzutreten kämen insbesondere Anpassungen im Versicherungsvertragsgesetz in Betracht, mit denen Vertragsgestaltungen (jedenfalls für die private Krankenversicherung) für unwirksam erklärt werden, die darauf basieren, dass Versicherungsnehmer laufend Gesundheitsdaten zum Zwecke der Erlangung eines günstigeren Versicherungstarifs preisgeben. Unberührt hiervon blieben anderweitige Anreizfunktionen, wie etwa Bonusprogramme entsprechend solchen gem. § 65a SGB V, mit denen gesundheitsbewusstes Verhalten ebenfalls gefördert werden kann.

E. Regelungsvorschlag

Die Arbeitsgruppe schlägt daher vor, § 213 VVG um einen Absatz 5 zu ergänzen, mit dem für die Krankenversicherung die laufende Erhebung personenbezogener Gesundheitsdaten zu Zwecken der Tarifgestaltung unabhängig von einer Einwilligung des Versicherten für unzulässig erklärt wird.

Weiter schlägt die Arbeitsgruppe vor, die Vereinbarung entsprechender Tarife in der Krankenversicherung für unzulässig zu erklären. Als Rechtsfolge sollte für den Fall, dass Versicherer dennoch derartige Tarife anbieten, die vereinbarte Tarifhöhe gelten, die Pflicht zur Datenübermittlung aber ersatzlos entfallen. Dies würde Versicherer effektiv dazu anhalten, keine derartigen Tarife bei der Krankenversicherung anzubieten. Eine derartige Regelung könnte in einem neuen § 203 Abs. 6 VVG bzw. in einem § 203a VVG im Rahmen der Vorschriften zur privaten Krankenversicherung geschaffen werden.

Ein neuer § 213 Abs. 5 VVG könnte lauten:

„(5) Die laufende Erhebung personenbezogener Gesundheitsdaten zu Zwecken der Tarifgestaltung im Rahmen von Krankenversicherungen ist unabhängig von einer Einwilligung der betroffenen Person unzulässig.“

Ein neuer § 203 Abs. 6 VVG könnte lauten:

„(6) Unzulässig sind Vereinbarungen, wonach die laufende Übermittlung personenbezogener Gesundheitsdaten Auswirkungen auf die Tarifhöhe hat. Wird ein derartiger Tarif entgegen Satz 1 vereinbart, gilt die in dem jeweiligen Vertrag vereinbarte Tarifhöhe, ohne dass dem Versicherer ein Anspruch auf die Übermittlung der Daten zusteht."

F. Ergebnis

Die laufende Erhebung personenbezogener Gesundheitsdaten zu Zwecken der Tarifgestaltung in der privaten Krankenversicherung sollte für unzulässig erklärt werden.

Literaturverzeichnis

Bach, Peter/ Moser, Hans	Private Krankenversicherung 5. Auflage, München 2015
Broy, Manfred	Informatik. Eine grundlegende Einführung. Bd. 1, 2. Auflage, Berlin 1998
Cormen, Thomas H.	Algorithms unlocked Massachusetts, London 2013
Giesen, Richard/ Kreikenbohm, Ralf/ Rolfs, Christian/ Udsching, Peter	Beck-Online Kommentar Sozialgesetzbuch (SGB) V, 49. Auflage, München 2018
Gola, Peter	Datenschutzgrundverordnung, Kommentar, 1. Auflage, München 2017
Grunewald, Barbara u.a.	Ermann, BGB, Handkommentar 15. Auflage, Köln 2017
Hauck, Karl/ Noftz, Wolfgang	Sozialgesetzbuch (SGB) V, Kommentar (Loseblatt), Berlin 2014
Härting, Niko	Internetrecht, 6. Auflage, Köln 2017
Herberger, Maximilian/ Martinek, Michael u.a. (Hrsg.)	Juris Praxiskommentar BGB, Bd. 2 8. Auflage, Saarbrücken 2017
Hromkovic, Juraj	Sieben Wunder der Informatik 2. Auflage, Wiesbaden 2009

Kiel, Heinrich/ Lunk, Stefan/ Oetker,H.(Hrsg.) — Münchner Handbuch zum Arbeitsrecht, Bd. 1, Individualarbeitsrecht 4. Auflage, München 2018

Körner, Anne/ Leitherer, Stephan/ Mutschler, Bernd — Kasseler Kommentar Sozialversicherungsrecht, SGV V, Loseblatt 99. Auflage, München 2018

Kühling, Jürgen/ Buchner, Benedikt — Datenschutzgrundverordnung, Kommentar, 2. Auflage, München 2018

Langheid, Theo/ Rixecker, Roland — Versicherungsvertragsgesetz, 5. Auflage, München 2016

Mangoldt, Herrmann von/ Klein, Friedrich/ Starck, Christian — Grundgesetz, Kommentar, Bd. I 6. Auflage, München 2010

Münch, Ingo von/ Kunig, Philip — Grundgesetz, Kommentar, Bd. I 6. Auflage, München 2012

Palandt, Otto — Bürgerliches Gesetzbuch 77. Auflage, München 2018

Plath, Kai-Uwe (Hrsg.) — DSGVO/BDSG, Kommentar, 3. Auflage, Köln 2018

Promberger, Gustav/ Dobler, Heinz — Algorithmen und Datenstrukturen. Eine systematische Einführung in die Programmierung München 2008

Rieble, Volker (Red.) — Staudinger, BGB Neubearbeitung, Berlin 2018

Roetteken, Torsten von — Allgemeines Gleichbehandlungsgesetz (AGG) Kommentar 57. Auflage, 2018

Säcker, Franz-Jürgen (Red.) — Münchner Kommentar zum Bürgerlichen Gesetzbuch,
Bd 1, 7. Auflage, München 2015
Bd. 2, 7. Auflage, München 2016

Sparwasser, Reinhard/ Engel, Rüdiger/ Voßkuhle, Andreas — Umweltrecht
3. Auflage, 2003

Weigend, Andreas — Data for the people
1. Auflage, Hamburg 2017

Inhaltsverzeichnis

Bericht vom 15. April 2019 133

Zusammenfassung und Ergebnisse 133

A. Robotic Law 133
B. Blockchain 137
C. Leistungsschutzrechte an maschinengenerierten Daten 138

Einführung 140

Teil 1: „Robotic Law“ 142

A. Zielsetzung und Herangehensweise 142
B. Begriffserklärungen 143
I. Künstliche Intelligenz 144
II. Algorithmus 144
III. Lernender Algorithmus 145
IV. Autonomes System 145
V. Selbstlernendes System 146
VI. Intelligente Roboter 146
C. Bisherige Vorschläge und laufende Arbeiten 147
D. Zulassungsrecht 150
I. Einführung 150
II. Zulassung von Fahrzeugen 151
III. Zulassung von Medizinprodukten 156
IV. Autonome Systeme 159
E. Allgemeine Grundsätze zum Haftungsrecht bei autonomen Systemen 165
I. Vorbemerkung 165

II. Deliktische Verschuldenshaftung 166
III. Gefährdungshaftung 170
IV. Insbesondere: Haftung nach dem Produkthaftungsgesetz und deliktische Produzentenhaftung 182
V. Ergebnis 199
F. Autonomes Fahren 200
I. Einführung 200
II. Betreiber-/Benutzerhaftung 202
III. Herstellerhaftung 209
IV. Ergebnis 223
G. Medizintechnik 225
I. Einführung 225
II. Betreiberhaftung 226
III. Herstellerhaftung 238
IV. Handlungsbedarf 259

Teil 2: „Blockchain“ 260

A. Einführung 260
B. Technische Grundlagen 262
I. Grundstruktur 262
II. Teilnahme an einer Blockchain 264
III. Digitales Schlüsselpaar (Public-Key-Verfahren) 264
IV. Hashing 265
V. Einleitung einer Transaktion 266
VI. Blockbildung 266
VII. „Gültigkeit“ eines Blocks / Verfahren bei Forkbildung 268
VIII. Gebühren / Belohnung 269
IX. Möglichkeiten zur Änderung der Blockchain 269
X. Vor- und Nachtteile der Blockchain-Technologie (insb. der unbeschränkt zugänglichen Blockchain) 271
C. Begriff des Smart Contracts 273
D. Begriff der Transaktion 275
E. Vertragsabschluss über eine Blockchain-Anwendung 276

I. Abgabe einer Willenserklärung 277
II. Zugang einer Willenserklärung 278
F. Pflichten im elektronischen Geschäftsverkehr (§§ 312i, 312j BGB) 279
G. Wirksamkeit des Vertrags 280
I. Nichtigkeitsgründe (§ 125, § 134, § 138, § 142 BGB) 280
II. Insbesondere: Anfechtung von computererzeugten Willenserklärungen 284
III. Schwebende Unwirksamkeit bei Beteiligung von Minderjährigen 284
IV. Schwebende Unwirksamkeit bei Vertretung ohne Vertretungsmacht 285
V. Welchen Formanforderungen genügt die Blockchain-Technologie? . 285
H. AGB-Recht 286
I. Beispiel: Smart Contracts im Versicherungswesen 288
J. Rücktritt 289
K. Rechtliche Grenzen der Vertragsdurchsetzung mittels Smart Contracts 290
I. Insbesondere: Verbotene Eigenmacht (§ 858 BGB) 290
II. Beispiel: Fernsperre im Bereich der Energieversorgung 292
L. Zwangsvollstreckung 293
I. Zwangsweise Durchsetzung einer Änderung der Blockchain 293
II. „Blockchain-Vermögen“ als Vollstreckungsgegenstand? 294
M. Befassung auf EU-Ebene 295

Teil 3:

„Leistungsschutzrechte an maschinengenerierten Daten“ 297

A. Vorbemerkung 297
B. Einführung in die Thematik und Begrifflichkeiten 297
I. Der Begriff des Leistungsschutzrechts 298
II. Datenbegriff, maschinengenerierte Daten 299
C. Schutz maschinengenerierter Daten nach geltendem Recht 302
I. Leistungsschutz im Bürgerlichen Gesetzbuch 302
II. Urheberrechtsschutz an maschinengenerierten Daten 313
III. Leistungsschutz nach dem *sui-generis*-Schutz des Datenbankherstellers 314

IV. Lauterkeitsrechtlicher Leistungsschutz 322
D. Überlegungen de lege ferenda 326
I. Kompetenz des deutschen Gesetzgebers zur Schaffung neuer Leistungsschutzrechte an maschinell generierten Daten 326
II. Rechtfertigung für die Schaffung eines neuen Leistungsschutzrechts 332
E. Gesamtergebnis 342

Literaturverzeichnis 344

Bericht vom 15. April 2019

Zusammenfassung und Ergebnisse

A. Robotic Law

Zulassungsrecht

Es besteht eine Wechselwirkung zwischen Haftungs- und Zulassungsrecht: Der Gesetzgeber hat die Aufgabe, durch das Zulassungsrecht die von automatisierten und autonomen Systemen ausgehenden Gefahren von vornherein auf ein gesellschaftlich akzeptiertes Maß zu begrenzen.

Zum Haftungsrecht allgemein

Allein in der Herstellung und in dem Inverkehrbringen eines autonomen Systems liegt keine „besondere Gefahr", die eine über die heutigen Haftungsnormen hinausgehende Gefährdungshaftung rechtfertigt. Auch der Umstand, dass sich Beweisschwierigkeiten ergeben können, genügt grundsätzlich nicht; allerdings können sie ggf. eine abweichende Ausgestaltung der Beweislastverteilung erforderlich machen, was nicht allgemein beurteilt werden kann, sondern nur produktbezogen zu beantworten ist.

Was die Haftung des Herstellers angeht, greift der Haftungsgrund, welcher der Produkthaftung zugrunde liegt, ohne weiteres auch dann ein, wenn es um autonome Systeme geht. Allerdings ist zu prüfen, ob einzelne Regelungen des Produkthaftungsgesetzes (ProdHaftG) auf den Einsatz autonomer Systeme abzustimmen sind. Etwaige Beweisschwierigkeiten, ob das Produkt fehlerhaft ist, rechtfertigen für sich genommen nicht die Einführung einer Gefährdungshaftung des Herstellers unabhängig vom Vorliegen eines Produktfehlers, sondern ggf. eine Beweislastumkehr. Eine Gefährdungshaftung des Herstellers ist vielmehr nur dann systemgerecht, wenn die Haftung an einen Produktfehler anknüpft.

Es besteht kein Bedürfnis für eine gesetzliche Regelung, mit der der Hersteller verpflichtet wird, im Rahmen der Produkthaftung Softwareupdates zur Verfügung zu stellen. Die damit zusammenhängenden Fragen können auf Basis des geltenden Rechts der Rechtsprechung überlassen bleiben.

Derzeit sind keine hinreichenden Gründe ersichtlich, warum in Bezug auf die von der Arbeitsgruppe untersuchten Produktbereiche die Entlastungsmöglichkeit nach § 1 Abs. 2 Nr. 5 ProdHaftG wegfallen sollte.

Im Rahmen der Prüfung, ob eine Gefährdungshaftung des Betreibers systemkonform ist, muss zunächst produktbezogen ermittelt werden, ob von der Sache eine „besondere Gefahr" ausgeht. Das wird man auch bei autonomen Systemen nicht generell annehmen können. Auch wenn diese Frage zu bejahen ist, ist eine Gefährdungshaftung des Betreibers jedenfalls dann nicht geboten, wenn für das Produkt ein besonderes Zulassungsverfahren existiert, dem Geschädigten im Falle eines Produktfehlers hinreichende Ansprüche gegen den Hersteller zustehen und mit dem Produkt typischerweise nur Personen in Berührung kommen, die sich freiwillig der Gefahr ausgesetzt haben und über die Gefahren, die von dem Betrieb des autonomen Systems ausgehen, sachgerecht aufgeklärt wurden.

Die Arbeitsgruppe ist diesen Fragen anhand zweier bedeutsamer und strukturell unterschiedlich geregelter Bereiche nachgegangen:

Autonomes Fahren

Bei einem Fahrzeug mit hoch- oder vollautomatisierter Fahrfunktion hat der Gesetzgeber das bisherige Haftungsregime mit Halter- und Fahrerhaftung als ausreichend erachtet. Dieses Haftungsregime ist auch für das autonome Fahren tauglich und berücksichtigt insbesondere die Interessen von Geschädigten, ihren Schaden auf einfache Weise ersetzt zu bekommen.

Der Wegfall der Fahrerhaftung nach Maßgabe des § 1b StVG wird beim hoch- oder vollautomatisierten Fahren durch die Verdoppelung der Haftungshöchstbeträge nach § 12 Abs. 1 StVG kompensiert; diese Regelung muss konsequenterweise auch auf das autonome Fahren anwendbar sein.

Mit dem Direktanspruch gegen den Kfz-Haftpflichtversicherer bzw. bei vorsätzlicher Schadensherbeiführung gegen einen Entschädigungsfonds für Schäden aus Kraftfahrzeugunfällen ist sichergestellt, dass der Geschädigte stets einen solventen Schuldner hat; diese Ansprüche müssen allerdings auch bei durch einen Hackerangriff verursachten Schäden bestehen.

Mit fortschreitender Automatisierung und Verselbstständigung der Fahrzeuge kommt mangels eigener Steuerung durch den Fahrer der dem Betrieb des Fahrzeugs zugrunde liegenden Software eine gesteigerte Funktion zu. Unfälle werden beim automatisierten/autonomen Fahrzeug in der Regel auf ein Versagen der Steuerungssoftware und nicht mehr auf ein Versagen des Fahrers zurückgeführt werden können. Sofern diese Software nicht durch den Endhersteller des Fahrzeugs selbst, sondern durch einen Zulieferer bereitgestellt wurde, kann nicht

nur der Fahrzeughersteller, sondern auch der Zulieferer im Wege der Produzentenhaftung in Anspruch genommen werden.

Der in einem autonomen System verwendete Steuerungsalgorithmus muss den Anforderungen an eine sorgfältige, dem Stand der Technik entsprechende Programmierung gerecht werden. Es dürfte den berechtigten Sicherheitserwartungen regelmäßig entsprechen, dass der Algorithmus auch in einer konkreten Verkehrssituation nicht hinter den Sorgfaltsanforderungen zurücksteht, die an einen sorgfältigen menschlichen Fahrer gestellt werden können, soweit er bestimmungsgemäß den menschlichen Fahrer ersetzen soll. Die Beurteilung der berechtigten Sicherheitserwartungen im Einzelfall kann der Rechtsprechung überlassen bleiben.

In Dilemmasituationen kann die Bestimmung der Anforderungen, die an die Ausgestaltung der Steuerungssoftware des autonomen Fahrzeugs zu stellen sind, allerdings nicht allein nach dem Stand von Wissenschaft und Technik erfolgen; vielmehr sind hier auch ethische Wertungen entscheidend. Angesichts des derzeitigen technischen Entwicklungsstandes, der eine Unterscheidung verschiedener Rechtsgüter und Personengruppen durch ein autonomes Fahrzeug noch nicht zulässt, erscheint ein zeitnahes gesetzgeberisches Handeln noch nicht erforderlich. Die Möglichkeit der Schaffung von mehr Rechtssicherheit für die Hersteller sollte jedoch – möglichst auf europäischer Ebene – weiter geprüft und verfolgt werden.

Es sollte überlegt werden, ob eine Zulassung autonomer Fahrzeuge nur dann erfolgen sollte, wenn das Fahrzeug über eine Blackbox verfügt, um den Geschädigten vor unüberwindbaren Beweisschwierigkeiten zu bewahren.

Medizintechnik

Beim Einsatz von autonomen Medizinprodukten kann es zu einer Verlagerung von Pflichten kommen. Je autonomer ein System agiert, desto häufiger wird der Arzt nicht mehr für Ausführungsfehler, sondern nur noch für Fehler bei der Auswahl, Überwachung und Wartung des Produkts haften. Dies gilt insbesondere dann, wenn der Schaden auf einer fehlerhaften Programmierung beruht. Vom Arzt wird aber – wie stets beim Einsatz von Medizinprodukten – weiter verlangt, dass er die autonom agierende Maschine sachgerecht auswählt, überwacht und – soweit diese Aufgabe nicht beim Krankenhausträger liegt – wartet.

Der Arzt muss ferner bei der Diagnostik und Behandlung grundsätzlich den medizinischen Standard einhalten. Hierbei darf er – vorbehaltlich der aufgeklärten Entscheidung des Patienten – zwischen mehreren Behandlungsmöglichkeiten, die alle dem Standard entsprechen, wählen. Soweit also in einigen Jahren der Fall eintritt, dass der Einsatz einer autonomen Technik dem medizinischen

Standard entspricht, bezieht sich die Wahlmöglichkeit des Arztes auch auf deren Einsatz. Ist dieser Stand noch nicht erreicht, können den Arzt besondere Aufklärungspflichten treffen. Der Arzt muss daher mit dem Patienten die Chancen und Risiken des in Rede stehenden autonomen Systems besprechen und bewerten, um dem Patienten eine sachgerechte Entscheidung über die zu wählende Behandlungsmethode zu ermöglichen.

Mangels relevanter Schutzlücke ist es nicht geboten, eine Gefährdungshaftung des Betreibers für autonome Medizinprodukte einzuführen. Dabei ist auch zu bedenken, dass mit der autonom agierenden Medizintechnik typischerweise keine unbeteiligte Dritte, sondern lediglich Personen in Berührung kommen, die über die typischen Risiken der eingesetzten Produkte hinreichend aufgeklärt wurden und sich in Anbetracht dieser Aufklärung für die Behandlung entschieden haben. Zwar kann es dazu kommen, dass ein Arzt seine ihn treffenden Aufklärungspflichten gegenüber dem Patienten verletzt. In diesem Fall greift aber in der Regel die Haftung aus § 280 Abs. 1 BGB.

Gegen eine hinreichend gewichtige Haftungslücke spricht auch, dass der Einsatz von Medizinprodukten von einer Zulassung abhängig ist. Es kann nämlich grundsätzlich davon ausgegangen werden, dass dann, wenn ein Zulassungsverfahren existiert, die Gefahr schädigender Ereignisse geringer ist, als würde es das Zulassungsverfahren nicht geben.

Auch im Hinblick auf die Haftung des Herstellers von autonom agierender Medizintechnik ist derzeit kein gesetzgeberischer Handlungsbedarf erkennbar. Die deliktische Haftung aus § 823 Abs. 1 BGB sowie die Produkthaftung nach ProdHaftG erscheinen ausreichend.

Im Gegensatz zum Arzneimittel- und Gentechnikhersteller, die nach § 84 AMG und § 37 Abs. 2 S. 2 GenTG auch für Entwicklungsfehler haften, ist der Medizinproduktehersteller, der autonome Systeme herstellt, nach § 1 Abs. 2 Nr. 5 ProdHaftG privilegiert. Momentan besteht aber kein Anlass, für die nach dem derzeitigen Stand der Technik in absehbarer Zeit zum Einsatz kommenden autonomen (nicht selbstlernenden) Systeme das Entwicklungsrisiko den Herstellern aufzuerlegen. Denn derzeit sind durch den Einsatz autonomer Systeme noch keine unabsehbaren Folgen zu erwarten, da es sich um abgekapselte Systeme handelt, die im Wesentlichen nachvollziehbar und letztlich auch beherrschbar sind.

Eine andere Problemlage könnte zukünftig entstehen, wenn Produkte eingesetzt werden, die nicht nur autonom, sondern auch selbstlernend agieren, da hierdurch eine klare Zurechnung von Verantwortlichkeiten nicht mehr gewährleistet sein könnte. Der Einsatz solcher Produkte ist aber nach Auskunft der von der Arbeitsgruppe angehörten Experten jedenfalls für den Medizinbereich in absehbarer Zeit nicht zu erwarten.

B. Blockchain

Die Blockchain-Technologie hat in den vergangenen Jahren medial große Beachtung gefunden; ihr tatsächlicher Einsatz in der Praxis ist hingegen bislang noch auf wenige Anwendungsfelder begrenzt.

Zivilrechtliche Probleme, die sich im Zusammenhang mit dem Einsatz der Blockchain-Technologie ergeben (könnten), lassen sich nach Ansicht der Arbeitsgruppe mit den bestehenden Regelungen, vor allem des Bürgerlichen Gesetzbuches, und den von Rechtsprechung und Lehre im Bereich des Privatrechts entwickelten Grundsätzen angemessen lösen.

Wesentlich ist dabei der Befund, dass die Blockchain lediglich tatsächliche Vorgänge protokolliert, nicht aber juristische Wertungen vollzieht oder als Rechtsscheinträger fungiert. Die rechtliche Bewertung, ob ein Vertrag zustande gekommen oder ein Recht wirksam übertragen worden ist, findet außerhalb der Blockchain anhand allgemeiner Regeln statt. Spezifischer Regelungen für Verträge, die über Blockchain-Anwendungen evtl. abgeschlossen oder vor allem abgewickelt werden, bedarf es zum jetzigen Zeitpunkt nicht. Insbesondere steht das Prinzip der Unveränderbarkeit einem Einsatz der Blockchain-Technologie zum Abschluss und zur Abwicklung oder ggf. auch zur Rückabwicklung von Verträgen nicht entgegen.

Aktuell sieht die Arbeitsgruppe daher keinen gesetzgeberischen Handlungsbedarf für den Bereich des Zivilrechts. Es kann vielmehr den Gerichten überlassen bleiben, etwaige Streitfragen im Einzelfall auf Grundlage des geltenden Rechts zu klären.

Die weitere technische Entwicklung sowie die Art und der Umfang des konkreten Einsatzes der Technologie in der Praxis bleiben abzuwarten. Sollten sich dabei künftig nicht hinnehmbare Regelungslücken ergeben oder inakzeptable Verschiebungen des Beweis- oder Prozessrisikos beispielweise mit Blick auf die Möglichkeiten der digitalisierten Rechtsdurchsetzung herausstellen, wird die Arbeitsgruppe diese Probleme aufgreifen und die Frage des gesetzgeberischen Handlungsbedarfs insoweit einer erneuten Prüfung unterziehen.

C. Leistungsschutzrechte an maschinengenerierten Daten

Untersuchungsgegenstand sind ohne unmittelbare Mitwirkung eines Menschen erzeugte digitale Daten, die nach einem bestimmten Code dargestellt sind und die deshalb von Computern und anderen Geräten zur digitalen Datenverarbeitung gelesen oder verarbeitet werden können. Diesen Maschinendaten kommt eine immense wirtschaftliche Bedeutung zu. Gängige Beispiele sind Mobilitätsdaten von Fahrzeugen oder Messwerte von Wetter, Grundstücken, Gebäuden etc. Neben Anwendungsbereichen im privaten Bereich liegt in der Analyse und Verarbeitung dieser Daten insbesondere für Landwirtschaft und Industrie ein erhebliches Potential für Automatisierung und Effizienzsteigerung.

Die Arbeitsgruppe hat daher untersucht, ob für maschinengenerierte Daten ein Schutz im Sinne eines Leistungsschutzrechts besteht bzw. etabliert werden sollte. Im Ergebnis ist dies kurz zusammengefasst aus folgenden Gründen zu verneinen:

Das Bürgerliche Recht kennt kein Ausschließlichkeitsrecht an maschinengenerierten Daten. Die gesetzlichen Schuldverhältnisse setzen eine bestehende Rechtezuweisung voraus, ohne sie selbst vorzunehmen. Dem Bürgerlichen Recht lässt sich auch kein Rechtsprinzip entnehmen, das gebietet, ein Leistungsschutzrecht an maschinengenerierten Daten anzuerkennen. Weder in direkter noch in analoger Anwendung treffen die Vorschriften der §§ 950, 951 BGB Aussagen über einen etwaigen Rechtsverlust an Daten durch Speicherung und Verarbeitung oder über eine Entschädigungsregelung. Leistungsschutz im Sinne von Investitionsschutz wird durch § 826 BGB gewährt.

Maschinengenerierte Daten unterliegen als solche auch nicht dem Schutz des Urheberrechts und des *sui-generis*-Leistungsschutzrechts des Datenbankherstellers. De lege lata genießen maschinengenerierte Daten auch keinen unmittelbaren Leistungsschutz nach § 3 UWG. Leistungsschutz kann durch § 4 UWG gegen unlautere Wettbewerbshandlungen gewährt werden.

Bei der Prüfung eines gesetzgeberischen Handlungsbedarfs wurde untersucht, ob die Schaffung eines neuen Leistungsschutzrechts im Allgemeininteresse liegt, weil ohne dieses keine ausreichenden Innovations- und Investitionsanreize hinsichtlich der Erzeugung dieser Daten bestehen, weil ein Leistungsschutzrecht zur Beseitigung von Hindernissen beim Datenzugang und zur Absenkung von Transaktionskosten beitragen oder bislang fehlende Offenbarungsanreize setzen würde. Es finden sich derzeit jedoch keine Belege dafür, dass ohne die Schaffung eines Leistungsschutzrechts an maschinengenerierten Daten künftig Innovationen unterblieben. Eine Unterversorgung mit maschinengenerierten Daten ist ebenfalls nicht feststellbar. Im Interesse eines freien Datenverkehrs, aber

auch zur Senkung von Transaktionskosten, erscheint die Etablierung von Zugangsregelungen gegenüber der Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten vorzugswürdig. Zugangsregelungen könnten sektorspezifisch dort vorgesehen werden, wo sich kartellrechtliche Regelungen als nicht (mehr) ausreichend erweisen. Mit der Schaffung eines neuen Leistungsschutzrechts an Daten wären Offenbarungsanreize nur bei gleichzeitiger Ausgestaltung dieses Rechts als Registerrecht verbunden. Die Schaffung eines Registerrechts erscheint hingegen als nicht praktikabel. Somit besteht für die Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten (derzeit) kein Bedarf.

Einführung

Die Frühjahrskonferenz der Justizministerinnen und Justizminister vom 21. und 22. Juni 2017 in Deidesheim hat unter TOP I.2 den Bericht der mit Beschluss vom 17. und 18. Juni 2015 eingesetzten Länderarbeitsgruppe „Digitaler Neustart“ gebilligt und der Arbeitsgruppe folgenden Arbeitsauftrag erteilt:

> *„Die Justizministerinnen und Justizminister sind sich darin einig, dass die Arbeitsgruppe die Diskussion um die zivilrechtlichen Folgen der Digitalisierung, sowohl auf nationaler als auch europäischer Ebene, weiter begleiten soll. Unter diesem Aspekt beauftragen sie die Arbeitsgruppe, ihre Arbeit fortzusetzen und*
>
> *a) sich vertieft mit bisher ausgeklammerten Themen, insbesondere den zivilrechtlichen Aspekten im Zusammenhang mit „Big Data“, zu befassen, sowie gegebenenfalls auch Fragestellungen, die sich aus der Dynamik der digitalen Entwicklung perspektivisch ergeben, aufzugreifen,*
>
> *b) die bereits behandelten Themen im Blick zu halten und auf der Grundlage des Berichts den Austausch mit der Fachöffentlichkeit zu suchen und*
>
> *c) bei Bedarf einzelne Themen wieder aufzugreifen und nochmals einer speziellen Prüfung zu unterziehen*.“

Die erste Sitzung der Länderarbeitsgruppe nach dem Beschluss der Frühjahrskonferenz der Justizministerinnen und Justizminister vom 21. und 22. Juni 2017 fand unter Federführung Nordrhein-Westfalens am 26. September 2017 statt.

Zur weiteren Bearbeitung wurde die Einrichtung von zwei Arbeitsgruppen zu den Themenbereichen „Big Data, Algorithmentransparenz und Gesundheitsdaten“ unter Federführung Hessens (Arbeitsgruppe 1) und „Robotic Law (einschließlich Haftungsfragen und selbstlernende Algorithmen), Blockchain und Leistungsschutzrecht an Daten“ (Arbeitsgruppe 2) unter der Gesamtfederführung von Nordrhein-Westfalen beschlossen. Die Arbeitsgruppe 2 untergliedert sich ihrerseits in drei Unterarbeitsgruppen. An der Arbeitsgruppe 2, Unterarbeitsgruppe „Robotic Law“, unter Federführung von Baden-Württemberg wirkten die Länder Bayern, Berlin, Niedersachsen, Nordrhein-Westfalen und Sachsen mit. An den Sitzungen der Unterarbeitsgruppe nahmen außerdem Vertreter des Bundesministeriums der Justiz und für Verbraucherschutz teil und ab dem

26. März 2018 nahm zudem zeitweise ein Vertreter der Europäischen Kommission teil.
Die Themen der Unterarbeitsgruppe „Blockchain“ wurden von den Ländern Berlin und Nordrhein-Westfalen bearbeitet. An der Unterarbeitsgruppe „Leistungsschutzrecht an Daten“ wirkten die Länder Niedersachsen und Nordrhein-Westfalen mit.

Die Frühjahrskonferenz der Justizministerinnen und Justizminister vom 6. und 7. Juni 2018 in Erfurt nahm unter TOP I.3. den Zwischenbericht der Länderarbeitsgruppe „Digitaler Neustart“ zur Kenntnis und bat die Arbeitsgruppe, ihre Arbeit zu den darin als prüfwürdig benannten Themenbereichen fortzusetzen.
Zur Herbstkonferenz der Justizministerinnen und Justizminister vom 15. November 2018 hat die Arbeitsgruppe ihren Bericht zu den Themenbereichen „Big Data, Algorithmentransparenz und Gesundheitsdaten“ vorgelegt.

Teil 1: „Robotic Law“

A. Zielsetzung und Herangehensweise

Der dem Beschluss der Frühjahrskonferenz der Justizministerinnen und Justizminister 2017 zugrunde liegende Bericht der Länderarbeitsgruppe „Digitaler Neustart“ setzt sich unter anderem mit der Frage auseinander, ob und welcher gesetzgeberische Handlungsbedarf im Hinblick auf haftungsrechtliche Aspekte beim Einsatz autonom agierender Maschinen und Systeme gesehen wird. Als Zwischenergebnis hält der Bericht fest, dass in Bezug auf die außervertragliche verschulden*sun*abhängige Haftung eine Haftungslücke drohen und daher ein gesetzgeberischer Handlungsbedarf in Betracht kommen *könnte*.

In ihrer ersten Sitzung am 28. November 2017 beschloss die Unterarbeitsgruppe „Robotic Law“, den sich hierzu im Einzelnen stellenden Fragen nachzugehen. Sie beschloss, beispielhaft anhand des bereits heute erfolgenden oder innerhalb der nächsten zehn bis 15 Jahre zu erwartenden Einsatzes digitaler Systeme im Straßenverkehr (Stichwort: autonomes Fahren) und in der Medizintechnik zu prüfen, ob eine Haftungslücke tatsächlich besteht oder absehbar ist und in welcher Weise diese Haftungslücke ggf. geschlossen werden sollte.

Mit dem der Untersuchung zugrunde gelegten Zeitraum von zehn bis 15 Jahren orientiert sich die Arbeitsgruppe an dem Zeitraum, den auch das Europäische Parlament seiner Entschließung vom 16. Februar 2017 zugrunde legte.[1] Angesichts der rasanten Entwicklung im Bereich der Informationstechnologie ist die Prognose der Entwicklung bereits für diesen Betrachtungszeitraum mit großen Unsicherheiten behaftet.

Die von der Arbeitsgruppe näher untersuchten Bereiche zeichnen sich dadurch aus, dass sie – abgesehen von der in beiden Bereichen geltenden Produkt- und Produzentenhaftung des Herstellers – derzeit unterschiedlichen Haftungsregimen unterliegen: Im Straßenverkehr ist der Betreiber (nämlich der Kraftfahrzeughalter) einer Gefährdungshaftung ausgesetzt; der Arzt und der Krankenhausträger haften dagegen nur aufgrund Verschuldens. Die Arbeitsgruppe ging

[1] In Ziff. 51 der Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)) forderte das Parlament die Kommission auf, „einen Vorschlag für ein Rechtsinstrument über rechtliche Fragen im Zusammenhang mit der Entwicklung und Verwendung von Robotik und künstlicher Intelligenz, wie sie in den nächsten zehn bis 15 Jahren vorhersehbar ist, zu unterbreiten“.

der Frage nach, ob der Einsatz autonomer Systeme Anlass dazu gibt, das Haftungsregime in diesen strukturell unterschiedlichen Bereichen zu ändern. Dass in dem betrachteten Zeitraum selbstlernende Systeme zum Einsatz kommen werden, konnte die Arbeitsgruppe weder für die untersuchten Bereiche noch für andere Produktbereiche identifizieren.[2]

Die Unterarbeitsgruppe hat sich mithilfe externen Sachverstands darüber informiert, welche Einsatzformen autonomer Systeme auf den genannten Gebieten es bereits heute gibt und welche in den nächsten zehn bis 15 Jahren zu erwarten sind. Sie befragte in der Sitzung am 7. März 2018 zum autonomen Fahren Dr. Nicole Leifeld, Zentralabteilung Recht, Unternehmensbereich Mobility Solutions und Unternehmensrecht, Robert Bosch GmbH, Stuttgart. Zu Fragen der Medizintechnik sprach die Arbeitsgruppe am 26. März 2018 mit Vertretern der Fa. Siemens Healthcare GmbH, Erlangen, nämlich mit David Kniß, Dr. Isabelle Gärtner (beide Legal and Compliance) und Dr. Dr. Björn Heismann (Diagnostic Imaging). Über Fragen der Sicherheit von autonomen Fahrzeugen sprach die Arbeitsgruppe am 18. Mai 2018 mit Prof. Dr. Frank Kargl, Institut für Verteilte Systeme, Universität Ulm. Am 18. Mai 2018 besuchte die Unterarbeitsgruppe außerdem das Fraunhofer-Institut, Projektgruppe für Automatisierung in der Medizin und Biotechnologie am Klinikum Mannheim, und sprach mit Prof. Dr.-Ing. Jan Stallkamp über den Stand seiner Forschung zum Thema „automatisiertes Krankenhaus“.

Am 15. Februar 2019 tauschte sich die Unterarbeitsgruppe mit einem Vertreter der Europäischen Kommission, Prof. Dr. Staudenmayer, Generaldirektion Justiz und Verbraucher, aus.

B. Begriffserklärungen

Die Arbeitsgruppe greift in ihrem Bericht auf verschiedene Begriffe aus den Bereichen der künstlichen Intelligenz, der Robotik und der autonomen Systeme zurück. Was genau unter diesen Begriffen zu verstehen ist, ist bislang noch nicht hinreichend genau definiert, so dass diese oftmals in verschiedenen Kontexten (leicht) unterschiedlich gebraucht werden. Dies hat zum Beispiel das Europäische Parlament in einer Entschließung dazu veranlasst, die Kommission für bestimmte Bereiche dazu aufzufordern, für eine Einheitlichkeit des Sprachgebrauchs zu sorgen, ohne dabei die Innovationsfreudigkeit zu hindern.[3] Die Ar-

---

[2] Zur Unterscheidung autonome – selbstlernende Systeme vgl. unter B. IV. und V.

[3] „Zivilrechtliche Regelungen im Bereich Robotik“ – Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)).

beitsgruppe hat sich aufgrund der bestehenden Unsicherheiten dazu entschlossen, ihren Ausführungen Definitionen voranzustellen, die sie den von ihr verwendeten Begrifflichkeiten beimisst.

I. Künstliche Intelligenz

Künstliche Intelligenz (KI)[4] bezeichnet Systeme mit einem „intelligenten“[5] Verhalten, die ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, um bestimmte Ziele zu erreichen. KI-basierte Systeme können rein softwaregestützt in einer virtuellen Umgebung arbeiten (z. B. Sprachassistenten, Bildanalysesoftware, Suchmaschinen, Sprach- und Gesichtserkennungssysteme), aber auch in Hardware-Systeme eingebettet sein (z. B. moderne Roboter, autonome Pkw, Drohnen oder Anwendungen des „Internet der Dinge“).[6]

II. Algorithmus

Ein Algorithmus bezeichnet eine genau definierte Rechen-, Handlungs- und/oder Verarbeitungsvorschrift zur Lösung eines Problems/Problemtyps. Dieser kann sowohl in menschlicher Sprache formuliert als auch zur Ausführung eines Computerprogramms geschrieben sein. Um die Definition eines Algorithmus zu erfüllen, darf dieser keine widersprüchliche Beschreibung enthalten (Eindeutigkeit), jeder Einzelschritt muss ausführbar sein (Ausführbarkeit), seine Beschreibung muss endlich sein (Finitheit), er muss auch nach endlich vielen Schritten ein Ergebnis liefern (Terminierung), er muss unter den gleichen Voraussetzungen stets das gleiche Ergebnis liefern (Determiniertheit) und er muss zu jedem Zeitpunkt der Ausführung nur eine Möglichkeit der Fortsetzung haben (Determinismus).[7]

---

[4] *Herberger*, „Künstliche Intelligenz“ und Recht - Ein Orientierungsversuch -, NJW 2018, 2825 - 2827, setzt sich ausführlich mit dem Begriff auseinander.

[5] *Spindler* führt in Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Systeme, CR 2015, 766 (767), zu recht aus, dass es immer noch fraglich sei, ob von Intelligenz und vor allem von autonomem Handeln gesprochen werden könne – insbesondere vor dem Hintergrund, was autonomes Handeln im Sinne der Betätigung des menschlichen Willens ausmache, nämlich der einerseits unabhängigen Entscheidung (was noch erfüllt wäre) und andererseits der sich selbst gesetzten Ziele, zu deren Umsetzung die Entscheidungen getroffen würden.

[6] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 25.4.2018 „Künstliche Inelligenz für Europa“ COM(2018) 237 final, S. 1.

[7] *Scheja*, Wie Unternehmen aufgrund der Umsetzung der Geschäftsgeheimnis-Richtlinie ihre Algorithmen wie auch Datenbestände besser schützen können, CR 2018, 485 (486).

III. Lernender Algorithmus

Ein lernender Algorithmus ist eine Rechen-, Handlungs- und/oder Verarbeitungsvorschrift zur Lösung eines Problems/Problemtyps, die im Sinne eines selbstlernenden Systems anhand von Beispielen Muster und Gesetzmäßigkeiten erkennt, die es nach Beendigung der Lernphase verallgemeinern und auf unbekannte Sachverhalte anwenden kann. Wenn es darum geht, einem Deep-Learning-Algorithmus beizubringen, Objekte einer bestimmten Kategorie zuzuordnen, legt man ihm eine große Zahl von beschrifteten Beispielobjekten (z. B. Bilder) vor, bei denen diese korrekt eingestuft sind (z. B. Bilder von Flugzeugen). Anschließend ist der Algorithmus in der Lage, auch solche Objekte korrekt einzuordnen, die ihm nie zuvor gezeigt wurden, wobei die Treffsicherheit in einigen Fällen höher liegt als beim Menschen.[8]

IV. Autonomes System

Wenn Systeme in der Lage sind, Aufgaben ohne menschliche Steuerung oder Aufsicht auszuführen, wird inzwischen oft von „autonomen" Systemen gesprochen. Diese sogenannten „autonomen" Systeme können sich in Form von High-Tech-Robotiksystemen oder als intelligente Software manifestieren. Oft werden sie unbeaufsichtigt in ihre Umwelt entlassen und können Dinge leisten, die ihre menschlichen Entwickler oder Besitzer nicht vorhergesehen haben.[9] Auf die Unterscheidung zwischen automatisierten und autonomen Fahrzeugen wird unter F. I. näher eingegangen.

---

[8] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 25.4.2018 „Künstliche Inelligenz für Europa" COM(2018) 237 final, S. 12.

[9] Europäische Gruppe für Ethik der Naturwissenschaften und der Neuen Technologien, Erklärung zu künstlicher Intelligenz, Robotik und „autonomen" Systemen, 2018, S. 7; verfügbar unter https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018_de.pdf (letzter Abruf: 11.2.2019).

V. Selbstlernendes System

Selbstlernende Systeme sind in der Lage, anhand von Beispielen, in denen sie Muster und Gesetzmäßigkeiten erkennen, die sie nach Beendigung der Lernphase verallgemeinern und auf unbekannte Sachverhalte anwenden können, sich selbst neue Strategien „beizubringen" und eigenständig nach neuen analysierbaren Informationen zu suchen. In diesem Sinne ist ihre Entscheidungsfindung nicht mehr nachvollziehbar und kann nicht mehr vom Menschen überprüft werden. Zum einen lässt sich nicht ermitteln, wie die Maschinen über die ersten Algorithmen hinaus ihre Ergebnisse erzielen. Zum anderen beruht ihre Leistung auf im Lernprozess verwendete Daten, die möglicherweise nicht mehr verfügbar oder zugänglich sind.[10] Auf diese Weise konnte sich zum Beispiel das Programm AlphaZero innerhalb von nur vier Stunden eigenständig zu einem Weltklassespieler entwickeln. Auf gleiche Weise war es dem Programm AlphaGo möglich, den menschlichen Go-Weltmeister zu schlagen, ohne dass es nachvollziehbar war, auf welche Weise sich das Programm die dafür erforderlichen Kenntnisse angeeignet hatte.

VI. Intelligente Roboter

Der Begriff „Roboter" geht auf ein Werk des tschechischen Schriftstellers Karel Čapek zurück und beschrieb lange Zeit die Idee des Menschen, intelligente Maschinen zu bauen – in den meisten Fällen Androiden mit menschlichen Zügen. Im Zuge der fortschreitenden Technisierung der Arbeitsabläufe kamen die Entwickler von Handhabungsgeräten auf die Idee, diese „Roboter" zu nennen. Ab diesem Zeitpunkt wurde der Begriff „Roboter" fast beliebig für verschiedene Geräte benutzt. So ist dann auch zum Beispiel nach der Definition der *Robotic Industries Association* ein Roboter ein programmierbares Mehrzweck-Handhabungsgerät für das Bewegen von Material, Werkstücken, Werkzeugen oder Spezialgeräten.[11] Eine feststehende Begriffsbestimmung gibt es auch heute noch nicht. Im Sinne der Entschließung des Europäischen Parlaments vom 16. Februar 2017[12] definiert die Arbeitsgruppe intelligente Roboter als „keine Le-

---

[10] Europäische Gruppe für Ethik der Naturwissenschaften und der Neuen Technologien, Erklärung zu künstlicher Intelligenz, Robotik und „autonomen" Systemen, 2018, S. 6/7; verfügbar unter https://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018_de.pdf (letzter Abruf: 11.2.2019).

[11] https://definitions.uslegal.com/r/robotics/ (letzter Abruf: 30.10.2018).

[12] „Zivilrechtliche Regelungen im Bereich Robotik" – Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)).

bewesen im biologischen Sinn“, die aber die Fähigkeit besitzen, ihr Verhalten und ihre Handlungen an ihre Umgebung anzupassen, die Autonomie über Sensoren und/oder über den Datenaustausch mit ihrer Umgebung (Interkonnektivität) und die Bereitstellung und Analyse dieser Daten erlangen können und die als optionales Kriterium über die Fähigkeit zum Selbstlernen durch Erfahrung und durch Interaktion verfügen.[13]

C. Bisherige Vorschläge und laufende Arbeiten

Mit Fragen der außervertraglichen Haftung bei autonomen Systemen beschäftigte sich in jüngster Zeit nicht nur die Länderarbeitsgruppe „Robotic Law“, sondern auch der Deutsche Bundestag, das Europäische Parlament, die Europäische Kommission und der Rat der Europäischen Union.

Am 20. Januar 2015 beschloss der JURI-Ausschuss des *Europäischen Parlaments*, eine Arbeitsgruppe zu rechtlichen Fragen im Zusammenhang mit der Entwicklung von Robotik und künstlicher Intelligenz in der Europäischen Union einzurichten. Der Schwerpunkt der Arbeitsgruppe sollte auf zivilrechtlichen Aspekten liegen. Auf Basis des Abschlussberichts der Arbeitsgruppe vom 31. Mai 2016 (Berichterstatterin: Mady Delveaux)[14] verabschiedete das Europäische Parlament am 16. Februar 2017 eine Entschließung mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik.[15] Das Parlament forderte die Kommission auf, „einen Vorschlag für ein Rechtsinstrument über rechtliche Fragen im Zusammenhang mit der Entwicklung und Verwendung von Robotik und KI, wie sie in den nächsten zehn bis 15 Jahren vorhersehbar ist, zu unterbreiten, und zwar kombiniert mit nicht-rechtlichen Instru-

---

[13] *Spindler* geht in seinem Aufsatz Roboter, Automation, künstliche Intelligenz, selbststeuernde Kfz – Braucht das Recht neue Haftungskategorien? - Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (Fn. 1) von dem etwas engeren Begriff des Roboters als eine automatisch kontrollierte, wiederprogrammierbare, zu mehreren Zwecken einsetzbare manipulierende Maschine aus. Diese Definition hebt den Grad der Autonomie allerdings nicht in dem Sinne hervor, wie er für die vorliegende Untersuchung gebraucht werden soll.

[14] Entwurf vom 31. Mai 2016 eines Berichts mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)); verfügbar unter (letzter Abruf: 11.2.2019):
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//DE.

[15] „Zivilrechtliche Regelungen im Bereich Robotik“ – Entschließung des Europäischen Parlaments vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik (2015/2103(INL)).

menten wie Leitlinien und Verhaltenskodizes".[16] Als Lösung schlug das Parlament die Einführung einer verschuldensunabhängigen Haftung oder einer Haftung basierend auf einer Risikobewertung[17] vor, jeweils kombiniert mit der Einführung einer Pflichtversicherung[18], ergänzt durch einen Fonds, der nicht versicherte Schäden abdecken soll[19]. Langfristig soll nach Ansicht des Europäischen Parlaments die Einführung eines „speziellen rechtlichen Status für Roboter" erwogen werden, „damit zumindest für die ausgeklügeltsten autonomen Roboter ein Status als elektronische Person festgelegt werden könnte, die für den Ausgleich sämtlicher von ihr verursachten Schäden verantwortlich wäre"[20]. Zu klären sei, ob bei der Entwicklung und Verwendung einer neuen Generation von Robotern, wie sie in den nächsten zehn bis 15 Jahren vorhersehbar sei, auch neue Grundsätze und Regeln für die Haftung erforderlich seien. Das Parlament forderte die Kommission zum gesetzgeberischen Tätigwerden auf, um Haftungsfragen zu klären, insbesondere bei selbstfahrenden Autos.

Am 22. März 2017 fand zum Thema „Künstliche Intelligenz und Robotik" eine Sachverständigenanhörung im *Deutschen Bundestag*, Ausschuss Digitale Agenda, statt. Dort wurden ebenfalls Fragen der Haftung thematisiert. Die Experten sahen Regelungsbedarf bei der Haftung für Schäden, die durch Systeme künstlicher Intelligenz verursacht werden. Die Mehrheit der angehörten Sachverständigen war der Meinung, dass die technologische Entwicklung eine Neuregelung von Haftungsfragen und Versicherungsmodellen erfordere.[21]

Am 10. Mai 2017 veröffentlichte die *Europäische Kommission* eine Mitteilung zu ihrer Halbzeitbilanz zur Strategie für einen digitalen Binnenmarkt, in der sie Haftungsfragen im Zusammenhang mit dem Internet der Dinge thematisierte. Sie teilte mit, prüfen zu wollen, ob es nötig sei, den gegenwärtigen Rechtsrahmen an neue technische Entwicklungen wie Robotik, Künstliche Intelligenz und 3D-Druck im Hinblick auf die zivilrechtliche Haftung anzupassen.[22]

Am 19. Oktober 2017 veröffentlichte der *Rat* Schlussfolgerungen zu Künstlicher Intelligenz und ersuchte die Kommission, bis Anfang 2018 ein europäisches Konzept für Künstliche Intelligenz und eine Initiative zur Stärkung der Rahmenbedingungen vorzulegen, damit die Europäische Union in die Lage versetzt

---

[16] Ziffer 51 der Entschließung.
[17] Ziffer 53 der Entschließung.
[18] Ziffer 57 der Entschließung.
[19] Ziffer 58 der Entschließung.
[20] Ziffer 59 Buchstabe f der Entschließung; hierzu: *Lohmann*, Ein europäisches Roboterrecht – überfällig oder überflüssig?, ZRP 2017, 168 ff.
[21] https://www.bundestag.de/dokumente/textarchiv/2017/kw12-pa-digitale-agenda/497340 (letzter Abruf: 11.2.2019).
[22] KOM(2017)228 endg., S. 14.

werde, „durch risikobasierte radikale Innovationen neue Märkte zu erschließen und die Führungsrolle ihrer Industrie zu bestätigen“. [23]

Am 25. April 2018 legte die *Kommission* eine „Mitteilung zur Künstlichen Intelligenz für Europa“ vor.[24] Die Kommission gab darin bekannt, sie wolle für die Entwicklung und Anwendung von Künstlicher Intelligenz einen geeigneten rechtlichen Rahmen gewährleisten und prüfen, ob die Haftungsvorschriften auf nationaler und europäischer Ebene vor dem Hintergrund der neuen Herausforderungen ihren Zweck erfüllen würden. Die Kommission kündigte an, zur Bewertung der Produkthaftungsrichtlinie[25] bis Mitte 2019 mit Unterstützung von Expertengruppen einen Auslegungsleitfaden herauszugeben. Außerdem kündigte sie an, bis Mitte 2019 einen Bericht zu veröffentlichen, der sich mit den Auswirkungen von Künstlicher Intelligenz, Internet der Dinge und Robotik auf den Haftungsrahmen sowie mit potentiellen Lücken befasse.

Im Herbst 2018 legte die Kommission den Entwurf einer Auslegungshilfe zur Produkthaftungsrichtlinie vor. Dieser Entwurf wurde im Laufe der Diskussion in der dazu tagenden Expertengruppe fortgeschrieben. Zum Zeitpunkt der Fertigstellung des Berichts durch die Arbeitsgruppe lag die endgültige Fassung der Auslegungshilfe noch nicht vor, sodass der Bearbeitung das vorläufige Konzeptpapier der Kommission vom 18. September 2018 zugrunde gelegt wurde.

---

[23] Tagung des Europäischen Rates (19. Oktober 2017) - Schlussfolgerungen, EUCO 14/17; verfügbar unter https://www.consilium.europa.eu/media/21602/19-euco-final-conclusions-de.pdf (letzter Abruf: 11.2.2019).

[24] KOM(2018)237 endg.

[25] Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte.

D. Zulassungsrecht

I. Einführung

Die Benutzung von autonomen Systemen kann Auswirkungen auf das Leben und die körperliche Unversehrtheit von Menschen haben. Da der Staat dazu verpflichtet ist, das Leben und die körperliche Unversehrtheit seiner Bürger zu schützen, kommt der Zulassung für die öffentliche Benutzung solcher Systeme auch eine verfassungsrechtliche Bedeutung zu.[26] Die Zulassung eines Fahrzeugs zum Straßenverkehr ist eine behördliche Erlaubnis, ein zulassungspflichtiges Fahrzeug auf öffentlichen Straßen in Betrieb zu setzen.[27] Das Zulassungsverfahren ist damit ein Steuerungsmechanismus, um die Risiken, die von der Benutzung bestimmter Produkte ausgehen, mit den verfassungsrechtlichen Anforderungen in Einklang bringen zu können. Das wird am Beispiel autonomer Kraftfahrzeuge im öffentlichen Verkehr oder auch beim Einsatz von computergesteuerter Medizintechnik im Gesundheitswesen besonders deutlich: Erst wenn bestimmte Kriterien geprüft wurden, kann die Nutzung von Kraftfahrzeugen oder Medizingeräten erlaubt werden. Die Festlegung solcher Kriterien bei autonomen Systemen befindet sich derzeit in der Diskussion. Im Hinblick auf im Verkehr eingesetzte autonome Fahrzeuge wird vertreten, dass es auch darauf ankomme, ob diese eine erhöhte Gefahr für die anderen Verkehrsteilnehmer darstellen oder ob hierdurch der Verkehr eher sicherer werde.[28]

Da eine Erlaubnis, ein Produkt in den Verkehr zu bringen, auch Auswirkungen auf das Haftungsrecht hat, ist das Zulassungsrecht in einem eigenen Abschnitt gesondert zu betrachten. Ausgehend von den in diesem Bericht untersuchten Themenfeldern des autonomen Fahrens und der Medizintechnik soll dabei zunächst der rechtliche Rahmen der Zulassung näher beleuchtet werden. Dabei wird auch auf Regelungen im Hinblick auf derzeit zu beachtende Sicherheitsstandards eingegangen. Anschließend werden Probleme aufgezeigt, denen sich das Zulassungsrecht stellen muss, um autonome Systeme in den Verkehr zu bringen. Die Lösung dieser Probleme ist auch für das Haftungsrecht von Bedeutung, da das Zulassungsrecht insoweit als Filter wirkt. Abschließend wird auf die derzeitige Entwicklung des Zulassungsrechts beim autonomen Fahren eingegangen.

---

[26] Oppermann/Stender-Vorwachs/*Stender-Vorwachs/Steege*, Grundrechtliche Implikationen des autonomen Fahrens, Autonomes Fahren, 2017, S. 253 ff. für das autonome Fahren.
[27] Hentschel/König/Dauer/*Dauer*, Straßenverkehrsrecht, § 1 StVG Rn. 13.
[28] Oppermann/Stender-Vorwachs/*Stender-Vorwachs/Steege*, Grundrechtliche Implikationen des autonomen Fahrens, Autonomes Fahren, 2017, S. 253 (257).

II. Zulassung von Fahrzeugen

1. Überblick

Das Recht der Fahrzeugzulassung bestimmt die Bedingungen, unter denen Fahrzeuge am Verkehr auf öffentlichen Straßen teilnehmen können.[29] Das Straßenverkehrsgesetz (StVG) formuliert in seinem § 1 Abs. 1 die entsprechenden Voraussetzungen. Danach müssen Kraftfahrzeuge und Anhänger, die auf öffentlichen Straßen in Betrieb gesetzt werden sollen, von der zuständigen Behörde (Zulassungsbehörde) zum Verkehr zugelassen sein. Die Zulassung erfolgt auf Antrag des Verfügungsberechtigten des Fahrzeugs bei Vorliegen einer Betriebserlaubnis, Einzelgenehmigung oder EG-Typgenehmigung durch Zuteilung eines amtlichen Kennzeichens.

Die Fahrzeugzulassungsverordnung (FZV) ist eine auf dem StVG basierende Rechtsverordnung, die auf die Zulassung von Kraftfahrzeugen mit einer bauartbedingten Höchstgeschwindigkeit von mehr als 6 km/h Anwendung findet.[30] Sie bestimmt in ihrem § 3 Abs. 1, dass diese Fahrzeuge auf öffentlichen Straßen nur in Betrieb gesetzt werden dürfen, wenn sie zum Verkehr zugelassen sind. Die Zulassung wird dabei auf Antrag erteilt, wenn das Fahrzeug einem genehmigten Typ entspricht oder eine Einzelgenehmigung erteilt ist und eine dem Pflichtversicherungsgesetz entsprechende Kraftfahrzeug-Haftpflichtversicherung besteht. In § 3 Abs. 2 FZV werden Fahrzeuge aufgeführt, für welche die Vorschriften über das Zulassungsverfahren keine Anwendung finden. Eine weitere Rechtsverordnung im Rahmen der Zulassung von Fahrzeugen ist die Straßenverkehrszulassungsverordnung (StVZO), die neben Vorschriften über die Zulassung von Fahrzeugen im Allgemeinen und Regelungen zur Betriebserlaubnis und Bauartgenehmigung auch Bau- und Betriebsvorschriften normiert.[31]

2. Arten der Genehmigung

Bei der Zulassung von Fahrzeugen wird zwischen Typengenehmigungen und Einzelgenehmigungen unterschieden. Eine Typengenehmigung erfolgt anhand eines Musterfahrzeugs des jeweiligen Typs entweder mit Geltung für die Mitgliedstaaten der EU (EG-Typgenehmigung nach § 2 Nr. 4 FZV) oder mit Geltung ausschließlich für die Bundesrepublik (nationale Typgenehmigung nach § 2

---

[29] *Arzt/Ruth-Schumacher*, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, NZV 2017, 57 (58).

[30] § 1 FZV.

[31] § 16 Abs. 1 StVZO („Zum Verkehr auf öffentlichen Straßen sind alle Fahrzeuge zugelassen, die den Vorschriften dieser Verordnung und der Straßenverkehrs-Ordnung entsprechen, soweit nicht für die Zulassung einzelner Fahrzeugarten ein Erlaubnisverfahren vorgeschrieben ist.“) findet Anwendung für die nicht unter die FZV fallenden Fahrzeuge.

Nr. 5 FZV). Die Einzelgenehmigung (§ 2 Nr. 6 FZV) bezieht sich nur auf ein Fahrzeug, das eine Einzelausführung darstellt, und gilt ebenfalls nur national.[32]

Mit einer Genehmigung wird bestätigt, dass das Fahrzeug den geltenden Anforderungen entspricht: Die EG-Typgenehmigung nach § 2 Nr. 4 FZV bescheinigt, dass der zur Prüfung vorgestellte Typ eines Fahrzeugs, eines Systems, eines Bauteils oder einer selbstständigen technischen Einheit in Anwendung der Richtlinien (EU) 2007/46/EG[33], 2002/24/EG[34] und 2003/37/EG[35] bzw. der Verordnungen (EU) Nr. 167/2013 und 168/2013[36] die einschlägigen Vorschriften und technischen Anforderungen erfüllt. Die nationale Typgenehmigung nach § 2 Nr. 5 FZV ist die behördliche Bestätigung, dass der zur Prüfung vorgestellte Typ eines Fahrzeugs, eines Systems, eines Bauteils oder einer selbstständigen technischen Einheit den geltenden Bauvorschriften entspricht und ist eine Betriebserlaubnis im Sinne des § 1 Abs. 1 StVG und eine Allgemeine Betriebserlaubnis im Sinne des § 20 StVZO. Die Einzelgenehmigung nach § 2 Nr. 6 FZV wiederum bestätigt, dass das betreffende Fahrzeug, System, Bauteil oder die selbstständige technische Einheit den geltenden Bauvorschriften entspricht und ist eine Betriebserlaubnis des § 1 Abs. 1 StVG und eine Einzelbetriebserlaubnis nach § 21 StVZO.

---

[32] *Arzt/Ruth-Schumacher*, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, NZV 2017, 57 (58).

[33] Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates vom 5. September 2007 zur Schaffung eines Rahmens für die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge.

[34] Richtlinie 2002/24/EG des Europäischen Parlaments und des Rates vom 18. März 2002 über die Typgenehmigung für zweirädrige oder dreirädrige Kraftfahrzeuge und zur Aufhebung der Richtlinie 92/61/EWG des Rates (ABl. L 124 vom 9.5.2002, S. 1) in der jeweils geltenden Fassung oder der Verordnung (EU) Nr. 168/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen.

[35] Richtlinie 2003/37/EG des Europäischen Parlaments und des Rates vom 26. Mai 2003 über die Typgenehmigung für land- oder forstwirtschaftliche Zugmaschinen, ihre Anhänger und die von ihnen gezogenen auswechselbaren Maschinen sowie für Systeme, Bauteile und selbstständige technische Einheiten dieser Fahrzeuge und zur Aufhebung der Richtlinie 74/150/EWG.

[36] Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen und Verordnung (EU) Nr. 168/2013 des Europäischen Parlements und des Rates vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- und dreirädrigen und vierrädrigen Fahrzeugen.

3. Regelungssystematik

Technische Anforderungen für Fahrzeuge und entsprechende Bauvorschriften ergeben sich aus nationalem Recht, europäischem Recht sowie aus völkerrechtlichen Regelungen. §§ 30 ff. StVZO enthalten nationale Bau- und Betriebsvorschriften. Die EG-Fahrzeuggenehmigungsverordnung (EG-FZV) setzt die Richtlinie 2007/46/EG um. Dieser Richtlinie unterfallen die häufigsten im Straßenverkehr verwendeten Fahrzeuge.[37]

Nach Art. 1 Richtlinie 2007/46/EG soll die Richtlinie einen harmonisierten Rahmen mit den Verwaltungsvorschriften und allgemeinen technischen Anforderungen für die Genehmigung aller in ihren Geltungsbereich fallenden Neufahrzeuge und der zur Verwendung in diesen Fahrzeugen bestimmten Systeme, Bauteile und selbstständigen technischen Einheiten schaffen. Dieser Richtlinie kommt damit eine grundlegende Bedeutung zu, da sie ein einheitliches Genehmigungsverfahren vorsieht, welches auf dem Grundsatz der vollständigen Harmonisierung der technischen Merkmale beruht.[38] Ziel ist insbesondere die Gewährleistung eines hohen Maßes an Verkehrssicherheit durch vollständige Harmonisierung der technischen Anforderungen auch im Hinblick auf den Bau der Fahrzeuge.[39] Für die dieser Richtlinie unterfallenden EG-Typgenehmigungen enthalten Art. 8 ff. Bestimmungen zum Verfahren. Diese Regelungen verweisen auf weitere Rechtsakte mit Bestimmungen zur Beschaffenheit. Dabei handelt es sich um eine Vielzahl weiterer Richtlinien und Verordnungen sowie Regelungen der Wirtschaftskommission für Europa der Vereinten Nationen (UN/ECE-Regelungen).

Die Grundlage dieser Regelungen ist ein Übereinkommen der Vereinten Nationen[40], welchem die EU mit Wirkung vom 23. Januar 1998 beigetreten ist[41]. Das Übereinkommen schafft einen rechtlichen Rahmen für die Etablierung technischer Regelungen. Diese wurden durch das „World Forum for Harmonization of Vehicle Regulations – WP.29“ verabschiedet, welches aus Vertretern der Parteien des Übereinkommens besteht. In Anhang IV der Richtlinie 2007/46/EG findet sich eine Aufstellung der für die EG-Typgenehmigung für Fahrzeuge anzu-

---

[37] *Arzt/Ruth-Schumacher*, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, NZV 2017, 57 (59).
[38] EuGH, Urt. v. 20.3.2014 (Kommission ./. Polen), Rs. C-639/11, Rn. 34; *Arzt/Ruth-Schumacher*, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, NZV 2017, 57 (59).
[39] EuGH, Urt. v. 20.3.2014 (Kommission ./. Polen), Rs. C-639/11, Rn. 35.
[40] Übereinkommen der Vereinten Nationen vom 20. März 1958 über die Annahme harmonisierter technischer Regelungen für Radfahrzeuge, Ausrüstungsgegenstände und Teile, die in Radfahrzeuge eingebaut oder dafür verwendet werden können, und die Bedingungen für die gegenseitige Anerkennung von Genehmigungen, die nach diesen Regelungen erteilt wurden.
[41] Beschluss 97/836/EG des Rates vom 27. November 1997.

wendenden Vorschriften. In Teil I des Anhangs IV finden sich UN/ECE-Regelungen, denen die EU beigetreten ist. Sie sind zu den gleichen Bedingungen wie die Einzelrichtlinien und Einzelverordnungen Bestandteil der EG-Typgenehmigung für Fahrzeuge.[42] Die in Anhang IV Teil II aufgeführten UN/ECE-Regelungen werden als gleichwertig mit den entsprechenden Einzelrichtlinien oder Einzelverordnungen anerkannt, sofern sie denselben Geltungsbereich und Gegenstand betreffen.[43]

Ein weiterer bedeutsamer völkerrechtlicher Vertrag ist das Wiener Übereinkommen über den Straßenverkehr (WÜ)[44], welches sowohl technische Anforderungen an Fahrzeuge als auch Regelungen für das Verhalten der Verkehrsteilnehmer fomuliert[45].

Im Ergebnis sind im Hinblick auf die Erteilung der Betriebserlaubnis von Fahrzeugen damit letztlich vor allem europarechtliche Regelungen entscheidend: § 19 Abs. 1 S. 2 StVZO bestimmt, dass die Betriebserlaubnis auch zu erteilen ist, wenn das Fahrzeug anstelle der Vorschriften der StVZO bestimmte Anforderungen des europäischen Rechts erfüllt. Damit stehen nicht die nationalen Bau- und Betriebsvorschriften in §§ 30 ff. StVZO im Blickpunkt, sondern die europäischen Regelungen bzw. die UN/ECE-Regelungen, die als verbindliches EU-Recht anerkannt werden.

4. Sicherheitsstandards

§ 30 Abs. 1 StVZO regelt zur Beschaffenheit der Fahrzeuge, dass diese so gebaut und ausgerüstet sein müssen, dass ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet, behindert oder belästigt (Nr. 1) und die Insassen insbesondere bei Unfällen vor Verletzungen möglichst geschützt sind und das Ausmaß und die Folgen von Verletzungen möglichst gering bleiben (Nr. 2). Aus den Formulierungen „niemanden (…) mehr als unvermeidbar gefährdet, behindert oder belästigt“ kann geschlussfolgert werden, dass ein absoluter Ausschluss von Gefährdungen, Behinderungen oder Belästigungen nicht erforderlich ist. Zudem sollen das Ausmaß und die Folgen von Verletzungen „möglichst gering“ bleiben. Auch dies zeigt, dass trotz eines Verletzungsrisikos bei Benutzung eine Zulassung des Fahrzeugs möglich ist.

---

[42] Art. 34 Abs. 1 S. 1 RL 2007/46/EG; vgl. insoweit auch Anhang XI für Merkmale von Fahrzeugen mit besonderer Zweckbestimmung.
[43] Art. 35 Abs. 1 S. 1 RL 2007/46/EG.
[44] Übereinkommen vom 8. November 1968 über den Straßenverkehr.
[45] Hierbei ist jedoch umstritten, ob den verhaltensrechtlichen Vorschriften eine zulassungsrechtliche Wirkung zukommt. Nur die Bundesrepublik ist Vertragspartner des WÜ, nicht jedoch die EU selbst, und das europäische Recht geht dem innerstaatlichen Recht wegen seines allgemeinen Anwendungsvorrangs vor, vgl. dazu *Arzt/Ruth-Schumacher*, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, NZV 2017, 57 (61).

Auch europarechtlichen Regelungen sind zum Maß der Sicherheit Hinweise zu entnehmen: VO (EG) 661/2009[46] bestimmt Sicherheitsanforderungen für die Typengenehmigung von Kraftfahrzeugen. Hier heißt es in Art. 5 Abs. 1, dass die Hersteller sicherstellen, dass Fahrzeuge so konstruiert, gefertigt und zusammengebaut sind, dass die Gefahr von Verletzungen der Fahrzeuginsassen und anderer Verkehrsteilnehmer möglichst gering ist. Auch hier ist zu schlussfolgern, dass keine absolute Sicherheit gewährleistet werden muss. Eine entsprechende Schlussfolgerung lässt sich beispielsweise auch aus der VO (EU) Nr. 168/2013[47] ziehen, die in Art. 22 Anforderungen für die funktionale Sicherheit von Fahrzeugen festlegt. Auch hier heißt es, dass der Hersteller sicherstellt, dass die von ihm hergestellten Fahrzeuge so ausgelegt, gefertigt und zusammengebaut sind, dass die Verletzungsgefahr für Fahrzeuginsassen und andere Verkehrsteilnehmer möglichst gering ist. In Art. 3 Nr. 22 dieser Verordnung wird „funktionale Sicherheit" als das Fehlen eines unzumutbaren Risikos der Verletzung oder Gesundheitsschädigung von Personen oder der Verletzung oder Beschädigung von Eigentum aufgrund einer Gefährdung durch die Fehlfunktion mechanischer, hydraulischer, pneumatischer, elektrischer oder elektronischer Systeme, Bauteile oder selbstständiger technischer Einheiten definiert. Auch das legt nahe, dass die Zulassung Risiken beim Inverkehrbringen von Fahrzeugen nicht ausschließt.

So ist im Ergebnis auch der EuGH in der Entscheidung Kommission ./. Polen[48] zu verstehen. In dieser Entscheidung wollte der EU-Mitgliedstaat Polen die Benutzung von Fahrzeugen mit Lenkanlagen auf der rechten Fahrzeugseite von der Umsetzung der Lenkanlagen auf die linke Seite abhängig machen. Personen, die in Polen eine Zulassung für Personenkraftwagen aus dem Vereinigten Königreich oder Irland – mithin Mitgliedstaaten mit Linksverkehr – begehrten, wären so zu einem kostspieligen Umbau gezwungen gewesen, was der EuGH ablehnte. Das Gericht war im Ergebnis der Ansicht, dass bei der Zulassung ein gewisses Risiko im Zusammenhang mit dem Straßenverkehr vom Gesetzgeber in Kauf genommen werden kann.[49]

---

[46] Verordnung (EG) Nr. 661/2009 vom 13. Juli 2009 über die Typgenehmigung von Kraftfahrzeugen, Kraftfahrzeuganhängern und von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge hinsichtlich ihrer allgemeinen Sicherheit.

[47] Verordnung (EU) Nr. 168/2013 vom 15. Januar 2013 über die Genehmigung und Marktüberwachung von zwei- oder dreirädrigen und vierrädrigen Fahrzeugen. Entsprechende Regelungen finden sich für land- und forstwirtschaftliche Fahrzeuge in Art. 17 und Art. 18 der Verordnung (EU) Nr. 167/2013 des Europäischen Parlaments und des Rates vom 5. Februar 2013 über die Genehmigung und Marktüberwachung von land- und forstwirtschaftlichen Fahrzeugen.

[48] EuGH, Urt. v. 20.3.2014 (Kommission ./. Polen), Rs. C-639/11.

[49] EuGH, Urt. v. 20.3.2014 (Kommission ./. Polen), Rs. C-639/11, Rn. 42.

III. Zulassung von Medizinprodukten

1. Überblick

Das Inverkehrbringen von Medizinprodukten regelt das Medizinproduktegesetz (MPG). Zweck dieses Gesetzes ist es, den Verkehr mit Medizinprodukten zu regeln und dadurch für die Sicherheit, Eignung und Leistung der Medizinprodukte sowie die Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritten zu sorgen.[50] Das Gesetz findet für Medizinprodukte, nicht jedoch für Arzneimittel im Sinne des § 2 des Arzneimittelgesetzes Anwendung.[51]

Grundsätzlich dürfen Medizinprodukte in Deutschland gemäß § 6 Abs. 1 MPG nur in den Verkehr gebracht oder in Betrieb genommen werden, wenn sie mit einer CE-Kennzeichnung versehen sind. Eine CE-Kennzeichnung darf ein Medizinprodukt nur erhalten, wenn die grundlegenden Anforderungen nach § 7 MPG erfüllt sind und ein für das jeweilige Medizinprodukt vorgeschriebenes Konformitätsbewertungsverfahren durchgeführt worden ist.[52] Gelten für das Medizinprodukt noch andere Rechtsvorschriften als diejenigen des MPG, darf eine CE-Kennzeichnung erst erfolgen, wenn auch die Voraussetzungen der anderen Rechtsvorschriften erfüllt sind.[53]

Die grundlegenden Anforderungen unterscheiden sich nach der Art der Medizinprodukte. Dabei wird zwischen aktiven implantierbaren Medizinprodukten, In-vitro-Diagnostika und sonstigen Medizinprodukten[54] unterschieden. Maßgeblich waren insoweit Richtlinie 90/385/EWG[55] (Aktive implantierbare Medizinprodukte), Richtlinie 98/79/EG[56] (In-vitro-Diagnostika) und Richtlinie 93/42/EWG[57] (Sonstige Medizinprodukte). § 7 Abs. 1 MPG verweist insoweit jeweils auf die in den Richtlinien formulierten Anforderungen.[58] Die Richtlinien

---

[50] § 1 MPG.
[51] § 2 Abs. 5 Nr. 1 MPG.
[52] § 6 Abs. 2 S. 1 MPG.
[53] § 6 Abs. 3 S. 1 MPG.
[54] Sonstige Medizinprodukte werden gemäß § 13 MPG nach den Klassifizierungsregeln des Anhangs IX der Richtlinie 93/42/EWG klassifiziert.
[55] Richtlinie 90/385/EWG vom 20. Juni 1990 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über aktive implantierbare medizinische Geräte.
[56] Richtlinie 98/79/EG des Europäischen Parlaments und des Rates vom 27. Oktober 1998 über In-vitro-Diagnostika.
[57] Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte.
[58] Für aktive implantierbare Medizinprodukte wird auf die Anforderungen des Anhangs 1 der Richtlinie 90/385/EWG, für In-vitro-Diagnostika auf die Anforderungen des Anhangs I der

90/385/EWG und 93/42/EWG wurden überarbeitet und in die europäische Medizinprodukteverordnung (Medical Device Regulation – MDR)[59] überführt, was sich insbesondere nach Ablauf der Übergangsfrist im Jahr 2020 auswirkt.[60] Zudem müssen Medizinprodukte, die auch Maschinen im Sinne der Richtlinie 2006/42/EG sind, grundlegenden Gesundheits- und Sicherheitsanforderungen nach dieser Richtlinie entsprechen, sofern diese spezifischer sind als die Gesundheits- und Sicherheitsanforderungen nach Richtlinie 93/42/EWG oder Richtlinie 90/385/EWG.[61]

2. Konformitätsbewertungsverfahren

Die Durchführung der Konformitätsbewertungsverfahren ist in einer Rechtsverordnung nach § 37 Abs. 1 MPG – der Verordnung über Medizinprodukte (MPV) – geregelt. Konformitätsbewertungsverfahren für aktive implantierbare Medizinprodukte regelt § 4 MPV, für In-vitro-Diagnostika § 5 MPV und für sonstige Medizinprodukte § 7 MPV. Die Prüfung der Konformitätsbewertungsverfahren erfolgt durch sogenannte „Benannte Stellen". Das sind für die Durchführung von Prüfungen und die Erteilung der maßgeblichen Bescheinigungen vorgesehene Stellen.[62] Hersteller können sich an eine Benannte Stelle wenden, die für das jeweilige Verfahren bzw. Produkt vorgesehen ist. Das sind regelmäßig private Unternehmen, wie z.B. der TÜV, die auf Antrag nach § 15 MPG staatlich autorisiert werden.[63] Die Benennung und Überwachung der Benannten Stellen

---

Richtlinie 98/79/EG und für die sonstigen Medizinprodukte auf die Anforderungen des Anhangs I der Richtlinie 93/42/EWG verwiesen.

[59] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates.

[60] Vgl. Art. 120 Abs. 1 der Verordnung (EU) 2017/745, wonach ab dem 26.5.2020 jede Veröffentlichung einer Notifizierung gemäß den Richtlinien 90/385/EWG und 93/42/EWG in Bezug auf eine Benannte Stelle ungültig wird.

[61] § 7 Abs. 2 MPG. § 7 Abs. 3 MPG stellt zudem die Voraussetzung auf, dass bei Produkten, die auch zur Verwendung entsprechend der Vorschriften über persönliche Schutzausrüstungen nach Richtlinie 89/686/EWG bestimmt sind, die Gesundheits- und Sicherheitsanforderungen dieser Richtlinie erfüllt werden müssen.

[62] § 3 Nr. 20 MPG.

[63] Im November 2018 wurde eine internationale Recherche mehrerer Journalisten veröffentlicht, in der erhebliche Kritik am Zulassungsverfahren und insbesondere der Zuständigkeit privater Unternehmen für die Durchführung der Konformitätsbewertungsverfahren und den Anforderungen an die klinischen Bewertungen geäußert wurde. Vgl. dazu beispielsweise die Veröffentlichungen im Internet: https://projekte.sueddeutsche.de/implantfiles/politik/implantfiles-sueddeutsche-de-e952128;https://www.daserste.de/information/reportage-dokumentation/dokus/sendung/ausser-kontrolle-folge-7-102.html.

ist in §§ 15 - 18 MPG geregelt und erfolgt durch die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten (ZLG).[64]

3. Sicherheitsstandards

Nach § 4 Abs. 1 MPG ist insbesondere das Inverkehrbringen von Medizinprodukten verboten, wenn der begründete Verdacht besteht, dass sie die Sicherheit und Gesundheit von Patienten, Anwendern oder Dritten über ein nach den Erkenntnissen der medizinischen Wissenschaften vertretbares Maß hinausgehend unmittelbar oder mittelbar gefährden. § 19 Abs. 1 MPG regelt, dass die Eignung von Medizinprodukten für den vorgesehenen Verwendungszweck durch eine klinische Bewertung zu belegen ist, welche die Beurteilung von unerwünschten Wirkungen sowie die Annehmbarkeit des in den grundlegenden Anforderungen der Richtlinien 90/385/EWG und 93/42/EWG genannten Nutzen-/Risiko-Verhältnisses einschließen muss. Die klinische Prüfung eines Medizinprodukts bei Menschen darf nach § 20 Abs. 1 S. 4 Nr. 1 MPG nur durchgeführt werden, wenn und solange die Risiken, die mit ihr für die Person verbunden sind, bei der sie durchgeführt werden soll, gemessen an der voraussichtlichen Bedeutung des Medizinprodukts für die Heilkunde ärztlich vertretbar sind. Dabei sind die potentiellen Risiken der Produkte maßgeblich, die indes nicht ausgeschlossen werden. Vielmehr wird auf das Nutzen-/Risiko-Verhältnis abgestellt, was im europäischen Recht spezifiziert ist.

Die Richtlinie 93/42/EWG normiert für sonstige Medizinprodukte in ihrem Art. 2 das Inverkehrbringen und die Inbetriebnahme. Danach müssen die Mitgliedstaaten alle erforderlichen Maßnahmen treffen, damit Produkte nur in den Verkehr gebracht werden dürfen, wenn sie die Sicherheit und die Gesundheit der Patienten, der Anwender und gegebenenfalls Dritter bei sachgemäßer Installation, Instandhaltung und ihrer Zweckbestimmung entsprechender Verwendung nicht gefährden.[65] In Anhang I der Richtlinie 90/385/EWG für aktive implantierbare Medizinprodukte steht ausdrücklich, dass etwaige unerwünschte Nebenwirkungen unter Berücksichtigung der vorgegebenen Leistungen keine unvertretbaren Risiken darstellen dürfen.[66] Auch in der Richtlinie 98/79/EG zu In-

---

[64] https://www.zlg.de/medizinprodukte/dokumente/stellenlaboratorien/benannte-stellen.html.

[65] Art. 3 der Richtlinie 93/42/EWG verweist auf Anhang I, der grundlegende Anforderungen enthält. Die im November 2018 veröffentlichte Recherche (vgl. Fn. 62) kritisiert insoweit auch die Durchführung der nach Anhang X der Richtlinie durchzuführenden klinischen Bewertungen, da die hierfür vorhandene Leitlinie MEDDEV 2.7.1 beispielsweise auch den Nachweis der Gleichwertigkeit mit vergleichbaren Medizinprodukten zulässt („Equivalent device“).

[66] Anhang I, Ziff. 5 Richtlinie 90/385/EWG. In dieser Richtlinie finden sich Regelungen zu den klinischen Bewertungen in Anhang 7. Die Leitlinie MEDDEV 2.7.1 (vgl. Fn. 66) findet auch hier Anwendung.

vitro-Diagnostika finden sich Regelungen zur Risikominimierung[67], die ebenfalls den Schluss zulassen, dass ein vollständiger Ausschluss des Risikos nicht gefordert wird. Im Ergebnis können damit auch Medizinprodukte zugelassen werden, denen Risiken anhaften, wobei die Art des jeweiligen Medizinprodukts für die Beurteilung maßgebend ist.[68]

IV. Autonome Systeme

1. Problemaufriss

Die Frage, welcher Regelungsbedarf besteht, wenn autonome Systeme zugelassen werden sollen, befindet sich in der Diskussion. Der aufgezeigte Rahmen wird die Grundlage entsprechender Regelungen bilden. Indes ist es nicht unproblematisch, Anforderungen für die Zulassung autonomer Systeme zu bestimmen. Das zeigt sich am Beispiel des autonomen Fahrens besonders deutlich und betrifft beispielsweise die Frage, wie im Rahmen des Zulassungsverfahrens die Komponenten, die ein autonomes Fahren ermöglichen, geprüft werden sollen. Sollen gesonderte Sicherheitsstandards angelegt werden? Wie sollen diese bestimmt werden? Wie wird mit Verkehrssituationen umgegangen, zu deren Auflösung es menschlicher Kommunikation bedarf? Zu bedenken ist auch, dass im Vorfeld nicht alle erdenklichen Verkehrssituationen bekannt sein werden und entsprechend nachgestellt bzw. behandelt werden können.[69] Hier liegen vor allem praktische und technische Fragestellungen zugrunde, deren Ergebnisse bei Vorliegen von Antworten in entsprechende Regelungen transformiert werden müssen.

Aber auch ethische Fragen sind in diesem Rahmen zu bedenken. So stellt sich zum Beispiel auch die sogenannte „Dilemma-Problematik“: Wie soll sich das autonome Fahrzeug in Situationen verhalten, in denen ein Schaden unvermeidbar ist? Soll es vorrangig die Fahrzeuginsassen oder die anderen Verkehrsteil-

---

[67] Vgl. insoweit Anhang I, Ziff. 2.1, 2.5., 2.7 Richtlinie 98/79/EG.

[68] Davon wird auch künftig auszugehen sein, denn in Anhang I der Verordnung (EU) 2017/745 finden sich grundlegende Sicherheits- und Leistungsanforderungen, die einen solchen Schluss ebenfalls zulassen. Hier heißt es in Kapitel I Nr. 1 unter anderem, dass die Produkte sicher und wirksam sind und weder den klinischen Zustand und die Sicherheit der Patienten noch die Sicherheit und die Gesundheit der Anwender oder gegebenenfalls Dritter gefährden, wobei etwaige Risiken im Zusammenhang mit ihrer Anwendung gemessen am Nutzen für den Patienten vertretbar und mit einem hohen Maß an Gesundheitsschutz und Sicherheit vereinbar sein müssen. Dabei ist der allgemein anerkannte Stand der Technik zugrunde zu legen.

[69] Vgl. Oppermann/Stender-Vorwachs/*Wagner,* Technik autonomer Fahrzeuge – eine Einführung, Autonomes Fahren, 2017, S. 1 (29 f.).

nehmer schützen?[70] Diese grundsätzlichen Fragen sollten soweit wie möglich im Zulassungsverfahren beantwortet werden. Andernfalls würden diese Wertentscheidungen – ohne entsprechende Vorgaben – durch die Hersteller selbst getroffen werden müssen.

Fraglich ist auch, wie Systeme, welche in der Lage sein werden, ihr Verhalten zu ändern, geprüft werden sollen.[71] Ausgehend von der hier verwendeten Begriffsdefinition kann ein solches System Dinge leisten, die ihre menschlichen Entwickler und Besitzer nicht vorhergesehen haben.[72] Entwickelt solch ein System ein „Innenleben", könnte das Verhalten des Systems unter Umständen unberechenbar sein.[73] Was kann passieren, wenn das System eigene Entscheidungen trifft? Darf ein solches System vor dem Hintergrund des Schutzes von Leben und körperlicher Unversehrtheit überhaupt zugelassen werden? Diese Probleme stellen sich indes immer, wenn Entscheidungen von Systemen nicht mehr nachvollzogen werden können. Diese Fragen sind auch im Rahmen der Zulassung autonomer Systeme von Bedeutung, um bereits im Vorfeld Auswirkungen auf das Leben und die körperliche Unversehrtheit von Menschen zu vermeiden.

2. Filterfunktion des Zulassungsrechts

Für Medizingeräte findet sich in § 6 Abs. 4 MPG eine Regelung, die ausdrücklich festlegt, dass die Durchführung eines Konformitätsbewertungsverfahrens im Rahmen der Zulassung die zivil- und strafrechtliche Verantwortlichkeit des Verantwortlichen unberührt lässt. Damit ist ein solches Verfahren eine Mindestmaßnahme zur Sicherung der Funktionsfähigkeit und Leistungsfähigkeit von Medizinprodukten, führt indes nicht zu einer Entlastung aus der Verantwortung.[74] Eine spezielle Gefährdungshaftung nach dem MPG gibt es nicht, weshalb bei Medizinprodukten für Schäden und Produktfehler nach allgemeinen Regelungen gehaftet wird.[75] Wird beim Betrieb eines Kraftfahrzeugs ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt, sieht § 7 Abs. 1 StVG die verschuldensunabhängige Haftung des Fahrzeughalters und § 18 Abs. 1 StVG die verschuldensabhängige Haftung des Fahrers vor. Bei Produktfehlern der Fahrzeuge kommen Ansprüche gegen den Produzenten aus Produkt- und Produzentenhaftung in Betracht. Diese Regelungen greifen auch bei Fahrzeugen, die für den Verkehr zugelassen sind.

---

[70] *Steiner*, Fahren ohne Fahrer im Fokus der Rechtswissenschaft, DAR 2017, S. 359 (360).
[71] In diesem Sinn auch Oppermann/Stender-Vorwachs/*Wagner*, Technik autonomer Fahrzeuge – eine Einführung, Autonomes Fahren 2017, S. 1 (30).
[72] Vgl. oben unter B. IV.
[73] Oppermann/Stender-Vorwachs/*Beck*, Selbstfahrende Fahrzeuge – aktuelle Probleme der (strafrechtlichen) Fahrlässigkeitshaftung, Autonomes Fahren, 2017, S. 33 (37).
[74] Spickhoff/*Lücker*, Medizinrecht, 2014, MPG, § 6 Rn. 9.
[75] Spickhoff/*Lücker*, Medizinrecht, 2014, MPG, § 6 Rn. 9.

Damit führt auch die Zulassung von Fahrzeugen grundsätzlich nicht zu einer Verantwortungsentlastung des Herstellers. Insoweit ist ein Gleichlauf mit den angesprochenen Sicherheitsstandards bei zugelassenen Fahrzeugen bzw. zugelassener Medizintechnik festzustellen: Diese schließen Risiken beim Inverkehrbringen von Fahrzeugen nicht aus. Verwirklicht sich dieses Risiko, greifen die jeweiligen Haftungstatbestände.

Gleichwohl steht die Frage der Zulassung auch im Zusammenhang mit der Frage der Haftung bei von diesen Systemen verursachten Schäden. Je höhere Anforderungen an die Zulassung autonomer Fahrzeuge gestellt werden, desto weniger Haftungsansprüche entstehen tatsächlich. Je weniger streng diese Anforderungen sind, desto öfter ist die Haftungsfrage von Relevanz. Dieses gegenseitige Wechselverhältnis wird maßgeblich durch die Anforderungen geprägt, welche das Zulassungsrecht vorgibt: Wird ein autonomes System aufgrund der damit einhergehenden Risiken nicht zugelassen, so stellt sich die Frage der Haftung für dieses System letztlich nicht.

Im Ergebnis kann die Zulassung eines autonomen Systems damit zwar nicht eine Haftung für von ihm verursachte Schäden verhindern, gleichwohl kann eine Zulassung entscheidenden Einfluss auf möglicherweise entstehende bzw. nicht entstehende Schäden haben. Das Zulassungsrecht hat damit eine Filterfunktion, indem es Systeme verhindern kann, die Schäden verursachen können. Ist ein solcher Schaden durch ein zugelassenes autonomes System eingetreten, gerät das Haftungsrecht in den Blickpunkt.

3. Exkurs: aktueller Stand beim autonomen Fahren

a. Zulassung

Für autonome Fahrzeuge wird vertreten, dass diese zugelassen werden können, wenn die nutzungsbedingte Selbstgefährdung zu rechtfertigen ist. Das soll dann der Fall sein, wenn die Fahrzeuge den aktuellen gesetzlich angepassten Sicherheitsanforderungen unterliegen und eine konkrete Todesgefahr ausgeschlossen werden kann.[76]

Der unter II. dargestellten Zulassung von Fahrzeugen ohne menschliche Steuerung standen bislang insbesondere Art. 8 Abs. 1, Art. 8 Abs. 5 und Art. 13 Abs. 1 WÜ entgegen: Nach Art. 8 Abs. 1 WÜ muss jedes Fahrzeug, das sich in Bewegung befindet, einen Führer haben. Art. 8 Abs. 5 WÜ fordert die jederzeitige Beherrschbarkeit des Fahrzeugs durch den Fahrzeugführer und Art. 13 Abs. 1 WÜ die Beherrschbarkeit des Fahrzeugs zur Erfüllung der Sorgfaltspflichten,

---

[76] So im Ergebnis Oppermann/Stender-Vorwachs/*Stender-Vorwachs/Steege*, Grundrechtliche Implikationen des autonomen Fahrens, Autonomes Fahren, 2017, S. 253 (287).

um in der Lage zu sein, alle ihm obliegenden Fahrbewegungen auszuführen. Nach einer Änderung des WÜ gelten jedoch die Voraussetzungen der Art. 8 Abs. 5 WÜ und Art. 13 Abs. 1 WÜ mit einer neu ergänzten Regelung des Abs. 5bis in Art. 8 als erfüllt, wenn Fahrzeugsysteme den einschlägigen (technischen) UN/ECE-Regelungen entsprechen oder die Systeme so gestaltet sind, dass sie durch den Fahrer übersteuerbar oder deaktivierbar sind.[77] Diese Änderung erfolgte speziell vor dem Hintergrund, Rechtssicherheit hinsichtlich bereits im Verkehr befindlicher Assistenz- bzw. automatisierter Systeme herzustellen und die weitere Entwicklung automatisierter Fahrsysteme zu unterstützen.[78] Derzeit arbeitet das „World Forum for Harmonization of Vehicle Regulations – WP.29" an einer Änderung der für diesen Bereich maßgeblichen UN/ECE-Regelungen: So wurde nunmehr die Arbeitsgruppe für automatisierte/autonome und vernetzte Fahrzeuge (GRVA) gegründet.[79] Insbesondere die UN/ECE-Regelung 79[80] zu Lenkanlagen ist in diesem Zusammenhang zu überarbeiten.[81]

Neben der Schaffung solcher Regelungen stellen sich auch die bereits aufgeworfenen Fragen der Bestimmung konkreter Anforderungen an die Zulassung. Das Bundesministerium für Wirtschaft und Energie (BMWi) fördert beispielsweise das Gemeinschaftsprojekt PEGASUS, ein „Projekt zur Etablierung von generell akzeptierten Gütekriterien, Werkzeugen und Methoden sowie Szenarien und Situationen zur Freigabe hochautomatisierter Fahrfunktionen". Das bis 2019 angelegte Forschungsprojekt dient der Entwicklung von einheitlichen Qualitätsstandards und Methoden zur Zulassung von automatisierten Fahrfunktionen. Zentrale Fragen sind dabei: Welche Rolle wird der Faktor Mensch in Zukunft spielen? Was muss die Technologie garantieren? Und wie kann das Zusammenspiel von Mensch und Technik optimal gestaltet werden?[82] Daneben gibt es auch auf europäischer Ebene entsprechende Untersuchungen, wie die Initiative „Prospective

---

[77] Die Änderung des Wiener Übereinkommens ist am 23. März 2016 in Kraft getreten. Vgl. hierzu auch das Gesetz zur Änderung der Artikel 8 und 39 des Übereinkommens vom 8. November 1968 über den Straßenverkehr vom 7. Dezember 2016, BGBl. II 2016, 1306.

[78] Gesetzentwurf der Bundesregierung vom 6. Mai 2016 zur Änderung der Artikel 8 und 39 des Übereinkommens vom 8. November 1968 über den Straßenverkehr, BT-Drs. 243/16, S. 2.

[79] Die Arbeitsgruppe ist Nachfolger der Arbeitsgruppe für Brems- und Fahrwerk (GRRF). Vgl. dazu https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/ECE-TRANS-WP.29-GRVA-2018-01e.pdf

[80] UN/ECE-Regelung 79: Einheitliche Bestimmungen für die Genehmigung von Fahrzeugen in Bezug auf die Lenkankage.

[81] *Arzt/Ruth-Schumacher*, Zulassungsrechtliche Rahmenbedingungen der Fahrzeugautomatisierung, NZV 2017, 57 (60).

[82] Zu Rahmeninformationen über das Projekt im Forschungsinformationssystem (FIS) des BMVI https://www.forschungsinformationssystem.de/servlet/is/471754/?clsId0=276664&clsId1=276670&clsId2=276957 sowie auf der Website des Projektes unter https://www.pegasusprojekt.de/en/.

Effectiveness Assessment for Road Safety“ (P.E.A.R.S.), deren Fokus auf der Entwicklung von Standards zur künftigen Bewertung der Verkehrssicherheit für fahrzeugintegrierte aktive Sicherheitstechnologien liegt.[83] Einen Überblick über die europäischen und internationalen Initiativen im Bereich des automatisierten Fahrens findet man auch in der „Automated Driving Roadmap“ der ERTRAC-Arbeitsgruppe „Konnektivität und automatisiertes Fahren“.[84]

b. Datenspeicherung und Datensicherheit

Mit zunehmender Automatisierung nimmt der Umfang im Fahrzeug generierter Daten zu.[85] Zur Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion finden sich Regelungen in § 63a und § 63b StVG. In § 63a Abs. 1 StVG wird zunächst festgestellt, dass Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben speichern, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt. Diese Daten müssen den für die Ahndung von Verkehrsverstößen zuständigen Behörden auf deren Verlangen übermittelt und dürfen durch diese gespeichert und genutzt werden, wobei der Umfang der Datenübermittlung auf das notwendige Maß zu beschränken ist (§ 63a Abs. 2 StVG). Unter bestimmten Voraussetzungen hat der Fahrzeughalter die Übermittlung dieser Daten an Dritte zu veranlassen (§ 63a Abs. 3 StVG). § 63b StVG ermächtigt zudem zum Erlass von Rechtsverordnungen über die technische Ausgestaltung und den Ort des Speichermediums sowie die Art und Weise der Speicherung, den Adressaten der Speicherpflicht und Maßnahmen zur Sicherung der gespeicherten Daten gegen unbefugten Zugriff bei Verkauf des Kraftfahrzeugs. Zu erwähnen ist, dass der 56. Verkehrsgerichtstag 2018 die Empfehlung ausgesprochen hat, dass die Speicherung der in § 63a Abs. 1 StVG genannten Daten sowohl im Fahrzeug selbst als auch bei einem unabhängigen Dritten erfolgen und der Gesetzgeber unverzüglich Einzelheiten regeln sollte.[86]

---

[83] https://pearsinitiative.com.

[84] http://ertrac.org/uploads/documentsearch/id48/ERTRAC_Automated_Driving_2017.pdf. Das „European Road Transport Research Advisory Council“ (ERTRAC) ist eine von der Europäischen Kommission unterstützte Technologieplattform für den Straßenverkehr, vgl. http://ertrac.org/index.php?page=what-is-ertrac.

[85] *Klink-Straub/Straub*, Vernetzte Fahrzeuge – portable Daten, ZD 2018, 459 mit Beispielen.

[86] https://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_56_vgt.pdf.

Zu beachten wären neben datenschutzrechtlichen Aspekten[87] auch Fragen der „Security". Insbesondere für die Verkehrssicherheit ist die „Security" des Fahrzeugs – also die Sicherheit des Systems vor Angriffen von außen – von Bedeutung: In den USA gibt es insoweit den „Self-Drive Act" [88], der diesbezügliche Vorgaben setzt und sogar einen eigenen Abschnitt zur Thematik „Cybersecurity" enthält.[89] So müssen die Hersteller einen „Cybersecurity Plan" entwickeln, der schriftliche Cybersicherheitsrichtlinien in Bezug auf die Praktiken des Herstellers zur Erkennung und Reaktion auf Cyberangriffe, die Benennung eines Ansprechpartners für die Cybersicherheit, Verfahren zur Beschränkung des Zugangs zu automatisierten Antriebssystemen sowie die Schulung und Überwachung der Mitarbeiter umfasst. Die Cybersicherheitsrichtlinien müssen ein Verfahren zum Identifizieren, Bewerten und Mildern von Schwachstellen durch Cyberangriffe oder unbefugte Eingriffe sowie ein Verfahren zum Ergreifen von Präventiv- und Korrekturmaßnahmen beinhalten.[90] Entsprechende Regelungen erscheinen sinnvoll, um ein größtmögliches Maß an Verkehrssicherheit gewährleisten zu können. Zudem sieht der „Self-Drive Act" vor, dass ein „Privacy-Plan" entwickelt werden muss, aus dem hervorgeht, wie die Hersteller mit diesen Daten umgehen.[91] Ähnliche Pläne hat das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) mit einem sogenannten „Datenausweis" für Kraftfahrzeuge verfolgt, der unter anderem vollumfänglich und verständlich über Umfang und Häufigkeit der Datenerhebung sowie über die Nutzung und Weitergabe der Daten aufklären soll.[92]

Es besteht eine Wechselwirkung zwischen Haftungs- und Zulassungsrecht: Der Gesetzgeber hat die Aufgabe, durch das Zulassungsrecht die von automatisierten und autonomen Systemen ausgehenden Gefahren von vornherein auf ein gesellschaftlich akzeptiertes Maß zu begrenzen.

---

[87] *Klink-Straub/Straub*, Vernetzte Fahrzeuge – portable Daten, ZD 2018, 459; *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201.

[88] H.R.3388 - Self Drive Act, vgl. https://www.congress.gov/bill/115th-congress/house-bill/3388/text.

[89] Sec. 5: Cybersecurity of automated driving systems.

[90] Vgl. sec. 5 (a) H.R.3388 - Self Drive Act.

[91] Sec. 12. Privacy Plan required for highly automated vehicles: „Ein schriftlicher Datenschutzplan in Bezug auf das Sammeln, Verwenden, Teilen und Speichern von Informationen über Fahrzeughalter oder Insassen, die von einem hochautomatisierten Fahrzeug, einem Fahrzeug, das eine teilweise Fahrautomatisierung durchführt, oder einem automatisierten Antriebssystem gesammelt wurden."

[92] Strategiepapier „Digitale Souveränität" des Bundesministeriums für Verkehr und digitale Infrastruktur (BMVI) https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html.

E. Allgemeine Grundsätze zum Haftungsrecht bei autonomen Systemen

I. Vorbemerkung

Im außervertraglichen Schadensrecht gilt der Grundsatz „casum sentit dominus“, d.h. die Schadensfolgen trägt der Geschädigte selbst, sofern das Gesetz diese nicht einem anderen zuweist.[93] Die Haftung ist daher die Ausnahme, die ihrerseits der Begründung bedarf.[94] Das Schadensersatzrecht dient primär dem Ausgleich in rechtswidriger Weise erlittener Nachteile. Dabei werden aber nicht die Person oder das Vermögen an sich geschützt, sondern die Haftung knüpft an bestimmte Tatbestände an; eine „große“, das gesamte Deliktsrecht beherrschende Generalklausel existiert dagegen nicht.[95]

Jede zivilrechtliche Haftung setzt einen Zurechnungsgrund voraus. Das deutsche Zivilrecht kennt in diesem Zusammenhang verschiedene Prinzipien der Schadenszurechnung. Grundform der Zurechnung ist das Verschuldensprinzip. Allerdings kennt das Gesetz auch eine Haftung, ohne dass den Schuldner ein Verschulden an der Rechtsgutsverletzung trifft. An dem Erfordernis eines Verschuldens fehlt es insbesondere in den Fällen der Gefährdungshaftung. Das BGB von 1900 sah lediglich einen Fall der Gefährdungshaftung vor, und zwar die Tierhalterhaftung in § 833 BGB. Im Übrigen hielten die Schöpfer des BGB die Gefährdungshaftung für systemfremd; Schadensersatz wurde nur bei Verschulden gewährt. Mit der fortlaufenden Schaffung neuer Tatbestände, die eine Gefährdungshaftung vorsehen, hat der Gesetzgeber in der Vergangenheit auf die Gefahren der modernen Technik reagiert.[96]

Im Folgenden wird untersucht, welche Wertungsprinzipien der geltenden Verschuldens- und Gefährdungshaftung zugrunde liegen und ob und inwieweit sie taugliche Instrumente dafür sein können, diejenigen Haftungsfragen, die sich beim Einsatz autonomer Systeme stellen, sachgerecht zu bewältigen. Als besonders relevanter Unterfall der Gefährdungshaftung soll dabei hier die Produkthaftung nach dem Produkthaftungsgesetz eingeordnet und gesondert dargestellt werden.[97]

---

[93] MüKo/*Wagner*, BGB, vor § 823 Rn. 7.
[94] Staudinger/*Hager*, BGB, Vorbem. zu §§ 823 ff. Rn. 24.
[95] MüKo/*Wagne*r, BGB, vor § 823 Rn. 7.
[96] S. nur *Larenz/Canaris*, SchuldR II/2, § 84 I 1, S. 600.
[97] Zum – für diese Untersuchung nicht maßgeblichen - Streit über die dogmatische Einordnung der Haftung nach dem ProdHaftG vgl. MüKo/*Wagner*, BGB, Einl. ProfHaftG Rn. 17 ff.

II. Deliktische Verschuldenshaftung

Auch beim Einsatz autonomer Systeme kann die auf Verschulden basierende Deliktshaftung eine wichtige Rolle spielen. Eine solche Haftung sieht das Gesetz insbesondere in den § 823 Abs. 1 und 2 BGB vor.

1. Anknüpfungspunkte der Haftung

Anknüpfungspunkt der Haftung ist das Verschulden. Von besonderer praktischer Bedeutung ist dabei die Frage, ob der Schädiger fahrlässig gehandelt hat; die hiermit zusammenhängenden Probleme stellen sich insbesondere auch beim Einsatz autonomer Systeme. Fahrlässigkeit (§ 276 Abs. 2 BGB) setzt voraus, dass ein bestimmtes schadensauslösendes Ereignis bei Anwendung pflichtgemäßer Sorgfalt voraussehbar und vermeidbar gewesen wäre. Dabei ist es grundsätzlich unerheblich, ob der Schadenseintritt auf ein aktives Tun oder – bei bestehender Pflicht zum Handeln – ein Unterlassen zurückzuführen ist. Es gilt hierbei – anders als im Strafrecht – ein rein objektiver Sorgfaltspflichtmaßstab, der sich nach den im jeweiligen Verkehrskreis geltenden Maßstäben richtet.[98] Seine innere Rechtfertigung findet dieser Ansatz auch in dem Gedanken des Vertrauensschutzes: Im Rechtsverkehr soll sich jeder grundsätzlich darauf verlassen dürfen, dass der andere die für die Erfüllung seiner Pflichten erforderlichen Fähigkeiten und Kenntnisse besitzt.[99]

Zur Bestimmung des Sorgfaltsmaßstabs kann – soweit vorhanden – auf Rechtsvorschriften zurückgegriffen werden, wobei der jeweils anwendbare Sorgfaltsmaßstab grundsätzlich im Einzelfall zu ermitteln ist; allgemein gilt, dass der zu betreibende Vermeidungsaufwand umso höher ist, je größer die Schadenswahrscheinlichkeit und je höher der zu erwartende Nutzen ist.[100] Insgesamt kann vom Verantwortlichen in der Regel allerdings nur erwartet werden, dass er alle ihm zumutbaren und angemessenen Sicherheitsvorkehrungen trifft, um eine Schädigung anderer zu verhindern, die berechtigterweise von ihm erwartet werden können.[101]

Fraglich ist, ob die Verschuldenshaftung beim Einsatz autonomer Systeme ein ausreichendes Haftungskonzept bietet. In der Literatur[102] wird dies bezweifelt. Je selbstständiger ein System agiere und reagiere, desto weniger erscheine es

---

[98] St. Rspr.; s. etwa BGH, Urt. v. 17.3.1981 – VI ZR 191/79, NJW 1981, 1603; BGH, Urt. v. 13.2.2001 – VI ZR 34/00, NJW 2001, 1786; aus der Lit. MüKo/*Grundmann*, BGB, § 276 Rn. 55 f.

[99] Palandt/*Grüneberg*, BGB, § 276 Rn. 15.

[100] Zutr. *Horner/Kaulartz,* Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (8).

[101] BGH, Urt. v. 2.3.2010 – VI ZR 223/09, NJW 2010, 1967.

[102] S. etwa *Horner/Kaulartz*, Haftung 4.0, CR 2016, 7 (8).

sachgerecht, dem Nutzer des Systems in Bezug auf die unmittelbare Verletzungshandlung einen Verschuldensvorwurf zu machen. Das fehlerhafte Verhalten sei für den Nutzer typischerweise nicht vorhersehbar und damit auch nicht mehr steuerbar.[103]

Auf dieser Grundlage stellt sich die Frage, wie der Sorgfaltsmaßstab bei der Herstellung oder dem Einsatz autonomer Systeme zu konkretisieren ist und ob relevante Haftungslücken dadurch drohen, dass Herstellern oder Betreibern aufgrund der spezifischen Eigenschaften dieser Systeme kein Fahrlässigkeitsvorwurf gemacht werden kann. Allgemeine Aussagen lassen sich hierzu schwerlich treffen. Vielmehr muss den hiermit zusammenhängenden Fragen anhand konkreter Anwendungsbeispiele näher nachgegangen werden. Insoweit wird auf die Ausführungen unter F. und G. verwiesen.

Das Gesetz sieht in bestimmten Fällen eine Schärfung der Haftung vor. Im hiesigen Kontext sind dabei unter Wertungsgesichtspunkten vor allem solche Regelungen interessant, nach denen aus Gründen der Beweiserleichterung für den Geschädigten in bestimmten Fällen das Verschulden vermutet wird, insbesondere in Fällen der Verletzung gesetzlich konkretisierter Sorgfaltspflichten (§§ 831, 832, 833 S. 2, 834, 836 - 838 BGB, § 18 StVG). Hintergrund hierfür dürfte neben der größeren Beweisnähe des Schädigers insbesondere der Gedanke des Einstehenmüssens für besondere Risiken sein, z.B. im Bereich des § 831 BGB das Einstehen für das Unternehmensrisiko.[104]

Ob auch bei der Haftung für autonome Systeme das Verschulden des Herstellers oder des Betreibers vermutet werden sollte, kann nicht allgemeingültig beantwortet werden. Es ist vielmehr produktbezogen zu untersuchen, ob sich Haftungslücken ergeben; erst im Anschluss daran kann die Frage beantwortet werden, wie diese geschlossen werden sollten.

2. Beim Einsatz autonomer Systeme relevante Haftungstatbestände

Das allgemeine Deliktsrecht gilt selbstverständlich auch dann, wenn es um die Herstellung und den Einsatz autonomer Systeme geht. Will man also – wie hier – untersuchen, ob das geltende Haftungsrecht ausreichend ist, müssen diese Regeln den Ausgangspunkt der Überlegungen bilden.

a. Allgemeine Haftungstatbestände des Deliktsrechts

Im allgemeinen Deliktsrecht kann zwischen dem Anspruch aus § 823 Abs. 1 BGB und demjenigen aus § 823 Abs. 2 BGB unterschieden werden.

---

[103] *Horner/Kaulartz*, Haftung 4.0, CR 2016, 7 (8).
[104] Staudinger/*Bernau*, BGB, § 831 Rn. 5.

(1) Anspruch aus § 823 Abs. 1 BGB (Rechtsgutsverletzung)

Die Haftung nach § 823 Abs. 1 BGB setzt die rechtswidrige und schuldhafte Verletzung eines geschützten Rechtsguts voraus. Der Sorgfaltsmaßstab im Rahmen der Verschuldenshaftung ist auch beim Einsatz autonomer Systeme nach den allgemeinen Grundsätzen anhand des konkreten Einzelfalls zu bilden.

Für den Betreiber eines autonomen Systems kommen insoweit Sorgfaltspflichten bei der Auswahl, Bedienung und Überwachung des Systems in Betracht. Je selbstständiger das eingesetzte System agiert, desto weniger werden Sorgfaltspflichtverletzungen bei der laufenden Bedienung in Betracht kommen. Die Pflichten des Betreibers dürften sich bei zunehmender Automatisierung vielmehr auf die Auswahl, Inbetriebnahme und Überwachung des Systems konzentrieren (Ist das System für den konkreten Einsatzzweck geeignet? Entspricht es den aktuellen Sicherheitsstandards, müssen zum sicheren Betrieb insbesondere noch Software-Updates vorgenommen werden? Zeigen sich sicherheitsrelevante Anomalien beim Betrieb des Systems?).[105] Ob dadurch Haftungslücken drohen, soll im Rahmen der Erörterung der konkreten Anwendungsbeispiele näher untersucht werden.

Hinsichtlich der den Hersteller autonomer Systeme treffenden Sorgfaltspflichten ist für die hiesige Untersuchung die sog. deliktsrechtliche Produzentenhaftung besonders relevant. Diese gründet auf dem Prinzip, dass derjenige, der eine Gefahrenquelle eröffnet oder beherrscht, für diese verantwortlich ist.[106] Im Unterschied zur Gefährdungshaftung nach dem ProdHaftG haftet der Produzent im Rahmen der §§ 823 ff. BGB verschuldensabhängig, wobei die praktischen Auswirkungen dieses Unterschieds nicht überschätzt werden dürfen[107]. Wie bei der Haftung nach dem ProdHaftG wird bei der deliktischen Produzentenhaftung eine Unterteilung in die Fehlerkategorien Konstruktion, Fabrikation und Instruktion vorgenommen mit entsprechenden Verkehrssicherungspflichten für das Inverkehrbringen eines Produkts. Hinzu treten ab dem Inverkehrbringen des Produkts die Pflicht zur Produktbeobachtung und die daran ggf. anknüpfenden Pflichten zur Gefahrenabwehr.[108] Die im Rahmen der deliktischen Produzentenhaftung entwickelten Kategorien gelten auch nach dem Inkrafttreten des ProdHaftG fort und sind nicht gegenstandslos geworden.[109] Bei der konkreten Ausgestaltung sind insbesondere die ggf. nicht vorhandenen technischen Kennt-

---

[105] *Horner/Kaulartz*, Haftung 4.0, CR 2016, 7 (8 f.)
[106] BeckOK BGB/*Förster*, Stand: 15.06.2017, § 823 Rn. 663 f.
[107] Näher *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (711 ff.).
[108] Vgl. Palandt/*Sprau*, BGB, § 823 Rn. 172 ff.
[109] BGH, Urt. v. 9.5.1995 – VI ZR 158/94, BGHZ 129, 353 Rn. 15.

nisse der Nutzer zu berücksichtigen.[110] Auch hier dienen technische Standards aus überbetrieblichen technischen Normen zur Konkretisierung unbestimmter Rechtsbegriffe und daraus resultierender Pflichten.

Da die sich im Hinblick auf die Haftung des Herstellers autonomer Systeme stellenden Fragen bei der deliktischen Produzentenhaftung und der Haftung nach dem ProdHaftG (hinsichtlich der Pflichten beim Inverkehrbringen des Produkts) weitgehend deckungsgleich sind, sollen beide Haftungstatbestände im Folgenden unter IV. behandelt werden.

(2) Anspruch aus § 823 Abs. 2 BGB (Schutzgesetzverletzung)

Unabhängig von einem Anspruch aus § 823 Abs. 1 BGB kann für den Hersteller eine Haftung infolge Schutzgesetzverletzung nach § 823 Abs. 2 BGB bestehen. Zumindest theoretische Bedeutung als Schutzgesetz haben hierbei im Zusammenhang mit Produkten die Vorschriften des Produktsicherheitsgesetzes (ProdSG). Ein Anspruch des Produktbenutzers besteht aufgrund des eingeschränkten Schutzbereichs des ProdSG jedoch nur für Verletzungen der Schutzgüter Leben und Gesundheit (vgl. § 3 ProdSG).

Bei fehlerhaften Medizinprodukten können etwa zudem die Vorschriften des MPG zur Anwendung kommen, da Zweck dieses Gesetzes nach § 1 MPG ist, den Verkehr mit Medizinprodukten zu regeln und dadurch für die Sicherheit, Eignung und Leistung der Medizinprodukte sowie die Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritter zu sorgen. Auch hier sind somit nur Leben und Gesundheit geschützt. Näheres hierzu unter D. III.

b. Besondere Tatbestände der Verschuldenshaftung

Wie bereits oben ausgeführt, sieht das deutsche Recht für einige besondere „Risikoquellen“ spezielle Haftungstatbestände vor, die auch beim Einsatz autonomer Systeme relevant werden können. Typischerweise setzt die Haftung nach diesen Vorschriften zwar ein Verschulden voraus, dieses wird aber vermutet, d.h. der Schädiger muss sich, um sich der Haftung zu entziehen, exkulpieren und trägt hierfür die Beweislast. Das ist gerechtfertigt, da die Frage des Verschuldens und die hierfür maßgeblichen Tatsachen meist allein in der Sphäre des Schädigers liegen; dies führt auf Seiten des Geschädigten zu Schwierigkeiten bei der Beweisführung. Auf der Grundlage der Beweislastumkehr wird es dem Geschädigten mithin erleichtert, eine Kompensation für den eingetretenen Schaden zu erhalten.

---

[110] *Vogt*, Fahrerassistenzsysteme – Neue Technik – Neue Rechtsfragen?, NZV 2003, 153 (156).

Neben der Haftung für Verrichtungsgehilfen (§ 831 BGB) und der Haftung des Aufsichtspflichtigen (§ 832 BGB) ist im Rahmen dieser Untersuchung insbesondere die Haftung des Fahrzeugführers nach § 18 Abs. 1 StVG von Interesse. Denn es wird in der Literatur[111] angenommen, dass dieser Haftungstatbestand bei zunehmendem Einsatz *automatisierter/autonomer* Systeme bei der Fahrzeugsteuerung an Bedeutung verlieren wird, da das fehlerhafte Verhalten eines autonomen Systems für den Nutzer typischerweise nicht vorhersehbar und damit steuerbar sein werde. Bei der Aktivierung von hoch- oder vollautomatisierten Fahrfunktionen im Zeitpunkt des Schadensfalls wird sich der Fahrzeugführer nach § 18 Abs. 1 Satz 2 StVG exkulpieren können, soweit er seinen Pflichten nach § 1b StVG nachgekommen ist.

III. Gefährdungshaftung

Es stellt sich die Frage, ob die Grundsätze zur Gefährdungshaftung – ggf. de lege ferenda – ein taugliches Instrument dafür sein können, um die sich bei autonomen Systemen stellenden Haftungsfragen interessengerecht und systemkonform in den Griff zu bekommen. Soweit derzeit spezielle Regeln fehlen, ist insbesondere zu klären, unter welchen Voraussetzungen der Haftungsgrund dieser Haftungsform auch in Bezug auf die Herstellung oder den Betrieb autonomer Systeme erfüllt ist.

1. Grundlagen

Für die Gefährdungshaftung gilt das Enumerationsprinzip. Aufgrund des Verzichts auf ein Verschulden besteht ein gesteigertes Bedürfnis nach Rechtssicherheit, da der Betroffene in der Lage sein sollte, Vorsorge zu treffen (z.B. Abschluss einer Haftpflichtversicherung).[112] Aus diesem Grund war die Rechtsprechung in der Vergangenheit äußerst zurückhaltend, wenn es darum ging, die Vorschriften über die Gefährdungshaftung auf ungeregelte Sachverhalte analog anzuwenden. All dies sollte man auch bei den Überlegungen berücksichtigen, ob für die Haftung beim Einsatz autonomer System eine Generalklausel geschaffen werden sollte. Aufgrund des Enumerationsprinzips ist es die Aufgabe des Gesetzgebers, diejenigen Sachverhalte zu identifizieren, in denen eine Gefährdungshaftung eingreifen sollte. Hiervon hat der Gesetzgeber zwar zurückhaltend, wohl aber regelmäßig Gebrauch gemacht. Anwendungsfälle sind etwa: § 1 HaftPflG (Vorläufer schon 1838), § 7 StVG (1908), § 33 LuftVG (1922), § 2 HaftPflG (1943, Elektrizität, Gase, Dämpfe oder Flüssigkeiten); zweite Hälfte 20. Jhdt.: §§ 25 ff. AtomG, § 22 WHG a.F. = § 89 WHG (Wasser), § 114

---

[111] *Horner/Kaulartz*, Haftung 4.0, CR 2016, 7 (8).
[112] S. nur *Larenz/Canaris*, SchuldR II/2, § 84 I 1, S. 602.

BBergG, § 1 UmweltHG, § 32 GenTG („Betreiber"), § 84 AMG (Arzneimittel) und vor allem §§ 1 ff. ProdHaftG.

In welchen Fällen der Gesetzgeber eine Gefährdungshaftung einführt, ist weitgehend in sein Ermessen gestellt. Der Gesetzgeber erfüllt seine verfassungsrechtliche Schutzpflicht regelmäßig schon dann, wenn jedenfalls eine verschuldensabhängige Haftung greift.[113]

Die Gefährdungshaftung ist nicht die einzige Haftung, die kein Verschulden voraussetzt. Sie ist vielmehr insbesondere von der Aufopferungshaftung abzugrenzen. Die Aufopferungshaftung zeichnet sich – wie etwa § 906 Abs. 2 S. 2 BGB – dadurch aus, dass dem Geschädigten an sich ein Abwehranspruch zustand, dieser ihm jedoch – unter Gewährung einer Entschädigung – von der Rechtsordnung genommen wird. Das ist bei der Gefährdungshaftung anders; diese Haftung greift auch dann ein, wenn dem Geschädigten ein entsprechender – gleichsam „vorgelagerter" – negatorischer Abwehranspruch nicht zustand. Ferner ist die Gefährdungshaftung von einer Haftung zu unterscheiden, die ohne ein weiteres Zurechnungserfordernis bereits dann eingreift, wenn das Verhalten des Schuldners für den Schadenseintritt kausal ist; eine solche Haftung, die als „Kausalhaftung" bezeichnet werden kann, ist dem deutschen Recht in dieser Form fremd.

2. Haftungsgrund

Auch wenn die Regelungen über die jeweilige Gefährdungshaftung sich in vielen Spezialgesetzen befinden, liegen ihnen strukturelle Gemeinsamkeiten zugrunde. Diese sind auch hier von Bedeutung; eine etwaige Gefährdungshaftung für autonome Systeme sollte sich schon aus Gründen der Rechtssicherheit in die Struktur des allgemeinen Haftungsrechts einfügen. Was den Haftungsgrund der Gefährdungshaftung angeht, haben sich verschiedene Wertungskriterien herauskristallisiert, die hier kurz skizziert werden sollen. Jene Kriterien stehen freilich nicht isoliert nebeneinander, sondern sind im Einzelfall zu gewichten; sie sind Teil eines beweglichen Systems.

a. „Besondere Gefahr"

Die Gefährdungshaftung wird insbesondere von den Prinzipien der Gefahrveranlassung und der Gefahrbeherrschung getragen. Erforderlich ist mithin insbesondere eine „besondere Gefahr";[114] gerade in ihrer Schaffung oder Aufrechterhaltung liegt der Haftungsgrund für die Gefährdungshaftung.

---

[113] *Larenz/Canaris*, SchuldR II/2, § 84 I 2, S. 606.
[114] *Larenz/Canaris*, SchuldR II/2, § 84 I 2, S. 607.

Betrachtet man die existierenden Tatbestände der Gefährdungshaftung näher, so kann wie folgt differenziert werden:

Die „besondere Gefahr“ kann auf einer besonderen Gefährlichkeit einer Sache oder einer Handlung aufbauen (so etwa § 7 StVG oder § 89 WHG). In beiden Fällen geht es in erster Linie um die Haftung desjenigen, der den Betrieb der Sache oder die gefahrauslösende Handlung verantwortet. Dass dieser die Gefahr „veranlasst“ oder „beherrscht“, liegt auf der Hand. Knüpft also das Gesetz die Gefährdungshaftung an die besondere Gefährlichkeit einer Sache oder einer Handlung, so sieht es eine Haftung des Betreibers (und nicht des Herstellers) vor.

Hiervon zu unterscheiden sind die Tatbestände der Gefährdungshaftung, in denen es um die Haftung des Herstellers geht. Soweit das Gesetz diesen als Schuldner vorsieht, knüpft die Haftung an einen Fehler der Sache an. Dies ist etwa bei der Produkthaftung nach dem ProdHaftG oder – trotz abweichender Beweislastverteilung – bei § 2 Abs. 1 S. 2 HPflG der Fall. In beiden Fällen haftet der Hersteller oder der Inhaber der Anlage dann nicht, wenn das Produkt oder die Anlage fehlerfrei sind. Betrachtet man also die Haftung des Herstellers, so wird deutlich, dass der Gesetzgeber von einer hinreichenden Gefahrveranlassung bislang nicht schon dann ausgegangen ist, wenn jemand eine – ggf. auch potentiell gefährliche – Sache herstellt und in den Verkehr bringt; es muss vielmehr hinzu kommen, dass die Sache fehlerhaft ist. Das ist auch in systematischer Hinsicht überzeugend. Allein in der Herstellung und dem Inverkehrbringen einer fehlerfreien Sache hat der Gesetzgeber bislang keine Gefahr erkannt, die eine Gefährdungshaftung rechtfertigt; jene Handlungen werden vielmehr grundsätzlich als haftungsrechtlich neutral angesehen. Vor diesem Hintergrund überzeugt es, dass auch § 84 AMG die Gefährdungshaftung des pharmazeutischen Unternehmers, der das Arzneimittel im Geltungsbereich dieses Gesetzes in den Verkehr gebracht hat, an einen Entwicklungs- oder Herstellungsfehler[115] (vgl. § 84 Abs. 1 S. 2 Nr. 1 AMG) oder an einen Instruktionsfehler (vgl. § 84 Abs. 1 S. 2 Nr. 2 AMG) knüpft.

b. Vorteil und korrespondierendes Risiko

Die Gefährdungshaftung wird ferner von dem Gedanken der Zusammengehörigkeit von Vorteil und korrespondierendem Risiko getragen. Besonders deutlich wird dies, wenn der Betreiber aus dem Betrieb einen wirtschaftlichen Nutzen zieht; allerdings kann jener Vorteil auch nicht-wirtschaftlicher Natur sein. Da ein nicht-wirtschaftlicher Vorteil jedoch nur in absoluten Ausnahmefällen ver-

[115] Vgl. BeckOGK/*Franzki*, Stand: 1.1.2019, AMG § 84 Rn. 66.1.

neint werden kann, kommt jenem Gedanken keine nennenswerte eingrenzende Wirkung zu; er taugt mithin für die weiteren Überlegungen nur bedingt.

c. Unausweichlichkeit der Gefahr für den Geschädigten

Ein weiterer Gesichtspunkt, der zur Rechtfertigung der Gefährdungshaftung herangezogen werden kann, ist derjenige, dass der Geschädigte sich der Gefahr nicht entziehen, ihr also nicht ausweichen kann. In diesen Fällen entfällt die Möglichkeit des Selbstschutzes. Als „Kompensation" hierfür erhält der Geschädigte einen verschuldensunabhängigen Anspruch. Voraussetzung ist freilich, dass der Geschädigte schutzbedürftig ist.

3. Zurechnungsadressat

Eng verknüpft mit der Frage, ob ein Haftungsgrund besteht, ist die Frage, wer der richtige Zurechnungsadressat ist.

Adressat der Haftung kann nur derjenige sein, dem die „besondere Gefahr" zuzurechnen ist. Zieht man die Kriterien der Gefahrveranlassung und der Gefahrbeherrschung heran, so trifft die Haftung denjenigen, der für die Gefahr verantwortlich ist, sie mithin veranlasst hat oder beherrschen kann.

a. Hersteller

Zu klären ist, unter welchen Voraussetzungen der Hersteller ein tauglicher Haftungsadressat ist.

(1) Hersteller eines fehlerhaften autonomen Systems

Wie bereits oben angesprochen, liegt in der Herstellung und in dem Inverkehrbringen einer Sache jedenfalls dann eine „besondere Gefahr", die eine Gefährdungshaftung rechtfertigt, wenn die Sache fehlerhaft ist. Dies gilt selbstverständlich auch für autonome Systeme. In jenen Fällen ist mithin eine Gefährdungshaftung sachgerecht, sie ergibt sich nach dem geltenden Recht aus dem ProdHaftG.

(2) Hersteller eines fehlerfreien autonomen Systems

Für ein fehlerfreies Produkt greift nach dem geltenden Recht keine Herstellerhaftung. Dies leuchtet für den Regelfall unmittelbar ein. Gleichwohl kann man die Frage aufwerfen, ob jener Grundsatz für autonome Systeme ebenfalls überzeugt. So ließe sich an eine Haftung des Herstellers denken, die dann eingreift, wenn sich eine spezifische Gefahr realisiert, die beim Einsatz autonomer Systeme geschaffen wird. Diese Gefahr kann ggf. darin gesehen werden, dass das System unvorhersehbare Entscheidungen trifft, die - unterstellt, nach den geltenden Maßstäben wäre ein „Fehler" zu verneinen - einen Schaden verursachen

können. Grundlage einer solchen Überlegung wäre die Erwägung, dass selbst ein autonomes System, das auf nahezu unendlich viele Situationen vorbereitet und programmiert wurde, bei einer gegebenenfalls dennoch eintretenden „Sondersituation“ versagt. Hierin könnte eine spezifische Gefahr gesehen werden, die der Sphäre des Herstellers als Produzent des autonomen Systems entstammt.

Gleichwohl erscheint es zweifelhaft, ob in diesen Fällen – also auch ohne einen Produktfehler – eine Gefährdungshaftung des Herstellers eingreifen sollte. Dagegen spricht insbesondere, dass es letztlich nicht der Hersteller ist, der konkret und eigenverantwortlich über den Einsatz des autonomen Systems entscheidet. Darüber hinaus ist zu berücksichtigen, dass der Einsatz eines autonomen Systems geeignet sein dürfte, insgesamt die Gefahren zu verringern, die ansonsten statistisch auf menschliches Fehlverhalten zurückzuführen wären, was letztlich (auch) dem Betreiber, Nutzer etc. zugute kommt. Bei einer wertenden Betrachtung ist es somit in der Regel nicht der Hersteller, der die Gefahr veranlasst. Für den Hersteller würde eine Haftung in diesen Fällen letztlich auf eine reine „Kausalhaftung“[116] hinauslaufen.

(3) Hersteller eines möglicherweise fehlerhaften autonomen Systems

Werden Schäden durch autonome Systeme verursacht, so mag es im Vergleich zu „analogen“ Sachverhalten größere Schwierigkeiten bereiten, den Fehler zu lokalisieren und nachzuweisen. Das betrifft insbesondere solche Fehler, die nur dann erkannt werden können, wenn der Algorithmus bekannt ist. Es stellt sich jedoch die Frage, ob die sich hieraus ggf. ergebenden Beweisschwierigkeiten eine Gefährdungshaftung rechtfertigen können. Zieht man die oben herausgearbeiteten Kriterien heran, kommt es darauf an, ob in der Herstellung und in dem Inverkehrbringen eines autonomen Systems bereits deshalb eine „besondere Gefahr“ liegt, weil im Zusammenhang mit Haftungsfragen besondere Beweisschwierigkeiten entstehen können.

Dies ließe sich ggf. mit dem Hinweis darauf bejahen, dass die Beweisschwierigkeiten dem autonomen System gleichsam immanent sind.[117] Gleichwohl überzeugt ein solcher Ansatz letztlich nicht. Besondere Beweisschwierigkeiten können auch in völlig anders gelagerten Sachverhalten entstehen, die mit autonomen Systemen in keinem Zusammenhang stehen. Um ihnen sachgerecht begegnen zu können, ist an eine Modifizierung der Darlegungs- und Beweislast zu denken. Insoweit muss untersucht werden, ob die Voraussetzungen erfüllt sind, die im Allgemeinen an eine Beweislastumkehr zu stellen sind. Sofern man auf der Grundlage der allgemeinen Regeln nicht zu sachgerechten Ergebnissen ge-

---

[116] Zu diesem Begriff s. oben unter 1.

[117] In dieser Richtung wohl *Kütük-Markendorf/Esser*, Zivilrechtliche Haftung des Herstellers beim autonomen Fahren, MMR 2016, 22 (25).

langt, ist zu prüfen, ob das Gesetz im Hinblick auf die Darlegungs- und Beweislast angepasst werden sollte, etwa in Bezug auf das Vorliegen eines Fehlers. Dabei kann auch eine Rolle spielen, ob eine Beweissicherung durch Protokollierung möglich ist („Blackbox"); falls ja, ist zu erwägen, ob eine entsprechende Pflicht zur Datensicherung bestehen sollte.[118] Eine solche „Blackbox" kann ggf. dazu beitragen, die Lokalisierbarkeit des Fehlers zu verbessern, was wiederum entweder gegen die Notwendigkeit sprechen kann, die Darlegungs- und Beweislast anzupassen, oder aber – umgekehrt – eine solche für den Hersteller als zumutbar erscheinen lässt. All dies muss unter Berücksichtigung der insoweit geltenden Wertungskriterien gesondert und produktbezogen untersucht werden.

(4) Ergebnis

Im Ergebnis kann festgehalten werden, dass allein in der Herstellung und in dem Inverkehrbringen eines autonomen Systems keine „besondere Gefahr" liegt, die eine Gefährdungshaftung rechtfertigt. Auch der Umstand, dass sich Beweisschwierigkeiten ergeben können, genügt grundsätzlich nicht; allerdings können sie ggf. eine abweichende Ausgestaltung der Beweislastverteilung erforderlich machen, was nicht allgemein beurteilt werden kann, sondern nur produktbezogen zu beantworten ist.

b. Betreiber

Es ist ferner zu prüfen, unter welchen Voraussetzungen der Haftungsgrund für die Gefährdungshaftung in der Person des Betreibers greift.

Wie bereits oben dargestellt, wird die Gefährdungshaftung von den Prinzipien der Gefahrveranlassung und der Gefahrbeherrschung getragen. Der Betreiber (Halter) eines Produkts ist derjenige, der die Gefahr – abstrakt gesehen – beherrscht, indem er die Quelle schafft (er erwirbt sie) und aufrechterhält (er behält sie). Hierin liegt mithin grundsätzlich ein tauglicher Zurechnungsgrund; auf einen Fehler des Produkts kommt es deshalb bei der Betreiberhaftung nicht an.

Eine Gefährdungshaftung ist freilich nur dann gerechtfertigt, wenn von der Sache eine „besondere Gefahr" ausgeht. Ob es sich um eine solche Sache handelt, ist produktbezogen zu prüfen. Dies gilt auch für autonome Systeme. Nicht von jedem Produkt, das autonom agiert, muss eine solche „besondere Gefahr" ausgehen. Allein die Autonomie eines Systems hat nicht zwingend zur Folge, dass eine besondere Gefährlichkeit damit verbunden wäre; es ist vielmehr das jeweilige Einsatzgebiet zu untersuchen. Je größer die möglichen Schäden sind, desto eher spricht dies für die Schaffung eines Gefährdungshaftungstatbestandes, wo-

[118] S. dazu *Horner/Kaulartz*, Haftung 4.0, CR 2016, 7 (10).

bei auch die typischerweise gefährdeten Rechtsgüter in Ansatz zu bringen sind. Dabei steht dem Gesetzgeber eine Einschätzungsprärogative zu.

Selbst wenn man zu dem Ergebnis gelangt, dass von dem Betrieb der Sache eine besondere Gefahr ausgeht, kann es trotzdem so liegen, dass kein ausreichender Haftungsgrund für eine Gefährdungshaftung besteht. An einer solchen Legitimation kann es etwa dann fehlen, wenn der Betreiber aus dem Einsatz der Maschine weder einen wirtschaftlichen noch einen nicht-wirtschaftlichen Vorteil generiert; das wird freilich nur sehr selten der Fall sein.
Es kann also festgehalten werden, dass der Betreiber des autonomen Systems im Rahmen der Gefährdungshaftung grundsätzlich ein tauglicher Zurechnungsadressat ist.

c. Roboter

Teilweise wird die Auffassung[119] vertreten, dass – unter bestimmten Voraussetzungen – auch der Roboter selbst als Haftungsadressat in Betracht kommen sollte. Dieser Ansatz überzeugt indes nicht. Insoweit wird insbesondere auf die Ausführungen im Bericht der Arbeitsgruppe vom 15. Mai 2017 verwiesen.[120]

4. Geschützter Personenkreis

Von der bislang untersuchten Frage, unter welchen Voraussetzungen in der Person des Herstellers oder des Betreibers ein Haftungsgrund für eine Gefährdungshaftung gegeben ist, muss die Frage unterschieden werden, welche Personen von der betreffenden Haftung geschützt werden sollten. Diese Frage ist nicht nur für die konkrete Ausgestaltung einer gesetzlichen Regelung von Bedeutung, sondern kann bereits dafür relevant werden, ob in Bezug auf das jeweilige Produkt überhaupt eine Gefährdungshaftung eingeführt werden sollte. Stellt sich nämlich heraus, dass mit dem Einsatz des betreffenden autonomen Systems nur solche Personen in Berührung kommen, die bei normativer Betrachtung den Schutz einer Gefährdungshaftung nicht erwarten können oder ausreichend durch andere Ansprüche geschützt sind, so kann dieser Befund von vornherein gegen die Notwendigkeit sprechen, eine entsprechende Haftung gesetzlich zu begründen.

a. Schutz unbeteiligter Dritter

Ist ein zureichender Haftungsgrund vorhanden (dazu oben unter 2.), so soll es gerade die Aufgabe der Gefährdungshaftung sein, unbeteiligte Dritte vor den

---

[119] Vgl. Ziffer 59 Buchstabe f der in der unter C. erwähnten Entschließung des Europäischen Parlaments vom 16. Februar 2017.
[120] AG Digitaler Neustart, Bericht vom 15. Mai 2017, S. 114.

Gefahren, die von der betreffenden Sache ausgehen, zu schützen. Dies gilt sowohl für die Betreiberhaftung als auch für die Herstellerhaftung. Sofern also davon auszugehen ist, dass das betreffende autonome System am öffentlichen Verkehr teilnimmt, liegt es auf der Hand, dass die Haftungsnorm unbeteiligte Dritte schützen sollte.

b. Schutz des Profiteurs

Schwieriger ist die Frage zu beantworten, ob auch der Profiteur von der Gefährdungshaftung geschützt werden sollte.

(1) Wer ist Profiteur?

Als Profiteur soll hier derjenige bezeichnet werden, zu dessen Gunsten das in Rede stehende autonome System eingesetzt wird; er zeichnet sich dadurch aus, dass er sich den Gefahren des autonomen Systems bewusst aussetzt. In Bezug auf diese Person ist genauer zu untersuchen, ob sie in den Schutz der Gefährdungshaftung einbezogen werden sollte.

So stellt sich etwa beim autonomen Fahren die Frage, ob auch die Insassen geschützt werden sollten. Das ist keineswegs selbstverständlich. Nach dem geltenden Recht wird der Fahrer (!) eines Kfz nicht von der Halterhaftung erfasst (§ 8 Nr. 2 StVG). Auch die Haftung aus § 33 LuftVG (Betreiber) kennt Einschränkungen; sie greift sogar nur gegenüber außenstehenden Dritten.[121] Gegenüber den Insassen sieht § 44 LuftVG – ab einer bestimmten Haftungsgrenze – demgegenüber „lediglich" eine Verschuldenshaftung mit Beweislastumkehr vor, die freilich nicht den Halter, sondern den Luftfrachtführer trifft.

(2) Betreiberhaftung gegenüber dem Profiteur

Bei den weiteren Überlegungen zu der Frage, welche Profiteure in den Vorteil einer Gefährdungshaftung kommen sollten, bietet es sich an, zwischen der Betreiberhaftung und der Herstellerhaftung zu differenzieren.

Zunächst soll der Frage nachgegangen werden, ob es sachgerecht ist, den Profiteur in die Gefährdungshaftung des Betreibers einzubeziehen.

(a) Keine Betreiberhaftung gegenüber dem Nutzer?

Wie bereits oben angesprochen, wird die Gefährdungshaftung auch von dem Gedanken getragen, dass sich der Geschädigte der Gefahr nicht entziehen kann.

---

[121] Dazu BeckOGK/*Förster*, Stand: 1.11.2018, LuftVG § 33 Rn. 30.

Auf dieser Grundlage ließe sich argumentieren, dass eine Gefährdungshaftung stets dann nicht angezeigt ist, wenn der Geschädigte sich freiwillig in die Gefahrensituation begeben hat. So meint *Canaris*[122], dass insbesondere § 8 Nr. 2 StVG lediglich den allgemeinen Rechtsgedanken zum Ausdruck bringe, dass die Gefährdungshaftung grundsätzlich nur vor solchen Risiken schützen soll, denen man nicht ausweichen könne.

Dieser dogmatischen Einordnung ist allerdings der BGH[123] entgegengetreten; bei § 8 Nr. 2 StVG handele es sich um eine Ausnahmevorschrift, die eng auszulegen sei. Der dieser Vorschrift zugrunde liegende Gedanke könne nicht dergestalt verallgemeinert werden, dass zugunsten des Nutzers einer Sache keine Gefährdungshaftung besteht. So bejaht der BGH[124] die Haftung des Pferdehalters auch gegenüber dem Reiter, dem das Pferd aus Gefälligkeit überlassen wurde (§ 833 BGB).

Auf der Grundlage dieser Rechtsprechung wird man annehmen können, dass der generelle Ausschluss der Gefährdungshaftung gegenüber einem Nutzer der Sache dann gerechtfertigt ist, wenn die Kontrolle, die der Nutzer über die Sache erhält, so stark ist, dass die von der Sache typischerweise ausgehenden Gefahren hinreichend stark verringert werden können. Das wird man zwar in Bezug auf den Fahrer eines Pkw annehmen können, nicht aber in Bezug auf den Reiter eines Pferdes; die tierspezifischen Gefahren wirken auch bei einem geübten Reiter fort.

Hieraus lässt sich ableiten, dass eine Gefährdungshaftung des Betreibers gegenüber dem Nutzer dann nicht angezeigt ist, wenn dieser typischerweise eine Kontrolle über den Gegenstand erhält, die so stark ist, dass es gerechtfertigt ist, den Betreiber aus seiner Haftung zu entlassen. Dies wird man jedenfalls bei autonomen Systemen[125] typischerweise verneinen müssen, da diese – definitionsgemäß – eigene Entscheidungen treffen. Ausgehend hiervon liegt es im Falle des autonomen Fahrens nahe, sämtliche Insassen in den Schutz der Halterhaftung (§ 7 StVG) einzubeziehen, also auch denjenigen, der die „Schlüsselgewalt“ hat.

(b) Haftungslücke und vertragliche Nähebeziehung

Eine Haftungslücke, die durch eine Gefährdungshaftung geschlossen werden müsste, wird man dann verneinen müssen, wenn der Geschädigte auf der Grundlage anderer Ansprüche ausreichend gesichert ist.

---

[122] *Larenz/Canaris*, SchuldR II/2, S. 617.
[123] BGH, Urt. v. 5.10.2010 – VI ZR 286/09, NJW 2011, 292 Rn. 23; Urt. v. 22.12.1992 – VI ZR 53/92, NJW 1993, 2611.
[124] BGH, Urt. v. 22.12.1992 – VI ZR 53/92, NJW 1993, 2611.
[125] Entsprechendes dürfte für automatisierte Systeme gelten, soweit sie selbstständig agieren.

(aa) Existenz einer Haftungslücke in den „Vertragsfällen“

Dabei sind insbesondere die Fälle näher zu betrachten, in denen der Geschädigte mit dem Betreiber typischerweise in einer vertraglichen Nähebeziehung steht. Hier steht dem Geschädigten u.a. der aus § 280 Abs. 1 S. 2 BGB folgende Vorteil zur Seite; danach muss der Schuldner sein fehlendes Vertretenmüssen darlegen und beweisen.

Beim Einsatz autonomer Systeme hilft dies jedoch typischerweise nicht weiter. Dabei fällt insbesondere ins Gewicht, dass sich die Sorgfaltsanforderungen des Vertragspartners durch den Einsatz des autonomen Systems verlagern. Diese beziehen sich in erster Linie auf die Auswahl der Maschine (Entscheidung über das „Ob“), die Bedienung, die Wartung, die Instandsetzung und Instandhaltung. Soweit die Maschine die Tätigkeit des Vertragspartners ersetzt oder an seiner Stelle „entscheidet“, fehlt es im Hinblick auf die – nunmehr von der Maschine autonom ausgeübte – Tätigkeit als solcher an einem Anknüpfungspunkt für eine verschuldensabhängige Haftung des Betreibers.

(bb) Gewichtung der Haftungslücke

Dennoch kann auch in den soeben angesprochenen Fällen nicht ohne weiteres angenommen werden, die etwaige Haftungslücke müsse zwingend durch eine Gefährdungshaftung des Betreibers geschlossen werden. Es ist vielmehr weiter zu prüfen, ob die hiermit einhergehende Haftungslücke ausreichend gewichtig ist, um eine entsprechende Gefährdungshaftung rechtfertigen zu können. Im Rahmen dieser Prüfung können die folgenden Kriterien eine Rolle spielen, die freilich nicht isoliert zu betrachten, sondern im Rahmen einer Gesamtabwägung zu gewichten sind:

- Zulassungsverfahren

Gegen eine relevante Haftungslücke kann es sprechen, wenn das Produkt einem besonderen Zulassungsverfahren ausgesetzt ist. In diesem Fall werden die Risiken, die mit dem Einsatz des Roboters verbunden sind, von einer unabhängigen Stelle bewertet. Das bietet eine gewisse Gewähr dafür, dass die Fälle, in denen es zu systembedingten Fehlern kommt, unter Berücksichtigung des Risikos vergleichsweise selten sind; dies kann – freilich nicht allein, aber unter Berücksichtigung weiterer Umstände – gegen eine relevante Haftungslücke und damit auch gegen einen weiteren Handlungsbedarf des Gesetzgebers sprechen.

- Risikoübernahme

Ist das Produkt fehlerfrei (oder kann der Geschädigte den Fehler nicht nachweisen), realisieren sich in einer gleichwohl eingetretenen Schädigung diejenigen

Risiken, die der Einsatz des autonomen Systems mit sich bringt. Hier mag im Allgemeinen eine Betreiberhaftung sachgerecht sein; Voraussetzung ist freilich, dass von dem Produkt eine „besondere Gefahr“[126] ausgeht. Etwas anderes gilt aber dann, wenn mit dem Produkt typischerweise nur Personen in Berührung kommen, die das von diesem Produkt ausgehende spezifische Risiko bewusst übernommen haben. Eine Haftung des Betreibers erscheint deshalb jedenfalls dann als nicht geboten, wenn jene Personen über die Risiken hinreichend aufgeklärt wurden. Aber auch dann, wenn diese Aufklärung nicht erfolgt ist, besteht nicht zwingend eine Haftungslücke, die auf der Grundlage einer Gefährdungshaftung des Betreibers geschlossen werden müsste. Da in der unterlassenen Aufklärung eine gesonderte Pflichtverletzung liegen kann, steht dem Geschädigten ein Anspruch auf Schadensersatz gem. § 280 Abs. 1 BGB zu, der grundsätzlich ausreichend Schutz bieten dürfte; jedenfalls ist bislang nicht erkennbar, dass dies nicht der Fall ist. Die Einzelheiten sind produktbezogen zu prüfen.

Dabei ist ferner zu berücksichtigen, dass grundsätzlich auch die Entscheidung und der Rat des Betreibers, an seiner statt ein autonomes System zur Anwendung kommen zu lassen, pflichtgebunden sind, was bei pflichtwidrigem Handeln zu Schadensersatzansprüchen führen kann. Pflichtwidrig dürfte eine solche Entscheidung dann sein, wenn die Risiken, die aus dem Einsatz der Maschine folgen, in keinem angemessenen Verhältnis zum Nutzen stehen, wobei auch berücksichtigt werden kann, welche Risiken bestanden hätten, wenn die Maßnahme durch einen Menschen durchgeführt worden wäre. Die Einzelheiten sind vertragsrechtlich zu beurteilen und produktbezogen zu untersuchen.

Man wird also davon ausgehen können, dass dann, wenn die Gefahren des Produkts typischerweise nur Personen treffen, die in diese eingewilligt haben, eine Betreiberhaftung nicht geboten ist.

(3) Herstellerhaftung gegenüber dem Profiteur

Grundsätzlich greift der Haftungsgrund der Herstellerhaftung auch – und gerade – gegenüber dem Profiteur des Produkts. Der Gedanke der freiwilligen Selbstgefährdung kann eine Eingrenzung der Herstellerhaftung im Allgemeinen schon deshalb nicht rechtfertigen, weil die Haftung einen Produktfehler voraussetzt; auf die sich hieraus ergebenden Gefahren erstreckt sich die Entscheidung, sich selbst zu gefährden, bei normativer Betrachtung grundsätzlich nicht. Auch der Umstand, dass ggf. auch ein vertraglicher Anspruch besteht, schließt die Herstellerhaftung nicht aus (vgl. § 1 ProdHaftG; § 84 AMG).

---

[126] Zu diesem Erfordernis s. oben unter 2. a.

(4) Zwischenergebnis

Es ist produktbezogen zu untersuchen, ob die Gefährdungshaftung des Betreibers auch gegenüber dem Profiteur bestehen sollte. Sofern mit dem Produkt typischerweise ausschließlich solche Personen in Berührung kommen, die über die Risiken des Produkts hinreichend aufgeklärt werden, ist eine Gefährdungshaftung des Betreibers (!) grundsätzlich nicht geboten. Das gilt jedenfalls dann, wenn für das Produkt ein besonderes Zulassungsverfahren existiert und dem Geschädigten – bei typisierender Betrachtung – im Falle eines Produktfehlers hinreichende Ansprüche gegen den Hersteller zustehen.

5. Ergebnis

Was die Haftung des Herstellers angeht, so greift der Haftungsgrund, welcher der Produkthaftung zugrunde liegt, ohne weiteres auch dann ein, wenn es um autonome Systeme geht. Allerdings ist zu prüfen, ob einzelne Regelungen des ProdHaftG auf den Einsatz autonomer Systeme abzustimmen sind. Etwaige Beweisschwierigkeiten, ob das Produkt fehlerhaft ist, rechtfertigen für sich genommen nicht die Einführung einer Gefährdungshaftung des Herstellers unabhängig vom Vorliegen eines Produktfehlers, sondern ggf. eine Beweislastumkehr. Eine Gefährdungshaftung des Herstellers ist vielmehr nur dann systemgerecht, wenn die Haftung an einen Produktfehler anknüpft.

Im Rahmen der Prüfung, ob eine Gefährdungshaftung des Betreibers systemkonform ist, muss zunächst produktbezogen ermittelt werden, ob von der Sache eine „besondere Gefahr“ ausgeht. Das wird man auch bei autonomen Systemen nicht generell annehmen können. Auch wenn diese Frage zu bejahen ist, ist eine Gefährdungshaftung des Betreibers jedenfalls dann nicht geboten, wenn für das Produkt ein besonderes Zulassungsverfahren existiert, dem Geschädigten im Falle eines Produktfehlers hinreichende Ansprüche gegen den Hersteller zustehen und mit dem Produkt typischerweise nur Personen in Berührung kommen, die freiwillig sich der Gefahr ausgesetzt haben und über die Gefahren, die von dem Betrieb des autonomen Systems ausgehen, sachgerecht aufgeklärt wurden.

IV. Insbesondere: Haftung nach dem Produkthaftungsgesetz und deliktische Produzentenhaftung

1. Hintergrund

Das Produkthaftungsgesetz (ProdHaftG) vom 15. Dezember 1989[127] dient der Umsetzung der Produkthaftungsrichtlinie[128]. Nach Erwägungsgrund 2 zur Richtlinie kann „nur bei einer verschuldensunabhängigen Haftung des Herstellers das unserem Zeitalter fortschreitender Technisierung eigene Problem einer gerechten Zuweisung der mit der modernen technischen Produktion verbundenen Risiken in sachgerechter Weise gelöst werden." Das Produkthaftungsrecht dient damit dem Schutz des Verbrauchers vor den besonderen Risiken der industriellen Produktion.[129] In der Begründung zum ProdHaftG wird darüber hinaus ausgeführt, das bestehende System von Sicherheitsvorschriften habe sich zwar bewährt und trage den Interessen von Produktbenutzern, Verbrauchern und Herstellern gleichermaßen Rechnung, diene aber vorrangig der Vorsorge und Schadensverhütung. Es könne aber nicht übersehen werden, dass trotzdem in Einzelfällen Konsumenten bei dem Gebrauch oder Verbrauch eines Produkts in ihrer körperlichen Integrität oder an ihrem Eigentum oder Vermögen geschädigt werden; hierfür bestehe ein Bedürfnis nach Ausgleich des erlittenen Schadens.[130]

Neben der oben dargestellten deliktischen Produzentenhaftung hat der nationale Gesetzgeber auch aus folgenden Gründen das Bedürfnis nach einer verschuldensunabhängigen Haftung gesehen:[131]

- Die deliktsrechtliche Produzentenhaftung basiere auf einer schwer überschaubaren Einzelfallrechtsprechung.
- Das angestrebte Ergebnis einer möglichst an objektiven Kriterien orientierten Haftung lasse sich mit den Mitteln des Deliktsrechts nur durch außerordentlich hohe abstrakte Sorgfaltsanforderungen erreichen.
- Der Vorwurf, gegen solche Sorgfaltsanforderungen verstoßen zu haben, sei der Vorwurf des „Unrechts", was den Beziehungen zwischen Herstellern und Abnehmern unter Berücksichtigung der modernen Produktionsmethoden nicht gerecht werde.

---

[127] BGBl. I 1989, 2198.
[128] Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte.
[129] Staudinger/*Oechsler*, BGB, Bearb. 2013, Einl zum ProdHaftG Rn. 18.
[130] BT-Drs. 11/2447, S. 7.
[131] BT-Drs. 11/2447, S. 8.

- Die im Bereich der deliktsrechtlichen Produzentenhaftung praktizierten Beweiserleichterungen in ihrer unterschiedlichen Art ließen im Einzelfall eine verlässliche Aussage über das Haftungsrisiko kaum zu.

2. Haftungsvoraussetzungen

Das Gesetz regelt die Haftung des Herstellers für Folgeschäden, die der bestimmungsgemäße Verbraucher oder sonstige Personen durch die Benutzung des fehlerhaften Produkts erleiden. Es handelt sich dabei um eine verschuldensunabhängige Gefährdungshaftung,[132] die einen Haftungshöchstbetrag bei Tod oder Körperverletzung (§ 10 ProdHaftG) und eine Selbstbeteiligung bei Sachschäden (§ 11 ProdHaftG) bestimmt. Der Anspruchsteller muss „lediglich" nachweisen, dass ein Fehler des Produkts vorlag und daraus ein kausaler Schaden entstanden ist, § 1 Abs. 4 ProdHaftG. Im Rahmen der Beweisführung kommt ihm der Anscheinsbeweis zugute, sofern ein typischer Geschehensablauf vorliegt.[133]

Die Unterschiede beim Nachweis der Haftungsvoraussetzungen gegenüber der verschuldensabhängigen Produzentenhaftung sind in der Praxis allerdings gering. Denn der BGH verlangt zum Nachweis der Produzentenhaftung vom Anspruchsteller ebenfalls lediglich den Nachweis eines Fehlers des Produkts und verzichtet auf Darlegungen und Nachweise zum pflichtwidrigen Verhalten des Herstellers.[134] Liegt ein Produktfehler vor, ist es Sache des Herstellers, darzulegen und nachzuweisen, welche Personen innerhalb seines Unternehmens welche Maßnahmen ergriffen haben, um das Inverkehrbringen des fehlerhaften Produkts zu vermeiden.

Im Folgenden werden die Grundlagen des ProdHaftG skizziert. Dabei wird das Hauptaugenmerk auf die Frage gelegt, welche Besonderheiten insoweit zu beachten sind, wenn es um Schäden geht, die durch den Einsatz autonom agierender Systeme verursacht wurden.

a. Produktbegriff

Der Produktbegriff des ProdHaftG umfasst nur bewegliche Sachen, auch wenn diese einen Teil einer anderen beweglichen oder einer unbeweglichen Sache bilden, sowie Elektrizität (§ 2 ProdHaftG). Damit wird letztlich der Zielrichtung der Produkthaftungsrichtlinie (Bewältigung der Risiken moderner technischer

---

[132] Palandt/*Sprau*, BGB, ProdhaftG, Einf. Rn. 1; a.A. Staudinger/*Oechsler*, BGB; Bearb. 2013, Einl. zum ProdHaftG, Rn. 27, der von einem Mischsystem aus Haftung für Verschuldensunrecht und Gefahr ausgeht.

[133] *Vogt,* Fahrassistenzsysteme: Neue Technik – Neue Rechtsfragen?, NZV 2003, 153 (157 f.).

[134] Ständige Rechtsprechung seit BGH, Urt. v. 26.11.1968 – VI ZR 212/66, BGHZ 51, 91 (102) – Hühnerpest.

Produktion) Rechnung getragen, deren Anwendungsbereich sich nach Erwägungsgrund 3 auf bewegliche Sachen beschränkt, die industriell hergestellt werden. Die Gesetzesbegründung zu § 2 ProdHaftG aus dem Jahre 1988 fasst hierunter neben Elektrizität jede bewegliche Sache im Sinne des § 90 BGB, ohne dass es auf eine spezifische Gefährlichkeit oder einen besonderen Verwendungszweck ankäme, unter anderem z.B. Konsumgüter, technische Anlagen, Maschinen und Geräte, Fahrzeuge, chemische Stoffe, Zubereitungen und Erzeugnisse und Verpackungsmaterialien.[135] Für Arzneimittel gelten die Vorschriften des ProdHaftG dagegen grundsätzlich nicht (§ 15 Abs. 1 ProdHaftG); dies vor dem Hintergrund, dass hierfür mit § 84 AMG Spezialregelungen bestehen (vgl. dazu unten).

Zum Zeitpunkt der Entstehung der Produkthaftungsrichtlinie und des ProdHaftG noch nicht ausdrücklich thematisiert wurden dagegen sog. verkörperte geistige Leistungen. Deren Bedeutung nimmt aber angesichts der fortschreitenden Technisierung von Arbeitsvorgängen, Anlagen, Maschinen und Produkten stetig zu. Insbesondere die Funktionsweise sog. Smart Products beruht maßgeblich auf elektronisch gespeicherten bzw. übermittelten Informationen sowie integrierten Computerprogrammen (Apps). Während die Anwendbarkeit des ProdHaftG noch unbestritten gegeben ist, wenn die schadensauslösende Fehlerhaftigkeit des Produkts in dessen körperlicher Beschaffenheit liegt,[136] ist die Einordnung schwieriger, wenn die gespeicherte Information selbst aufgrund ihres Inhalts den Schaden auslöst. Die Leistung bewegt sich in diesem Zusammenhang nämlich an der Schnittstelle zwischen Produkt und Dienstleistung, wobei letztere keinesfalls von der Produkthaftungsrichtlinie und dem darauf basierenden ProdHaftG erfasst wird.[137]

In Teilen der Literatur[138] wird angeführt, die Anknüpfung der Produkthaftung an die Verkörperung sei willkürlich. Dies zeige die fortdauernde technische Entwicklung; insofern könne es keinen Unterschied mehr machen, ob beispielsweise die Reparaturanleitung für ein Gerät in (verkörperter) Druckform oder via Internet oder einer App erteilt werde. Auf dieser Grundlage wird (auch aus Gründen der Praktikabilität) auch die Auffassung[139] vertreten, das ProdHaftG solle auch auf solche „Produkte“ bzw. Fehlerkategorien anzuwenden sein. Nach

---

[135] BT-Drs. 11/2447, S. 16.
[136] BeckOK BGB/*Förster*, Stand: 1.11.2017, § 2 ProdHaftG Rn. 18; *Cahn*, Produkthaftung für verkörperte geistige Leistung, NJW 1996, 2899 (2901); so auch Palandt/*Sprau*, BGB, § 2 ProdHaftG Rn. 1, wonach bei verkörperten geistigen Leistungen die Verkörperung Produkt ist.
[137] MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 12.
[138] MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 15 m.w.N.
[139] So etwa *Cahn,* Produkthaftung für verkörperte geistige Leistung, NJW 1996, 2899 (2901); *Kort*, Software – eine Sache?, DB 1994, 1505.

anderer Auffassung[140] ist darauf abzustellen, ob die geistige Leistung überhaupt mit einem Träger verbunden ist; bereits unter dieser Voraussetzung sei die Produkteigenschaft zu bejahen. Unklar bleibt allerdings, ob hiervon nur „klassische" Datenträger wie z.B. Festplatten, USB-Sticks, etc. erfasst werden sollen oder auch Datenträger, die selbst wiederum in einem Produkt verbaut sind (z.B. Datenträger für Software in Smart Products, Steuerungseinheiten in Fahrzeugen etc.). In jüngster Zeit stellt sich diese Frage verstärkt dadurch, dass Software nicht immer unter Zuhilfenahme eines körperlichen Datenträgers erworben wird, sondern entweder aus dem Internet heruntergeladen und erst vom Nutzer auf einem eigenen Datenträger gespeichert wird oder Anwendungen gar nicht erst heruntergeladen werden, sondern über eine Cloud genutzt werden.[141] Knüpft man indes maßgeblich an die Körperlichkeit an, unterfällt jedenfalls die in Produkten, insbesondere in Smart Products, integrierte Software eindeutig dem ProdHaftG.[142] In diese Richtung dürfte auch der BGH[143] im Rahmen seiner sog. Airbag-Entscheidung tendieren, in der er ein Fahrzeug einschließlich des darin verbauten Airbagsystems und der entsprechenden Steuergerätesoftware unproblematisch als Produkt ansah.

Die Europäische Kommission führt diesbezüglich in einem „vorläufigen Konzept" zu zukünftigen Leitlinien zur ProdHaftRL aus, dass die rechtliche Kategorisierung von Software nicht von dem Medium der Überlieferung bzw. Installation abhängen solle.[144] Es sei zudem gut begründbar, Software, die zu jedem erdenklichen Zeitpunkt heruntergeladen und von einem System auf weitere übertragen werden kann, als beweglich und damit als Produkt im Sinne der ProdHaftRL zu kategorisieren.[145] Jedoch erkennt die Europäische Kommission auch, dass vereinzelte Stimmen für eine Einordnung von Software als Dienstleistung plädieren.[146]

---

[140] Staudinger/*Oechsler*, Berarb. 2013, § 2 ProdHaftG Rn. 64; Erman/*Wilhelmi*, BGB, § 2 ProdHaftG Rn. 2.

[141] Eine Produkteigenschaft bejahend z.B. *Cahn*, Produkthaftung für verkörperte geistige Leistung, NJW 1996, 2899 (2904), MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 15; ablehnend dagegen etwa Staudinger/*Oechsler*, Bearb. 2013, § 2 ProdHaftG Rn. 65 ff.

[142] MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 19.

[143] BGH, Urt. v. 16.6.2009 – VI ZR 107/08, BGHZ 181, 253.

[144] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 4.1.3. (22) [Stand: 18.9.2018].

[145] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 4.1.3. (24) [Stand: 18.9.2018].

[146] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 4.1.3. (24) [Stand: 18.9.2018].

Die bislang wohl überwiegende Meinung[147] geht jedenfalls davon aus, dass zumindest Standardsoftware als Produkt im Sinne des § 2 ProdHaftG zu qualifizieren ist, auch wenn der Fehler nicht dem Datenträger (sofern überhaupt vorhanden), sondern der Software selbst innewohnt. Begründet wird dies mit der kaufrechtlichen Wertung, nach der Standardsoftware als Kaufsache betrachtet wird;[148] dagegen stehe bei Individualsoftware eher die mit der Erstellung der Software verbundene geistige Leistung im Vordergrund, sodass diese nicht mehr als Produkt zu qualifizieren sei, sondern eher in die (schuldrechtlichen) Kategorien des Werks bzw. der Dienstleistung einzuordnen sei. Dagegen wird wiederum angeführt, die Unterscheidung zwischen Standard- und Individualsoftware sei nicht einsichtig, da es keinen Unterschied machen könne, ob die geistige Leistung auf eine allgemeinspezifische oder anwenderspezifische Nutzung ausgerichtet sei.[149] Ein gewichtiges Argument spricht indes für eine Abgrenzung zwischen Software als Massenprodukt auf der einen und Software als individuell auf die Kundenwünsche angepasste Leistung auf der anderen Seite: Die Produkthaftungsrichtlinie ist nach Erwägungsgrund 2 gerade auf Produkte anwendbar, die „industriell hergestellt“ werden, d.h. in größerer Vielzahl nach einem einheitlichen Produktionsschema und für den allgemeinen Markt angefertigte Gegenstände. Nichts anderes darf dann auch für geistige Leistungen gelten. Zweck des harmonisierten Produkthaftungsrechts ist es, dem Hersteller industriell hergestellter Güter Anreize zu sorgfältigem Verhalten zu vermitteln und den Nutzer vor Schäden beim Gebrauch dieser Güter zu schützen.[150] Allerdings ist auch die Frage der Abgrenzung zwischen Standard- und Individualsoftware nicht eindeutig geklärt. So wird zum Teil vertreten, dass der reine Dienstleistungscharakter nicht bereits bei der Erstellung individueller Software überwiege, sondern erst beispielsweise bei einem Software-Wartungsvertrag.[151]

b. Erfasste Schäden

Die Haftung ist beschränkt auf Fälle des Todes und der Verletzung von Körper oder Gesundheit sowie auf die Beschädigung von Sachen (§ 1 Abs. 1 ProdHaftG); primäre Vermögensschäden, die nicht an eine Rechtsgutsverletzung

---

[147] Herberger/Martinek/Rüßmann u.a./*M. Hamdan/Günes* jurisPK-BGB, 8. Aufl. 2017, § 2 ProdHaftG Rn. 9; Staudinger/*Oechsler*, Bearb. 2013, § 2 ProdHaftG Rn. 69; *Kort,* Software – eine Sache?, DB 1994, 1505; *Deutsch*, Das neue System der Gefährdungshaftungen – Gefährdnungshaftung, erweiterte Gefährdnungshaftung und Kausal-Vermutungshaftung, NJW 1992, 73 (76); s. auch MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 20: Anwendung des ProdHaftG im Wege der teleologischen Auslegung auch auf nicht verkörperte reine Online-Anwendungen.

[148] MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 15.

[149] Herberger/Martinek/Rüßmann u.a./*M. Hamdan/Günes*, jurisPK-BGB, 8. Aufl. 2017, § 2 ProdHaftG Rn. 9.

[150] MüKo/*Wagner*, BGB, § 2 ProdHaftG Rn. 19.

[151] BeckOK BGB/*Förster*, Stand: 1.11.2017, § 2 ProdHaftG Rn. 2.

anknüpfen, sind dagegen nicht ersatzfähig.[152] Bei der Verursachung eines Schadens an der Gesundheit oder dem Körper durch ein fehlerhaftes Produkt oder System besteht die Haftung des Herstellers unabhängig davon, ob der Schaden bei einem gewerblichen Käufer, dem Endabnehmer oder einem Dritten eingetreten ist. § 1 Abs. 1 S. 2 ProdHaftG erfasst dagegen nur den Sachschaden, der einem privaten Endverbraucher oder einem unbeteiligten Dritten entstanden ist. Gewerblich genutzte Sachen erhalten insoweit durch das ProdHaftG keinen Schutz. Relevante Schutzlücken dürften dadurch aber nicht entstehen, da nach § 15 Abs. 2 ProdHaftG die verschuldensabhängige Haftung des Produzenten gemäß §§ 823 ff. BGB unberührt bleibt, die nicht nach der Art der Nutzung der beschädigten Sache differenziert. Zumindest sind insoweit keine Besonderheiten hinsichtlich der Herstellung und des Inverkehrbringens autonomer Systeme ersichtlich, die eine Sonderregelung für diesen Bereich rechtfertigen könnten. Das gilt auch für die Ausklammerung primärer Vermögensschäden.

c. Fehlerbegriff

Das Produkthaftungsrecht verfügt in Abgrenzung zum kauf- oder werkvertragsrechtlichen Mangelbegriff über einen eigenen Fehlerbegriff, § 3 ProdHaftG. Die Fehlerhaftigkeit des Produkts ist gegeben, „wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände insbesondere seiner Darbietung, des Gebrauchs, mit dem billigerweise gerechnet werden kann, und dem Zeitpunkt, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartet werden konnte“. Anknüpfungspunkt ist daher eine Fehlerhaftigkeit im Zeitpunkt des Inverkehrbringens. § 3 Abs. 2 ProdHaftG stellt klar, dass ein Produkt nicht allein deshalb einen Fehler aufweist, weil später ein verbessertes Produkt in den Verkehr gebracht wurde. Ein nach dem Zeitpunkt des Inverkehrbringens bereitgestelltes Update oder Upgrade des Produkts lässt demnach nicht notwendigerweise auf einen Fehler des Ursprungsprodukts schließen.[153] Die nach § 3 Abs. 1 ProdHaftG maßgeblichen Sicherheitserwartungen beurteilen sich grundsätzlich nach denselben objektiven Maßstäben wie die Verkehrspflichten des Herstellers im Rahmen der deliktischen Haftung gemäß § 823 Abs. 1 BGB.[154]

In der Regel wird zwischen Konstruktionsfehlern, Fabrikationsfehlern und Instruktionsfehlern unterschieden.[155] Dadurch, dass der Hersteller die Erwartungshaltung der Öffentlichkeit durch die Beschreibung der Qualität und Leistungsfä-

---

[152] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 2015, 766 (773).
[153] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 4.3.(33) [Stand: 18.9.2018].
[154] BGH, Urt. v. 17.3.2009 – VI ZR 176/08, VersR 2009, 649 f. m.w.N.
[155] *Lutz/Tang/Lienkamp*, Die rechtliche Situation von teleoperierten und autonomen Fahrzeugen, NZV 2013, 57 (61).

higkeit selbst schafft, beeinflusst er den maßgeblichen Fehlerbegriff für seine Haftung nach dem ProdHaftG; eine absolute Gefahrlosigkeit darf der Verkehr aber nach der sog. Kirschkern-Entscheidung des BGH[156] jedenfalls nicht erwarten.

(1) Konstruktionsfehler

Konstruktionsfehler ergeben sich typischerweise durch fehlerhafte technische Konzeption. Nach der Rechtsprechung des BGH[157] liegt ein Konstruktionsfehler vor, wenn das Produkt schon seiner Konzeption nach unter dem gebotenen Sicherheitsstandard bleibt. Zur Gewährleistung der erforderlichen Produktsicherheit hat der Hersteller bereits im Rahmen der Konzeption und Planung des Produkts diejenigen Maßnahmen zu treffen, die zur Vermeidung einer Gefahr objektiv erforderlich und nach objektiven Maßstäben zumutbar sind. Erforderlich sind die Sicherungsmaßnahmen, die nach dem im Zeitpunkt des Inverkehrbringens des Produkts vorhandenen neuesten Stand der Wissenschaft und Technik konstruktiv möglich sind und als geeignet und genügend erscheinen, um Schäden zu verhindern. Dabei darf der insoweit maßgebliche Stand der Wissenschaft und Technik nicht mit Branchenüblichkeit gleichgesetzt werden; die in der jeweiligen Branche tatsächlich praktizierten Sicherheitsvorkehrungen können durchaus hinter der technischen Entwicklung und damit hinter den rechtlich gebotenen Maßnahmen zurückbleiben. Zu dem Mindeststandard, den die Allgemeinheit berechtigterweise erwarten kann, gehört dabei die Einhaltung technischer Normen und gesetzlicher Sicherheitsbestimmungen. Technische Normen und öffentliche Zulassungsverfahren bieten zwar eine wertvolle Orientierungshilfe für die Konkretisierung deliktsrechtlicher Sorgfaltspflichten. Ihre Einhaltung bzw. die öffentlich-rechtliche Zulassung genügen aber nicht, wenn die technische Entwicklung darüber hinausgegangen ist.[158]

Die Möglichkeit der Gefahrvermeidung ist gegeben, wenn nach gesichertem Fachwissen der einschlägigen Fachkreise praktisch einsatzfähige Lösungen zur Verfügung stehen. Hiervon kann grundsätzlich erst dann ausgegangen werden, wenn eine sicherheitstechnisch überlegene Alternativkonstruktion zum Serieneinsatz reif ist. Der Hersteller ist dagegen nicht dazu verpflichtet, solche Sicherheitskonzepte umzusetzen, die bisher nur „auf dem Reißbrett erarbeitet" oder noch in der Erprobung befindlich sind. Sind bestimmte mit der Produktnutzung einhergehende Risiken nach dem maßgeblichen Stand von Wissenschaft und Technik nicht zu vermeiden, ist unter Abwägung von Art und Umfang der Risiken, der Wahrscheinlichkeit ihrer Verwirklichung und des mit dem Produkt ver-

---

[156] BGH, Urt. v. 17.3.2009 – VI ZR 176/08, NJW 2009, 1669 (1670 f.).
[157] Zusammenfassend dargestellt etwa in der sog. Airbagentscheidung, BGH, Urt. v. 16.6.2009 – VI ZR 107/08, NJW 2009, 2952.
[158] BGH, Urt. v. 9.9.2008 – VI ZR 279/06, NJW 2008, 3779 Rn. 16.

bundenen Nutzens zu prüfen, ob das gefahrträchtige Produkt überhaupt in den Verkehr gebracht werden darf.

Lassen sich mit der Verwendung eines Produkts verbundene Gefahren nach dem Stand von Wissenschaft und Technik durch konstruktive Maßnahmen nicht vermeiden oder sind konstruktive Gefahrvermeidungsmaßnahmen dem Hersteller nicht zumutbar und darf das Produkt trotz der von ihm ausgehenden Gefahren in den Verkehr gebracht werden, so ist der Hersteller grundsätzlich verpflichtet, die Verwender des Produkts vor denjenigen Gefahren zu warnen, die bei bestimmungsgemäßem Gebrauch oder nahe liegendem Fehlgebrauch drohen und die nicht zum allgemeinen Gefahrenwissen des Benutzerkreises gehören (Instruktionspflicht).

Die Frage, ob eine Sicherungsmaßnahme nach objektiven Maßstäben zumutbar ist, lässt sich nur unter Berücksichtigung sämtlicher Umstände des Einzelfalls beurteilen. Maßgeblich ist insbesondere die Größe der vom Produkt ausgehenden Gefahr. Je größer die Gefahren sind, desto höher sind die Anforderungen, die in dieser Hinsicht gestellt werden müssen. Bei erheblichen Gefahren für Leben und Gesundheit von Menschen sind dem Hersteller weitergehende Maßnahmen zumutbar als in Fällen, in denen nur Eigentums- oder Besitzstörungen oder aber nur kleinere körperliche Beeinträchtigungen zu befürchten sind. Maßgeblich für die Zumutbarkeit sind darüber hinaus die wirtschaftlichen Auswirkungen der Sicherungsmaßnahme, im Rahmen dieser insbesondere die Verbrauchergewohnheiten, die Produktionskosten, die Absatzchancen für ein entsprechend verändertes Produkt sowie die Kosten-Nutzen-Relation.

Diese Grundsätze erscheinen auch zur Bestimmung der an eine sichere Konstruktion von autonomen Systemen zu stellenden rechtlichen Anforderungen im Prinzip passend und sachgerecht. Es liegt aber auf der Hand, dass ihre konkrete Anwendung gerade im Hinblick auf die äußerst dynamische technische Entwicklung in diesem Bereich erhebliche praktische Schwierigkeiten aufwerfen kann.

Für autonome Systeme relevante softwarespezifische Konstruktionsfehler können dabei vor allem im Hinblick auf den Entwurf, die Programmierung oder die Kompilierung vorliegen. Insbesondere zählt es zu den berechtigten Sicherheitserwartungen, vor allem an autonome Systeme, dass jede sicherheitsrelevante Software gegen unautorisierte Eingriffe von außen (Hackerangriffe) hinreichend abgeschirmt ist. Nach den oben dargestellten Grundsätzen kann allerdings auch

in dieser Hinsicht produkthaftungsrechtlich keine absolute Sicherheit erwartet werden.[159]

Soweit autonom agierende Produkte sicherheitsrelevante Aktionen steuern, die bislang von Menschen vorgenommen wurden, stellt sich die Frage, ob und ggf. inwieweit das hypothetische Verhalten eines sorgfältigen Menschen als Vergleichsmaßstab herangezogen werden kann, um das erforderliche konstruktive Maß an Sicherheit des autonomen Systems zu bestimmen, oder ob insoweit kein „anthropozentrischer" sondern ein „systembezogener" Sorgfaltsmaßstab entwickelt werden muss.[160] Diese Problematik soll am Beispiel des autonomen Fahrens im Folgenden unter F. III. noch vertieft werden.

(2) Fabrikationsfehler

Von einem Fabrikationsfehler wird gesprochen, wenn das Produkt zwar fehlerfrei konzipiert ist, es jedoch im Fertigungsprozess zu einer planwidrigen Abweichung von der vom Hersteller vorgesehenen Soll-Beschaffenheit kommt.[161] Sog. Ausreißer, d. h. einzelne Stücke, die vom für eine Produktserie geltenden Standard abweichen, obgleich der Hersteller alle zumutbaren Maßnahmen vorgenommen hat und der Fehler dennoch nicht zu vermeiden war, können zwar von der Haftung nach dem ProdHaftG, mangels Verschulden aber nicht von der deliktischen Produzentenhaftung erfasst werden. Bei Produkten mit integrierter Software kommen Fabrikationsfehler insbesondere in Betracht, wenn bei der Übertragung des Programms von einem auf einen anderen Speicherort Fehler erzeugt werden oder sich Schadprogramme einschleichen.[162]

(3) Instruktionsfehler

Instruktionspflichten sind bei mangelhaften Gebrauchsanweisungen oder nicht ausreichenden Warnungen vor Gefahr bringenden Eigenschaften des an sich fehlerlosen Produkts verletzt.[163]

---

[159] So auch *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707, (727 f.); zumindest tendenziell weitergehend *Gomille,* Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (77 f.).
[160] Vgl. dazu *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (733 ff.).
[161] Staudinger/*Hager*, BGB, Bearb. 2016, § 823 Rn. F 17.
[162] *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (78).
[163] *Lutz/Tang/Lienkamp*, Die rechtliche Situation von teleoperierten und autonomen Fahrzeugen, NZV 2013, 57 (61).

d. Haftungsausschlusstatbestände

Von Interesse ist hier insbesondere die Regelung in § 1 Abs. 2 Nr. 5 ProdHaftG, wonach für unvermeidbare Entwicklungsfehler die Haftung ausgeschlossen ist, wenn der Produktfehler zum Zeitpunkt des Inverkehrbringens bei Einhaltung des Stands der Wissenschaft und Technik für den Hersteller nicht erkennbar war, wobei die Beweislast insoweit den Hersteller trifft (im Rahmen der deliktischen Produzentenhaftung fehlt es in diesen Fällen am Verschulden). Zwingend ist diese Einschränkung nicht: Die sog. Produkthaftungsrichtlinie[164], deren Umsetzung das ProdHaftG dient, sieht eine solche Einschränkung zwar in Art. 7 lit. e grundsätzlich vor; gem. Art. 15 Abs. 1 lit. b der Richtlinie können mitgliedstaatliche Vorschriften aber eine Haftung auch in diesen Fällen vorsehen. Hiervon hat der deutsche Gesetzgeber allerdings keinen Gebrauch gemacht. Der Rechtsausschuss des Bundestages hatte sich insoweit mehrheitlich dafür ausgesprochen, eine Haftung für Entwicklungsrisiken nicht einzuführen, letztlich im Rahmen einer Abwägung zwischen einer aus Sicht des Ausschusses geringen Haftungslücke mit den Konsequenzen, die eine solche Haftung für die Innovationsbereitschaft von Wirtschaft und Industrie hätte. In BT-Drs. 11/5520, S. 13 heißt es:

> „In der Anhörung und den Beratungen ist dem entgegengehalten worden, dass damit die in einer fortschreitenden Technik liegenden Risiken auf den Geschädigten verlagert würden. Dies sei nicht hinnehmbar. Dem Hersteller, der aus technischen Neuerungen seinen Nutzen ziehe, regelmäßig über bessere Möglichkeiten der Abschätzung auch entlegener potentieller Risiken verfüge und diese versichern könne, müsse auch die Haftung für solche Risiken zugemutet werden.
>
> Die Mehrheit verwies darauf, dass es sich hier nur um einen äußerst schmalen haftungsfreien Raum handele. Die haftungsbefreiende Wirkung trete nur dann ein, wenn die die Schädlichkeit des Produkts begründenden Wirkungszusammenhänge nach dem Stand der naturwissenschaftlich-technischen Erkenntnis objektiv nicht erkennbar waren, als das Produkt in Verkehr gebracht wurde. Hierbei komme es nicht auf die eigenen Erkenntnismöglichkeiten des Herstellers an, sondern auf den objektiven ggf. über Ländergrenzen hinausreichend festzustellenden Erkenntnisstand. Es komme hinzu, dass die Voraussetzungen für diesen Haftungsausschluss der Hersteller zu beweisen habe. Außerdem greife, sobald die Gefährlichkeit des Produkts erkennbar werde, die herkömmliche Deliktshaftung ein, sobald die Produktbeobachtungspflicht verletzt oder die aus der Produktbeobachtung folgenden Konsequenzen nicht gezogen würden.

---

[164] Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte.

> Es gelte mithin, diese eher als gering zu veranschlagende Haftungslücke abzuwägen mit den Konsequenzen, die ein Verzicht auf diesen Haftungsausschlussgrund für die Innovationsbereitschaft von Wirtschaft und Industrie entfalten müsse. Diese sei aber eine wesentliche Triebfeder der wirtschaftlichen Entwicklung insgesamt und dürfe auch im Interesse der Allgemeinheit nicht unvertretbar beengt und geschwächt werden. Auch müsse davon ausgegangen werden, dass innerhalb der Europäischen Gemeinschaft nach dem derzeitigen Stand der Umsetzung der Richtlinie weiterhin von diesem Haftungsausschlussgrund Gebrauch gemacht werde, so dass auch aus Wettbewerbsgründen von einer entsprechenden Regelung nicht abgegangen werden könne."

Der Entlastungstatbestand des § 1 Abs. 2 Nr. 5 ProdHaftG kommt nur dann zum Tragen, wenn es sich um ein Produkt handelt, das nach den Sicherheitserwartungen zum Zeitpunkt des Inverkehrbringens als fehlerhaft zu beurteilen war.[165] Nach der Rechtsprechung[166] gelangt § 1 Abs. 2 Nr. 5 ProdHaftG bei Konstruktions- und Instruktionsfehlern, nicht aber bei Fabrikationsfehlern zur Anwendung.

Weitere Voraussetzung ist, dass die von dem Produkt ausgehende Gefahr nach dem Stand von Wissenschaft und Technik im Zeitpunkt des Inverkehrbringens nicht erkannt werden konnte. Es handelt sich um den anspruchsvollsten Standard, den das Technikrecht kennt, denn er geht über den Maßstab der „Regeln der Technik“ und denjenigen des „Stands der Technik“ hinaus.[167] Nach der Gesetzesbegründung[168] ist darunter „der Inbegriff der Sachkunde zu verstehen, die im wissenschaftlichen und technischen Bereich vorhanden ist, also die Summe an Wissen und Technik, die allgemein anerkannt ist und allgemein zur Verfügung steht. Es kommt demnach nicht auf die wissenschaftlichen oder technischen Erkenntnismöglichkeiten des einzelnen Herstellers, sondern objektiv auf den gegebenenfalls über Ländergrenzen hinausreichenden Stand von Wissenschaft und Technik an. Nur wenn vor diesem Hintergrund die potentielle Gefährlichkeit des Produkts nicht erkannt werden konnte, weil diese Erkenntnismöglichkeit zum Zeitpunkt des Inverkehrbringens (noch) nicht weit genug fortgeschritten war, ist die Haftung ausgeschlossen.“ An das Qualitätsmanagement des Herstellers sind in diesem Zusammenhang hohe Anforderungen zu stellen: Regelmäßig wird ein Entlastungsbeweis nur gelingen, wenn der Hersteller aufzeigt, dass er seine Produkte vor der Inverkehrgabe einem Kontrollverfahren

---

[165] BGH, Urt. v. 5.2.2013 – VI ZR 1/12, NJW 2013, 1302; *Taschner*, Die künftige Produzentenhaftung in Deutschland, NJW 1986, 611 (615).
[166] BGH, Urt. v. 9.5.1995 - VI ZR 158/94, LMRR 1995, 23, Urt. v. 16.6.2009 - VI ZR 107/08, NJW 2952 (2955).
[167] MüKo/*Wagner*, BGB, § 1 ProdHaftG Rn. 54.
[168] BT-Drs. 11/2447, S. 15 f.

unterzieht, das sämtliche nach dem aktuellen Stand der Technik verfügbaren Möglichkeiten ausschöpft, um etwaige verborgene Konstruktionsfehler zu entdecken.[169] Nach der Airbag-Entscheidung des BGH ist unter der potentiellen Gefährlichkeit des Produkts nicht der konkrete Fehler des schadensstiftenden Produkts, sondern das zugrunde liegende allgemeine, mit der gewählten Konzeption verbundene Fehlerrisiko zu verstehen, d.h. das zugrunde liegende allgemeine Fehlerrisiko.[170]

Ausgehend von diesen Grundsätzen liegt der Schluss nahe, dass es auch bei selbstlernenden Produkten, die „eigenständige" Entscheidungen treffen können, nicht auf die im konkreten Einzelfall „falsche" bzw. schadensauslösende Entscheidung ankommt, sondern auf das Risiko, welches das selbstlernende Produkt wegen eben dieser Fähigkeit mit sich bringt. Dementsprechend ist in der Literatur darauf hingewiesen worden, dass sich ein Hersteller nicht durch Hinweis auf die „Unkontrollierbarkeit" selbstlernender autonomer Systeme von seiner Haftung gemäß § 1 Abs. 2 Nr. 5 ProdHaftG entlasten kann. Denn diese Eigenschaft selbstlernender autonomer Systeme (Unkontrollierbarkeit) sei erkennbar und damit gerade kein Entwicklungsrisiko.[171] Demgegenüber wird vertreten, dass das Entwicklungsrisiko für nachträglich auftretende Fehler gelte, die auf der Lernfähigkeit von Algorithmen beruhen und zum Zeitpunkt der Inverkehrgabe nach dem Stand der Wissenschaft und Technik nicht erkennbar waren. Insoweit scheide mangels Verschuldens auch eine Haftung nach der deliktischen Produzentenhaftung aus, wenn der vorhandene Fehler objektiv nicht erkannt werden konnte, was aufgrund der indeterminierten Verhaltensweise intelligenter Produkte regelmäßig der Fall sein werde.[172]

Für die von der Arbeitsgruppe untersuchten Produktbereiche ist die Problematik der „unkontrollierbaren" Systeme mit erheblichem Gefährdungspotenzial allerdings noch nicht aktuell. Nach dem Ergebnis der von der Arbeitsgruppe durchgeführten Expertenanhörungen werden zumindest in den – zulassungspflichtigen – Bereichen der Fahrzeug- und Medizintechnik nur „gekapselte" Systeme auf den Markt gebracht, die sich nach dem Inverkehrbringen nicht mehr durch „Selbstlernen" verändern. Die Gefahr einer „unkontrollierbaren" Entscheidung wurde daher verneint.

Da in absehbarer Zeit keine selbstlernenden Systeme zum Einsatz kommen werden und angesichts der allgemein äußerst strengen Maßstäbe bei der Bestim-

---

[169] *Gomille,* Herstellerhaftung für automatisierte Fahrzuge, JZ 2016, 76 (79).
[170] BGH, Urt. v. 16.6.2009 - VI ZR 107/08, NJW 2009, 2952 (2955 f.); Staudinger/*Oechsler*, Bearb. 2013, § 1 ProdHaftG Rn. 120.
[171] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (713, 750).
[172] *Droste,* Intelligente Medizinprodukte: Verantwortlichkeit des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (111).

mung eines Entwicklungsfehlers, sind derzeit keine hinreichenden Gründe ersichtlich, warum in Bezug auf die von der Arbeitsgruppe untersuchten Produktbereiche die Entlastungsmöglichkeit nach § 1 Abs. 2 Nr. 5 ProdHaftG wegfallen sollte. Auch nach der bestehenden Regelung dürfte ein hinreichender Anreiz für die Hersteller bestehen, möglichst sichere Produkte auf den Markt zu bringen.

Genauso wie beim Fehlerbegriff spielen das öffentliche Sicherheitsrecht, technische Normen sowie behördliche Produktzulassungen auch bei der Definition der Entwicklungsrisiken eine Rolle.[173] Werden Sicherheitsstandards öffentlich-rechtlicher, technischer oder behördlicher Provenienz verletzt, scheidet die Klassifikation der daraus folgenden Schadensrisiken als Entwicklungsrisiken von vornherein aus. Umgekehrt lässt sich aus der Einhaltung dieser Standards nicht schließen, dass verbleibende Schadensszenarien automatisch als Entwicklungsrisiken zu qualifizieren sind; insbesondere schließt die Zertifizierung eines Produkts als konform mit dem EU-Recht (CE) oder mit technischen Normen (GS) es nicht aus, dass es vorhersehbare und mit zumutbaren Mitteln vermeidbare Schadenspotentiale in sich trägt, für die sich der Hersteller nicht nach § 1 Abs. 2 Nr. 5 ProdHaftG entlasten kann.[174]

Die Prüfung der Erkennbarkeit der Gefahr vollzieht sich in zwei Schritten:[175] Zunächst ist zu klären, ob der Fehler für irgendeinen Wissenschaftler oder Techniker dieser Welt erkennbar war. Ist dies zu verneinen, greift die Entlastung nach § 1 Abs. 2 Nr. 5 ProdHaftG durch. Wird hingegen „in wissenschaftlichen Kreisen auch nur eine einzige Stimme laut, mit der auf die potentielle Fehlerhaftigkeit des Produkts hingewiesen wird“,[176] ist die Erkennbarkeit zu bejahen, ohne dass deswegen die Entlastung schon scheitern muss. Vielmehr ist weiter zu prüfen, ob dieses Gefahrenwissen einem sorgfältigen Hersteller im Zeitpunkt des Inverkehrbringens objektiv zugänglich war. Dies setzt voraus, dass hinsichtlich des Gefahrenwissens ein Mindestmaß an Publizität gewährleistet ist. Neue wissenschaftliche Erkenntnisse, die von den beteiligten Forschern nicht veröffentlicht worden sind oder die von dem Unternehmen, dessen Forschungsabteilung sie zu verdanken sind, geheim gehalten werden, sind zwar vorhanden, einem sorgfältigen Hersteller jedoch nicht zugänglich. Zählt er hingegen selbst zu den eingeweihten Kreisen, ist sein Sonderwissen zu berücksichtigen. Auf die subjektiven Erkenntnismöglichkeiten des einzelnen Herstellers kommt es dagegen nicht an.[177]

---

[173] MüKo/*Wagner*, BGB, § 1 ProdHaftG Rn. 54.
[174] BGH, Urt. v. 5.2.2013 – VI ZR 1/12, NJW 2013, 1302 (1303).
[175] Im Folgenden dargestellt nach MüKo/*Wagner*, BGB, § 1 ProdHaftG Rn. 56.
[176] Generalanwalt Tesauro in EuGH Slg. 1997, I-2649, 2660 – Kommission/Vereinigtes Königreich.
[177] BGH, Urt. v. 16.6.2009 - VI ZR 107/08, NJW 2009, 2952 (2955).

e. Verletzung von Sicherungspflichten nach Inverkehrbringen des Produkts

Das ProdHaftG regelt ausschließlich die Haftung des Herstellers aufgrund des Inverkehrbringens eines (fehlerhaften) Produkts. Auch nach Inverkehrbringen eines Produkts wird der Hersteller nach der deliktischen Produzentenhaftung aber nicht vollständig von seiner Verantwortung frei. Nach gefestigter höchstrichterlicher Rechtsprechung[178] ist er vielmehr verpflichtet, auch nach diesem Zeitpunkt alles zu tun, was ihm nach den Umständen zumutbar ist, um Gefahren abzuwenden, die sein Produkt erzeugen kann. Er muss es auf noch nicht bekannte schädliche Eigenschaften hin beobachten und sich über seine sonstigen, eine Gefahrenlage schaffenden Verwendungsfolgen informieren (Produktbeobachtungspflicht). Hieraus können sich insbesondere Reaktionspflichten zur Warnung vor etwaigen Produktgefahren ergeben, wobei Inhalt und Umfang einer Warnung und auch ihr Zeitpunkt wesentlich durch das jeweils gefährdete Rechtsgut bestimmt werden und vor allem von der Größe der Gefahr abhängig sind. Erst recht treffen den Hersteller solche Pflichten, sobald er erkennt oder für möglich hält, dass sein Produkt einen ihm anzulastenden Konstruktionsfehler aufweist.

(1) Umfang der Sicherungspflichten

Die Sicherungspflichten des Herstellers nach Inverkehrbringen seines Produkts sind nicht notwendig auf die Warnung vor etwaigen Gefahren beschränkt. Sie können etwa dann weiter gehen, wenn Grund zu der Annahme besteht, dass die Warnung, selbst wenn sie hinreichend deutlich und detailliert erfolgt, den Benutzern des Produkts nicht ausreichend ermöglicht, die Gefahren einzuschätzen und ihr Verhalten darauf einzurichten. Ferner kommen weitergehende Sicherungspflichten dann in Betracht, wenn die Warnung zwar ausreichende Gefahrkenntnis bei den Benutzern eines Produkts herstellt, aber Grund zu der Annahme besteht, diese würden sich – auch bewusst – über die Warnung hinwegsetzen und dadurch Dritte gefährden. In solchen Fällen kann der Hersteller aufgrund seiner Sicherungspflichten aus § 823 Abs. 1 BGB verpflichtet sein, dafür Sorge zu tragen (ggf. durch Einschaltung der zuständigen Behörden), dass bereits ausgelieferte gefährliche Produkte möglichst effektiv aus dem Verkehr gezogen oder nicht mehr benutzt werden. Wie weit die Gefahrabwendungspflichten des Herstellers gehen, lässt sich nur unter Berücksichtigung aller Umstände des Einzelfalls entscheiden.

Nach Auffassung des BGH[179] würde aus deliktischer Sicht eine weitergehende Pflicht des Herstellers, bereits im Verkehr befindliche fehlerhafte Produkte nicht nur zurückzurufen (vgl. zur Definition des Rückrufs § 2 Nr. 25 ProdSG), son-

---

[178] Vgl. BGH, Urt. v. 16.12.2008 – VI ZR 170/07, BGHZ 179, 157-168 (Pflegebetten) m.w.N.
[179] Vgl. BGH, Urt. v. 16.12.2008 – VI ZR 170/07, BGHZ 179, 157, 161 (Pflegebetten).

dern das Sicherheitsrisiko durch Nachrüstung oder Reparatur auf seine Kosten zu beseitigen[180], jedenfalls voraussetzen, dass eine solche Maßnahme im konkreten Fall erforderlich ist, um Produktgefahren, die durch § 823 Abs. 1 BGB geschützten Rechtsgütern der Benutzer oder unbeteiligter Dritter drohen, effektiv abzuwehren. Dabei ist zu berücksichtigen, dass der deliktsrechtliche Schutz nicht deren Äquivalenzinteresse, sondern allein ihr Integritätsinteresse erfasst. Der BGH hat insoweit betont, dass der Hersteller aufgrund der deliktischen Produzentenhaftung und damit auch seiner etwaigen Pflichten zum Produktrückruf regelmäßig nur die von dem fehlerhaften Produkt ausgehenden Gefahren für die in § 823 Abs. 1 BGB genannten Rechtsgüter so effektiv wie möglich und zumutbar ausschalten muss, nicht aber dem Erwerber oder Nutzer ein fehlerfreies, in jeder Hinsicht gebrauchstaugliches Produkt zur Verfügung zu stellen und so sein Interesse an dessen ungestörter Nutzung und dessen Wert oder die darauf gerichtete Erwartung des Erwerbers (Nutzungs- und Äquivalenzinteresse) zu schützen hat. Der Schutz solcher Interessen muss vielmehr grundsätzlich, abgesehen etwa von Sonderfällen vorsätzlicher Schädigung i. S. v. § 826 BGB, der Vertragsordnung vorbehalten bleiben.

Diese Grundsätze erscheinen auch zur Bestimmung der Sicherungspflichten nach dem Inverkehrbringen von autonomen Systemen grundsätzlich sachgerecht. Hinsichtlich selbstständig operierender Systeme und ihrer Subkomponenten dürften sich bereits angesichts deren Komplexität ausgeprägte Produktbeobachtungspflichten der Hersteller ergeben; insbesondere die fortschreitende Vernetzung derartiger Produkte eröffnet dem Hersteller völlig neue Möglichkeiten der Produktbeobachtung.[181]

(2) Insbesondere: Pflichten bei Softwareupdates

Die den Hersteller nach den dargelegten Grundsätzen treffende Pflicht zur Beobachtung seiner Produkte und zur Reaktion auf erkannte Fehler ist insbesondere im Hinblick auf Softwareupdates durch den Hersteller von Relevanz. Gerade im Bereich komplexer IT-Systeme trifft den Hersteller im Wissen um die Gefahr von Programmierungsfehlern eine besonders sorgfältige Produktbeobachtungspflicht[182], deren Erstreckung auf die Verpflichtung zur Bereitstellung und ggf. Durchführung von Softwareupdates indes fraglich erscheint.

Ein Update der Betriebssoftware ist als Nachrüstung des Produkts zu verstehen. Mit dem Aufspielen der Updatesoftware wird der Benutzer eines Produkts nicht

---

[180] Vgl. dazu OLG Karlsruhe, Urt. v. 2.4.1993 – 15 U 293/91, NJW-RR 1995, 594, 597; OLG Düsseldorf, Urt. v. 31.5.1996 – 22 U 13/96, NJW-RR 1997, 1344, 1345.
[181] *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (80).
[182] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbststeuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 2015, 766 (769).

nur vor den erkannten Gefahren eines Produkts gewarnt; vielmehr wird – oftmals vom Softwarenutzer unerkannt – der dem Betriebssystem zugrunde liegende Algorithmus geändert.

Insoweit wird in der Literatur teilweise vertreten, dass ein effektiver und kostengünstiger Rechtsgüterschutz durch Softwareupdates vom Hersteller zu leisten sei.[183] Angesichts der gesteigerten Produktbeobachtungspflichten des Softwareherstellers sei dieser dazu verpflichtet, später entdeckte Fehler durch kostenfreie Patches oder Updates zu korrigieren.[184] Im Hinblick auf den Betrieb autonomer Systeme könne im Hinblick auf die geringen Kosten eines Softwareupdates zur Gefahrvermeidung demzufolge ein gesteigerter Maßstab an Nachrüstungspflichten angenommen werden.[185] Sogar eine Rückrufpflicht des Herstellers durch Softwareupdates sei zu bejahen.[186] Ein Hersteller sei demnach zur Bereitstellung von Softwareupdates verpflichtet, sofern nach erstmaliger Vermarktung eines Produkts unvorhergesehene Gefahren erkennbar oder neue Vermeidungstechnologien verfügbar werden, denen durch eine Anpassung der Steuerungsprogramme Rechnung getragen werden könne.[187] Dies solle auch eine kongruente Verpflichtung des Herstellers zur Verbesserung bereits im Verkehr befindlicher Produkte miteinschließen.[188] Statt eines Softwareupdates könne sich der Hersteller hingegen auf eine Warnung beschränken, sofern er die Weiterentwicklung seiner Produkte aufgegeben oder der Betreiber seine Zustimmung zu dem Aufspielen eines Softwareupdates verweigert habe.[189]

Unter Berücksichtigung der gefestigten höchstrichterlichen Rechtsprechung[190] zu Bestehen und Umfang der Nachrüstpflichten des Herstellers kann ein derart weitgehender, aus der Produkthaftung herrührender Anspruch auf Softwareupdates indes nicht generell bejaht werden.[191] Die Bejahung einer entsprechenden Nachrüstungspflicht würde grundsätzlich Äquivalenz- und Integritätsinteresse vermengen. Nach der Grundstruktur des Deliktsrechts ist der Hersteller lediglich zum Ausgleich der durch ein fehlerhaftes Produkt verursachten Schäden und zur Abwehr von Produktgefahren, jedoch nicht zur Bereitstellung mangelfreier Produkte verpflichtet. Dementsprechend käme eine Pflicht des Herstellers zu Softwareupdates dann in Betracht, wenn die Maßnahme im konkreten

---

[183] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (755, 756).
[184] *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (81).
[185] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (756).
[186] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (756).
[187] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (756).
[188] *Wagner*, Produkthaftung für autonome Systeme, AcP, 217, 707 (757).
[189] *Wagner*, Produkthaftung für autonome Systeme, AcP, 217, 707 (757)
[190] Vgl. BGH, Urt. v. 16.12.2008 – VI ZR 170/07, BGHZ 179, 157-168.
[191] Vgl. *Schrader/Engstler*, Anspruch auf Bereitstellung von Software-Updates?, MMR 2018, 356 (360).

Fall erforderlich ist, um Produktgefahren, die den in § 823 Abs. 1 BGB geschützten Rechtsgütern oder Dritten drohen, effektiv abzuwehren.

Kann eine bestehende Gefahr etwa durch Warnung, Rückruf oder durch Stilllegung gebannt werden, kann der Schutzfunktion des Deliktsrechts damit Genüge getan sein.[192] Dabei ist zu berücksichtigen, dass der Einsatz von gefahrgeneigten Produkten regelmäßig den eigenen Interessen des – vernünftigen – Betreibers zuwider laufen wird, da dieser nicht nur eigene Schäden vermeiden wollen wird, sondern auch rechtlich verpflichtet ist, die Sicherungsvorkehrungen stets an neue Erkenntnisse anzupassen[193], um Gefahren für andere vorzubeugen. Ob der Hersteller darauf vertrauen kann, dass Warnungen in Bezug auf sicherheitsrelevante Eigenschaften des Produkts auch Folge geleistet wird, ist nach den Umständen des Einzelfalls von der Rechtsprechung zu bewerten. Soweit die Bereitstellung eines Softwareupdates geeignet und deliktsrechtlich erforderlich ist, um Produktgefahren effektiv abzuwehren, ist es primär eine Frage des Vertragsrechts, ob diese kostenlos oder kostenpflichtig zur Verfügung gestellt werden müssen. Auch diese Frage kann der Rechtsprechung überlassen bleiben.

Eine allgemeine deliktsrechtliche Pflicht zur Bereitstellung von neuer, gegenüber dem Zeitpunkt des Inverkehrbringens des Produkts verbesserter Software würde dem Benutzer eine kostenlose Teilnahme am technischen Fortschritt ermöglichen und damit sogar ggf. das Äquivalenzinteresse des Benutzers, das sich in der Bereitstellung eines bei Gefahrübergang mangelfreien Produktes erschöpft, übersteigen. Die Kosten der Verbesserung der Sicherheitsstandards, die durchaus erheblich sein können, auch wenn die Übertragung der verbesserten Software dann letztlich kostengünstig ist, würden demgegenüber ausschließlich von den Neukunden getragen. Auch unter Berücksichtigung der berechtigten wirtschaftlichen Interessen der Beteiligten ist daher eine allgemeine deliktische Pflicht zur kostenlosen Bereitstellung von Softwareupdates abzulehnen. Die Frage, wie lange ein Kunde die Bereitstellung von Softwareupdates verlangen kann, ist in erster Linie dem Vertragsrecht zuzuordnen. Derzeit wird auf europäischer Ebene ein Vorschlag der EU-Kommission für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte[194] beraten. Dabei wird auch diskutiert, ob gesetzliche Vertragspflichten zur Bereitstellung von Softwareupdates eingeführt werden sollen.

---

[192] Vgl. *Spindler*, Roboter, Automation, künstliche Intelligenz, selbststeuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 2015, 766 (770); *Lüftenegger*, Die deliktische Pflicht zum Rückruf von Fahrzeugen, NJW 2018, 2087 (2091).

[193] Vgl. *Spindler*, Roboter, Automation, künstliche Intelligenz, selbststeuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 2015, 766 (771).

[194] COM (2016) 5656 final.

V. Ergebnis

Allein in der Herstellung und in dem Inverkehrbringen eines autonomen Systems liegt keine „besondere Gefahr“, die eine Gefährdungshaftung rechtfertigt. Auch der Umstand, dass sich Beweisschwierigkeiten ergeben können, genügt grundsätzlich nicht; allerdings können sie ggf. eine abweichende Ausgestaltung der Beweislastverteilung erforderlich machen, was nicht allgemein beurteilt werden kann, sondern nur produktbezogen zu beantworten ist.

Was die Haftung des Herstellers angeht, so greift der Haftungsgrund, welcher der Produkthaftung zugrunde liegt, ohne weiteres auch dann ein, wenn es um autonome Systeme geht. Allerdings ist zu prüfen, ob einzelne Regelungen des ProdHaftG auf den Einsatz autonomer Systeme abzustimmen sind. Etwaige Beweisschwierigkeiten, ob das Produkt fehlerhaft ist, rechtfertigen für sich genommen nicht die Einführung einer Gefährdungshaftung des Herstellers unabhängig vom Vorliegen eines Produktfehlers, sondern ggf. eine Beweislastumkehr. Eine Gefährdungshaftung des Herstellers ist vielmehr nur dann systemgerecht, wenn die Haftung an einen Produktfehler anknüpft.

Es besteht kein Bedürfnis für eine gesetzliche Regelung, mit der der Hersteller verpflichtet wird, im Rahmen der Produkthaftung Softwareupdates zur Verfügung zu stellen. Die damit zusammenhängenden Fragen können auf Basis des geltenden Rechts der Rechtsprechung überlassen bleiben.

Derzeit sind keine hinreichenden Gründe ersichtlich, warum in Bezug auf die von der Arbeitsgruppe untersuchten Produktbereiche die Entlastungsmöglichkeit nach § 1 Abs. 2 Nr. 5 ProdHaftG wegfallen sollte.

Im Rahmen der Prüfung, ob eine Gefährdungshaftung des Betreibers systemkonform ist, muss zunächst produktbezogen ermittelt werden, ob von der Sache eine „besondere Gefahr“ ausgeht. Das wird man auch bei autonomen Systemen nicht generell annehmen können. Auch wenn diese Frage zu bejahen ist, ist eine Gefährdungshaftung des Betreibers jedenfalls dann nicht geboten, wenn für das Produkt ein besonderes Zulassungsverfahren existiert, dem Geschädigten im Falle eines Produktfehlers hinreichende Ansprüche gegen den Hersteller zustehen und mit dem Produkt typischerweise nur Personen in Berührung kommen, die sich der Gefahr freiwillig ausgesetzt haben und über die Gefahren, die von dem Betrieb des autonomen Systems ausgehen, sachgerecht aufgeklärt wurden.

F. Autonomes Fahren

I. Einführung

Wird ein automatisiertes/autonomes Kraftfahrzeug im öffentlichen Straßenverkehr genutzt und kommt dabei jemand zu Schaden, stellt sich die Frage, wer für diesen Schaden haftet. Auf dem 53. Deutschen Verkehrsgerichtstag im Jahr 2015 wurde die Empfehlung abgegeben, dass der Fahrer bei hochautomatisiertem Fahrbetrieb und bestimmungsgemäßem Gebrauch von Sanktionen und Fahrerhaftung freizustellen sei.[195] Demgegenüber lautete eine der Empfehlungen des 56. Verkehrsgerichtstages im Jahr 2018, das geltende Haftungssystem beizubehalten.[196] Damit wird nicht zuletzt an dieser Entwicklung der Empfehlungen des Verkehrsgerichtstages exemplarisch aufgezeigt, welcher Diskussionsbedarf bei der Frage der Haftung beim automatisierten/autonomen Fahren derzeit besteht.

Ausgehend von den bislang geltenden Regelungen soll nachfolgend untersucht werden, ob und gegebenenfalls welcher Regelungsbedarf vorliegt, wenn automatisierte/autonome Kraftfahrzeuge für die Nutzung im öffentlichen Verkehr zugelassen werden. Die Haftung des Fahrers nach § 18 StVG bzw. des Halters nach § 7 StVG werden dabei unter den Gliederungspunkt Betreiber-/Benutzerhaftung (II.) zusammengefasst betrachtet. Die dargestellten Haftungstatbestände des Herstellers werden nachfolgend unter dem Gliederungspunkt Herstellerhaftung erörtert (III.).

Eine Projektgruppe der Bundesanstalt für Straßenwesen (BASt) hat die **Grade der Automatisierung** von Fahrzeugen wie folgt definiert[197]:

Grad	Fahraufgabe des Fahrers nach Automatisierungsgrad
Vollautomatisiert	Das System übernimmt Quer- und Längsführung vollständig in einem definierten Anwendungsfall - Der Fahrer muss das System dabei nicht überwachen. - Vor dem Verlassen des Anwendungsfalls fordert das System den Fahrer mit ausreichender Zeitreserve zur Übernahme der Fahraufgabe auf. - Erfolgt dies nicht, wird in den risikominimalen Systemzustand zurückgeführt. - Systemgrenzen werden alle vom System erkannt, das System ist in allen Situationen in der Lage, in den risikominimalen Systemzustand zurückzuführen.

[195] https://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_53_vgt.pdf.
[196] https://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_56_vgt.pdf.
[197] https://www.bast.de/BASt_2017/DE/Publikationen/Foko/2013-2012/2012-11.html.

Hochautomatisiert	Das System übernimmt Quer- und Längsführung für einen gewissen Zeitraum in spezifischen Situationen - Der Fahrer muss das System dabei nicht überwachen. - Bei Bedarf wird der Fahrer zur Übernahme der Fahraufgabe mit ausreichender Zeitreserve aufgefordert. - Systemgrenzen werden alle vom System erkannt. Das System ist nicht in der Lage, aus jeder Ausgangssituation den risikominimalen Zustand herbeizuführen.
Teilautomatisiert	Das System übernimmt Quer- und Längsführung (für einen gewissen Zeitraum oder/und in spezifischen Situationen) - Der Fahrer muss das System dauerhaft überwachen. - Der Fahrer muss jederzeit zur vollständigen Übernahme der Fahrzeugführung bereit sein.
Assistiert	Fahrer führt dauerhaft entweder die Quer- oder die Längsführung aus. Die jeweils andere Fahraufgabe wird in gewissen Grenzen vom System ausgeführt - Der Fahrer muss das System dauerhaft überwachen - Der Fahrer muss jederzeit zur vollständigen Übernahme der Fahrzeugführung bereit sein.
Driver only	Fahrer führt dauerhaft (während der gesamten Fahrt) die Längsführung (beschleunigen/verzögern) und die Querführung (lenken) aus.

Zur **Abgrenzung von automatisierten/autonomen Fahrzeugen** hat sich die Definition der Society of Automotive Engineers (SAE) durchgesetzt. Dieser internationale Standard unterteilt in folgende Stufen:[198]

- Stufe 0 - keine Automatisierung: Fahrer lenkt Fahrzeug selbst.
- Stufe 1 - „Assistiertes Fahren“: Fahren mit einzelnen Assistenzsystemen, das Fahrzeug übernimmt Längs- oder Querführung, der Mensch überwacht (zum Beispiel Einparkhilfe).
- Stufe 2 - „Teilautomatisiertes Fahren“: das Fahrzeug übernimmt Längs- und Querführung in einem spezifischen Anwendungsfall (Anwendungsfälle beinhalten Straßentypen, Geschwindigkeitsbereiche und Umfeldbedingungen), der Mensch muss gegebenenfalls selbstständig eingreifen (zum Beispiel Stauassistent).
- Stufe 3 - „Hochautomatisiertes Fahren“: System übernimmt Längs- und Querführung in einem spezifischen Anwendungsfall; das System erkennt, wenn der Mensch die Steuerung wieder übernehmen muss (Beispiel: automatisiertes Fahren auf Autobahnen).
- Stufe 4 - „Vollautomatisiertes Fahren“: System kann im spezifischen Anwendungsfall alle Situationen automatisch bewältigen.
- Stufe 5 - „volle Autonomie des Fahrens“: das Fahrzeug bewegt sich zielgerichtet, selbstständig ohne Einflussnahme eines Menschen von A nach B unter allen Bedingungen (im Folgenden: autonomes Fahren genannt).

---

[198] Vgl. die Wiedergabe auf der Seite des österreichischen Bundesministeriums für Verkehr, Innovation und Technologie:
https://www.bmvit.gv.at/verkehr/automatisiertesFahren/faq/hintergrundinfos.html. und
www.vda.de/de/services/Publikationen/automatisierung.html.

II. Betreiber-/Benutzerhaftung

1. Halterhaftung

a. Haftung nach § 7 Abs. 1 des Straßenverkehrsgesetzes (StVG)

Der Halter eines Kraftfahrzeugs haftet nach § 7 Abs. 1 StVG für Schäden, die beim Betrieb eines Kraftfahrzeugs entstehen. *Halter* ist, wer das Fahrzeug für eigene Rechnung gebraucht, also dessen Kosten bestreitet und die Verwendungsnutzungen zieht.[199] Der *Betrieb* des Fahrzeugs als Grund der Haftung wird weit gefasst: Der Schaden ist beim Betrieb entstanden, wenn sich die vom Fahrzeug ausgehenden Gefahren bei seiner Entstehung ausgewirkt haben, ohne dass in jedem Fall der Motor des Fahrzeugs in Betrieb gewesen sein oder sich eine der Betriebseinrichtungen bewegt haben muss.[200] Diese Gefährdungshaftung des Kraftfahrzeughalters gilt in gleicher Weise für nicht-automatisierte wie für hoch- oder vollautomatisierte Fahrzeuge (vgl. § 1a StVG).

Nicht ausdrücklich im StVG geregelt ist bislang der Betrieb eines autonomen Fahrzeugs. Wird ein autonomes Fahrzeug im Sinne der Stufe 5 nach der oben angeführten Definition der SAE zum Verkehr zugelassen werden, ist es aus Sicht des Geschädigten die einfachste Lösung, wenn der Fahrzeughalter weiterhin haftet. Der Geschädigte muss dann nämlich zum einen nicht aufklären, ob es sich bei dem Fahrzeug, bei dessen Betrieb er geschädigt wurde, um ein autonomes Fahrzeug oder nur um ein hoch- oder vollautomatisiertes Fahrzeug handelt, zum anderen muss er sich nicht die Frage stellen, ob er sich statt an den Fahrzeughalter an den Hersteller des Fahrzeugs wenden muss, um Schadensersatz zu erhalten. Soll der Halter beim autonomen Fahren haften, muss der Wortlaut des § 7 Abs. 1 StVG im Übrigen nicht geändert werden.

Die Kritik daran, dass es beim autonomen Fahrzeug bei der Halterhaftung bleiben soll, wird damit begründet, dass Verbraucher mit einem Haftungsrisiko belastet würden, obwohl die Hersteller für das Funktionieren des autonomen Fahrzeugs im Verkehr verantwortlich seien.[201] Diese Kritik könnte schon durch die tatsächliche Entwicklung abgeschwächt werden: Es wird angenommen, dass autonome Fahrzeuge erst einmal nicht von Verbrauchern gekauft, sondern nur zeitweilig angemietet werden können.[202] Halter des Fahrzeugs und damit derjenige, den die Halterhaftung nach § 7 StVG trifft, wäre das Unternehmen, das das Fahrzeug vermietet – etwa eine Tochter des Automobilherstellers –, nicht der

---

[199] Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 7 StVG, Rn. 14.
[200] Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 7 StVG, Rn. 4 ff.
[201] Vgl. hierzu auch die Kritik des Bundesrates, BT-Drs. 18/11534, S. 5 (Nr. 8)
[202] „Autonom nur bei Sonne“, Die Zeit vom 3. Januar 2019, S. 31.

Verbraucher.[203] Die Halterhaftung träfe – allein aus tatsächlichen Gründen – dann nicht den Verbraucher.

b. Ausschluss der Haftung

Die Schadensersatzpflicht des Halters ist gemäß § 7 Abs. 2 StVG ausgeschlossen, wenn der Unfall durch *höhere Gewalt* verursacht wird. Höhere Gewalt wird definiert als „außergewöhnliches, betriebsfremdes, von außen durch elementare Naturkräfte oder durch Handlungen dritter (betriebsfremder) Personen herbeigeführtes und nach menschlicher Einsicht und Erfahrung unvorhersehbares Ereignis, das mit wirtschaftlich erträglichen Mitteln auch durch nach den Umständen äußerste, vernünftigerweise zu erwartende Sorgfalt nicht verhütet werden kann und das auch nicht im Hinblick auf seine Häufigkeit in Kauf genommen zu werden braucht".[204]

Da ein Ereignis nur dann als höhere Gewalt angesehen wird, wenn es betriebsfremd ist, ergibt sich bereits heute keine rechtliche Besonderheit für hoch- oder vollautomatisierte Fahrzeuge im Vergleich zu nicht-automatisierten Fahrzeugen. Ein Versagen des Systems des hoch- oder vollautomatisierten Fahrzeugs ist nicht betriebsfremd und führt daher nicht zum Haftungsausschluss. Der Haftungsausschlusstatbestand des § 7 Abs. 2 StVG würde auch für den Betrieb autonomer Fahrzeuge passen: Dass der Halter z.B. für Schäden aufgrund reiner Naturereignisse haftet, ist auch für das autonome Fahrzeug nicht gerechtfertigt.

c. Sonderproblem: Hackerangriffe

(1) Höhere Gewalt?

Führt ein Hackerangriff zu einem Verkehrsunfall, könnte argumentiert werden, dass ein Eingriff eines betriebsfremden Dritten und damit nach der unter b. wiedergegebenen Definition ein Fall der „höheren Gewalt" gegeben ist. Es läge dann ein Haftungsausschlussgrund nach § 7 Abs. 2 StVG vor. Die Frage, ob der Haftungsausschlussgrund „höhere Gewalt" greift, könnte davon abhängen, welches Sicherheitsniveau das Auto zum Schutz gegen Hackerangriffe hat. Denn ab einem bestimmten höchsten Sicherheitsniveau könnte nach obiger Definition der Hackerangriff als höhere Gewalt anzusehen sein. Da mit der Gefahr von Hackerangriffen beim autonomen Fahren allerdings gerechnet wird[205] und ein sol-

---

[203] Vgl. *Freise*, Rechtsfragen des automatisierten Fahrens, VersR 2019, 65 (69) m.w.N.

[204] BGH, Urt. v. 16.10.2007 – VI ZR 173/06, NJW-RR 2008, 335; Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 7 StVG, Rn. 32.

[205] Vgl. den Bericht darüber, wie realistisch Hackerangriffe beim autonomen Fahrn sein werden: „Hacker am Steuer", Wirtschaftswoche vom 23.11.2018, S. 80.

cher – zu Demonstrationszwecken – im Jahr 2015 auch tatsächlich schon verübt und darüber berichtet wurde[206], wird nach Ansicht der Arbeitsgruppe nicht anzunehmen sein, dass es sich bei einem Hackerangriff um ein Ereignis handelt, das „nach menschlicher Einsicht und Erfahrung unvorhersehbar war".[207]

(2) Fall des § 7 Abs. 3 S. 1 StVG?

Liegt ein Fall wie der aus dem Jahr 2015 berichtete vor, bringt ein Hacker also das autonome Fahrzeug aus der Ferne unter seine Kontrolle und lenkt es per Laptop zum Unfall,[208] könnte darin ein Fall des § 7 Abs. 3 S. 1 StVG gesehen werden: Jemand benutzt das Fahrzeug ohne Wissen und Willen des Halters. Die Rechtsfolge wäre, dass der Hacker anstelle des Halters zum Ersatz des Schadens verpflichtet ist. Denn die Steuerung des Fahrzeugs durch den Hacker könnte in diesem Fall nicht anders zu bewerten sein als die heute unter § 7 Abs. 3 S. 1 StVG zu fassende Schwarzfahrt: In beiden Fällen wird das Fahrzeug ohne Wissen und Willen des Halters durch einen Fremden gesteuert. Dass der „Benutzer" in dem Fahrzeug sitzt, ist schon bisher für die Anwendung des § 7 Abs. 3 S. 1 StVG nicht erforderlich.[209] Entscheidend für die Haftung des Dritten nach § 7 Abs. 3 S. 1 HS 1 StVG ist, dass der Dritte die Verfügungsgewalt über das Fahrzeug ausübt, wie sie sonst dem Halter zusteht.[210]

Wenn der Halter die Benutzung des Fahrzeugs durch sein Verschulden ermöglicht hat, haftet er ebenfalls, § 7 Abs. 3 S. 1 HS 2 StVG. Ein solches Verschulden könnte etwa dann vorliegen, wenn der Halter vom Hersteller des Fahrzeugs zur Verfügung gestellte Updates nicht installiert hat, mit denen die Sicherheitslücke, die der Hacker ausgenutzt hat, hätte geschlossen werden können. Weiß der Halter allerdings nichts von den erforderlichen Sicherheitsupdates und musste auch nichts davon wissen, wird kein Verschulden vorliegen.

Führt der Hackerangriff nicht dazu, dass eine entsprechende Verfügungsgewalt über das Fahrzeug ausgeübt wird, bleibt es bei der Halterhaftung. Der Hacker haftet dann nicht anstelle des Halters nach § 7 Abs. 3 S. 1 HS 1 StVG.

---

[206] Siehe die Berichterstattung unter: https://www.adac.de/rund-ums-fahrzeug/autonomes-fahren/autonomes_fahren_hacker-angriff/.
[207] So auch *Freise*, Rechtsfragen des automatisierten Fahrens, VersR 2019, S. 65 (69).
[208] Vgl. die Schilderung unter https://www.adac.de/rund-ums-fahrzeug/autonomes-fahren/autonomes_fahren_hacker-angriff/.
[209] BGH, Urt. v. 24.1.1961, BB 1961, 310; Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 7 StVG, Rn. 52.
[210] BGH, Urt. v. 4.12.1956 – VI ZR 161/55, NJW 1957, 500.

(3) Ist der Hackerangriff versichert?

Sollte der Hacker nach Vorstehendem anstelle des Halters nach § 7 Abs. 3 S. 1 StVG haften, stellt sich die Frage, ob der Geschädigte einen Anspruch gegen die für den Gebrauch des Fahrzeugs abgeschlossene Kfz-Haftpflichtversicherung hat und damit – der Intention des PflVG entsprechend – „abgesichert" ist. Nach § 1 PflVG sind in der Kfz-Haftpflichtversicherung allerdings nur der Halter, der Eigentümer und der Fahrer eines Fahrzeugs versichert. Der Hacker ist kein Halter, er haftet nur wie der Halter. Ob der Hacker als Fahrer eines autonomen Fahrzeugs – das definitionsgemäß keinen Fahrer hat – angesehen werden kann, ist fraglich. Zum Vergleich: Beim nicht-autonomen Fahrzeug fällt der Schwarzfahrer, jedenfalls soweit er im Fahrzeug sitzt, unter den Begriff des Fahrers im Sinne des § 1 PflVG.[211]

Würde man den Hacker nicht als Fahrer ansehen, könnte der durch einen Hackerangriff geschädigte Dritte allerdings weder einen Anspruch gegen den Kfz-Haftpflichtversicherer, noch gegen den – bei vorsätzlicher Schädigung – einspringenden Entschädigungsfonds für Schäden aus Kraftfahrzeugunfällen nach § 12 Abs. 1 S. 1 Nr. 3 PflVG geltend machen.[212] Der Geschädigte bliebe im Fall der Unerreichbarkeit oder Zahlungsunfähigkeit des Hackers auf seinem Schaden sitzen. Nach Auffassung der Arbeitsgruppe muss sichergestellt sein, dass der Kfz-Haftpflichtversicherer auch im Fall von Hackerangriffen vom Geschädigten in Anspruch genommen werden kann bzw. im Fall der vorsätzlichen Schadensherbeiführung – wie nach der heutigen Rechtslage im Fall einer Schwarzfahrt – zumindest ein Anspruch gegen den Entschädigungsfonds für Schäden aus Kraftfahrzeugunfällen besteht.

d. Haftungsausschluss nach § 8 Nr. 2 StVG beim autonomen Fahren

Nach § 8 Nr. 2 StVG ist die Halterhaftung nach § 7 StVG ausgeschlossen, wenn der Verletzte bei dem Betrieb des Kfz tätig war. Diese Vorschrift ist als Ausnahmeregelung eng auszulegen.[213] Nach der vom BGH herangezogenen Definition erfasst § 8 Nr. 2 StVG Personen, „die durch die unmittelbare Beziehung ihrer Tätigkeit zum Betrieb des Kraftfahrzeugs den von ihm ausgehenden besonderen Gefahren stärker ausgesetzt sind als die Allgemeinheit, auch wenn sie nur aus Gefälligkeit beim Betrieb des Kraftfahrzeugs tätig geworden sind".[214]

---

[211] Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 18 StVG, Rn. 2.
[212] Bei vorsätzlicher Schadensherbeiführung greift der Haftungsausschluss nach § 103 VVG, vgl. OLG Nürnberg, Urt. v. 17.5.2011 – 3 U 188/11, NZV 2011, 538; zustimmend: *Maier*, jurisPR-VersR 2/2012 Anm. 5 mit Verweis auf OLG Oldenburg, Urt. v. 29.4.1998 – 2 U 264/97, VersR 1999, 482.
[213] BGH, Urt. v. 5.10.2010 – VI ZR 286/09, NZV 2010, 609 (611).
[214] BGH, Urt. v. 5.10.2010 – VI ZR 286/09, NZV 2010, 609 (611).

Dem liegt der Gedanke zugrunde, dass derjenige, der sich durch seine Tätigkeit freiwillig den besonderen Gefahren des Betriebs eines Fahrzeugs aussetzt, der erhöhte Schutz nicht zuteil werden soll.[215] Die Tätigkeit beim Betrieb eines Kfz setzt nach der Rechtsprechung eine gewisse Dauer voraus, wie sie beispielsweise der Fahrer im Verkehr ausübt.[216] Nicht beim Betrieb tätig wird, wer lediglich befördert wird.[217]

Die Arbeitsgruppe geht davon aus, dass beim autonomen Fahren der Ausschlussgrund des § 8 Nr. 2 StVG in der Regel nicht greifen kann. Es gibt – anders als beim hoch- oder vollautomatisierten Fahren – gerade keinen, der in der Lage sein muss, die Fahrzeugsteuerung unverzüglich zu übernehmen, vgl. § 1b Abs. 2 StVG. Zwar wird einer der Insassen das autonome Fahrzeug „einschalten", also in Betrieb nehmen. Der, der das Fahrzeug „einschaltet", setzt sich allerdings den vom Kraftfahrzeug ausgehenden Gefahren nicht stärker aus als die übrigen Insassen des Fahrzeugs. Anders könnte die Tätigkeit dessen zu bewerten sein, der z.B. einen „Nothalt-Knopf" des Fahrzeugs drückt und gerade dadurch den Schaden herbeiführt.

2. Fahrerhaftung

a. Haftung nach § 18 StVG

Nach § 18 StVG[218] haftet in den Fällen des § 7 Abs. 1 StVG neben dem Halter auch der Fahrzeugführer. Bis zur Automatisierungsstufe 4 nach den unter I. dargestellten Definitionen nach BASt und SAE gibt es einen Fahrer. In Stufe 4 nach beiden Definitionen hat der Fahrer zwar keine Überwachungsfunktion mehr, allerdings wird auch hier ein Fahrzeugführer noch gebraucht: Er hat bei Bedarf die Fahraufgabe vom Fahrzeug zu übernehmen. In Stufe 5 unterscheiden sich die Definitionen nach BASt und SAE: Während nach SAE in Stufe 5 kein Fahrer mehr benötigt wird und damit das autonome Fahren beschrieben wird, beschreibt die Definition des BASt in Stufe 5 nur das vollautomatisierte Fahrzeug, also das „autonome Fahren" beschränkt auf einen „definierten Anwendungsfall" (z.B. Autobahnfahrt). Wird das Fahrzeug außerhalb des definierten Anwendungsfalls betrieben, wird ein Fahrer benötigt.

---

[215] BGH, Urt. v. 9.12.1953 – VI ZR 121/52, NJW 1954, 392; Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 8 StVG, Rn. 3.
[216] BGH, Urt. v. 5.10.2010 – VI ZR 286/09, NZV 2010, 609 (611); BGH, Urt. v. 9.12.1953 – VI ZR 121/52, NJW 1954, 392.
[217] Hentschel/König/Dauer/*König*, Straßenverkehrsrecht, § 8 StVG, Rn. 4.
[218] Die Haftung des Fahrers nach § 823 Abs. 1 BGB soll im Folgenden nicht näher betrachtet werden, da sie neben § 18 StVG praktisch keine eigenständige Rolle spielt.

Das Problem, ob man in den verschiedenen Stufen der oben genannten Definitionen noch einen Fahrzeugführer und damit einen nach § 18 StVG Haftenden hat, auch wenn er die Fahrzeugsteuerung nicht mehr in jeder Situation selbst übernimmt, hat auch der Gesetzgeber erkannt. Er definiert in § 1a Abs. 4 StVG, wer beim „hoch- oder vollautomatisierten Fahren" Fahrzeugführer ist: Fahrzeugführer ist der, der eine hoch- oder vollautomatisierte *Fahrfunktion* aktiviert und zur Fahrzeugsteuerung verwendet, auch wenn er im Rahmen der bestimmungsgemäßen Verwendung *dieser Funktion* das Fahrzeug nicht eigenhändig steuert. Der Gesetzgeber ist durch diese Regelung Überlegungen entgegengetreten, wonach Fahrer bei Verwendung einer automatisierten Fahrfunktion der Fahrzeughersteller sein könnte.[219]

Der Gesetzgeber regelt allerdings gerade nicht das autonome Fahren, bei dem überhaupt kein Fahrer im herkömmlichen Sinn mehr benötigt wird.[220] Dies zeigt auch die Definition des hoch- oder vollautomatisierten Fahrens im StVG: Beim hoch- oder vollautomatisierten Fahren muss die Fahrzeugsteuerung durch den Fahrzeugführer bei Bedarf nach § 1a Abs. 2 StVG übernommen werden können und nach § 1b Abs. 2 StVG auch übernommen werden.

Geht man davon aus, dass künftig nicht nur hoch- und vollautomatisierte Fahrzeuge, sondern auch autonome Fahrzeuge zum Straßenverkehr zugelassen werden, wird es den Fahrer des Fahrzeugs im herkömmlichen Sinn als Haftungssubjekt nicht mehr geben. Die Fahrereigenschaft im Sinne des § 18 StVG wird man beim autonomen Fahren nicht allein in der Inbetriebnahme des Fahrzeugs sehen können, wenn derjenige, der das Fahrzeug in Betrieb nimmt und/oder als Fortbewegungsmittel benutzt, ansonsten keinen Einfluss mehr auf die Fahrfunktionen hat, vor allem keine Pflicht zur Übernahme der Fahrzeugsteuerung im Einzelfall mehr hat. Fahrer im Sinne des § 18 StVG wird aber auch nicht der Fahrzeughersteller sein.[221]

b. Ausschluss der Haftung nach § 18 StVG

Der Fahrer kann sich nach § 18 Abs. 1 S. 2 StVG entlasten, indem er nachweist, dass der Schaden nicht durch sein Verschulden verursacht wurde. Wenn der Fahrer bei der Benutzung einer hoch- oder vollautomatisierten Fahrfunktion in der konkreten Unfallsituation die Pflicht zur Übernahme der Fahrzeugsteuerung

---

[219] Vgl. *Meyer-Seitz*, Automatisiertes Fahren (Zivilrechtliche Fragen), 56. Deutscher Verkehrsgerichtstag 2018, S. 59; zu der Ansicht, dass der Hersteller der Fahrer sein könnte: *Bodungen/Hoffmann*, Autonomes Fahren – Haftungsverschiebung entlang der Supply Chain? (2. Teil), NZV 2016, 503.

[220] Vgl. Gesetzentwurf der Bundesregierung, BR-Drs. 69/17, S. 14.

[221] So aber *Bodungen/Hoffmann*, Autonomes Fahren – Haftungsverschiebung entlang der Supply Chain? (2. Teil), NZV 2016, 503.

nach § 1b Abs. 2 StVG beachtet hat, wird dem Fahrer dieser Entlastungsbeweis gelingen. Bei der nachträglichen Feststellung, ob er diese Pflicht beachtet hat, hilft die in § 63a StVG vorgeschriebene Datenaufzeichnung.

Beim autonomen Fahren kommt es auf den Haftungsausschluss nicht an, da es keinen Fahrer als Haftungssubjekt mehr gibt.

c. Kritik

Teilweise wird beklagt, dass dem Geschädigten ein Haftungssubjekt verloren geht, soweit der Fahrer beim hoch- und vollautomatisierten Fahren aus der Pflicht genommen wird. Diese Kritik muss erst Recht beim autonomen Fahren gelten, bei dem es keinen Fahrer mehr gibt.

Auf diese Kritik hat der Gesetzgeber – für die Fälle des hoch- und vollautomatisierten Fahrens – in der Weise reagiert, dass er als Ausgleich die für die Halterhaftung geltenden Haftungshöchstbeträge nach § 12 Abs. 1 S. 1 StVG bei der Nutzung einer hoch- oder vollautomatisierten Fahrfunktion gegenüber den bisher geltenden Höchstgrenzen verdoppelt hat.[222] Die Frage ist, ob diese Maßnahme auch die Kritik entkräftet, wenn der Fahrer beim autonomen Fahren als Haftungssubjekt ganz entfällt. Hier ist zu bedenken, dass mit der Herausnahme des Fahrers aus der Fahrzeugführung auch eine bedeutende Fehlerquelle ausscheidet: das menschliche Spontanversagen in der konkreten Fahrsituation.

d. Pflichtversicherung mit Direktanspruch

Der Schutz des Geschädigten bei einem automatisierten und künftig ggf. autonomen Fahrzeug wird vervollständigt durch die nach § 1 PflVG bestehende Pflicht des Halters eines Kraftfahrzeugs, für sich, den Eigentümer und den Fahrer eines Kraftfahrzeugs eine Haftpflichtversicherung zur Deckung der durch den Fahrzeuggebrauch verursachten Schäden abzuschließen. Nach § 115 Abs. 1 S. 1 Nr. 1 VVG hat der Geschädigte einen Direktanspruch gegen den Versicherer. Ist das Fahrzeug nicht versichert oder kann es nicht ermittelt werden, hat der Geschädigte Ansprüche gegen einen „Entschädigungsfonds für Schäden aus Kraftfahrzeugunfällen“ nach § 12 Abs. 1 PflVG.

Ersetzt der Versicherer den Schaden, geht auf ihn gem. § 86 VVG ein Anspruch des Fahrzeughalters auf Gesamtschuldnerausgleich gegen den Hersteller des Fahrzeugs über. Der Hersteller hat für den Schaden als Gesamtschuldner aufzukommen, falls die Voraussetzungen der Produkt- oder Produzentenhaftung vorliegen (dazu im Folgenden unter III.).

---

[222] Vgl. Gesetzentwurf der Bundesregierung, BR-Drs. 69/17, S. 8.

e. Zusammenfassung

Durch den Einsatz eines Fahrzeugs mit hoch- oder vollautomatisierter Fahrfunktion im Sinne des § 1a Abs. 2 StVG ändert sich an der Halterhaftung dem Grunde nach nichts. Selbst beim Einsatz – bisher im StVG nicht geregelter – autonomer Fahrzeuge greift die Halterhaftung nach dem Wortlaut des § 7 StVG ein.

Dem Fahrer wird es bei der Nutzung einer hoch- oder vollautomatisierten Fahrfunktion im Sinne des § 1a Abs. 2 StVG voraussichtlich häufig gelingen, sich durch ein fehlendes Verschulden von seiner Fahrerhaftung zu entlasten. Beim autonomen Fahren gibt es nach der Definition keinen Fahrer und damit auch keine Fahrerhaftung mehr. Der Wegfall der Fahrerhaftung wird beim hoch- und vollautomatisierten Fahren durch die Verdoppelung der Haftungshöchstbeträge nach § 12 Abs. 1 StVG kompensiert; diese Regelung muss konsequenterweise dann auch für das autonome Fahren für anwendbar erklärt werden.

Mit dem Direktanspruch gegen den Kfz-Haftpflichtversicherer ist heute sichergestellt, dass der Geschädigte stets einen solventen Schuldner hat; dieses System sollte auch für das autonome Kfz gelten, wenn dieses zugelassen wird; dieser Direktanspruch/Entschädigungsanspruch muss allerdings auch bei durch einen Hackerangriff verursachten Schäden bestehen.

III. Herstellerhaftung

Im Zusammenhang mit der Herstellung autonomer Systeme zum Einsatz in autonom bzw. automatisiert gelenkten Fahrzeugen sollen folgende bereits unter E. IV. allgemein dargestellten Voraussetzungen der den Hersteller treffenden Produkt- und Produzentenhaftung näher untersucht werden:

1. Produktbegriff

Wie bereits ausgeführt[223], sind Produkte nach der Regelung des § 2 ProdHaftG bewegliche Sachen, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bilden, sowie Elektrizität. Nach dem Wortlaut der Norm ist die sondergesetzliche Produkthaftung daher auf bewegliche Sachen beschränkt.[224] Die deliktischen Sorgfalts- bzw. Verkehrspflichten sind dagegen nicht auf die Herstellung beweglicher Sachen beschränkt, sondern erfassen jeg-

---

[223] Vgl. E. IV. 2. a.

[224] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (713).

liche Aktivität.[225] Nach den obigen Erwägungen unterfallen auch Softwareprodukte dem Anwendungsbereich des Produkthaftungsgesetzes.[226]

Im Bereich des autonomen/automatisierten Fahrens stellt sich damit insbesondere die Frage, ob die Einzelkomponenten des Automobils oder dieses in Gänze bei der Beurteilung der Produkteigenschaft im Sinne des § 2 ProdHaftG zu betrachten sind. In der Regel dürfte es sich bei einem autonomen/automatisierten Fahrzeug um ein sog. „embedded system", mithin ein Kombinationsprodukt aus Hard- und Software handeln.[227] Der Anwendungsbereich des § 2 ProdHaftG beschränkt sich dabei nicht auf die einzelnen Komponenten eines Produkts, sondern erfasst dieses in seiner Gesamtheit.[228] So führt auch die Europäische Kommission in ihrem „vorläufigen Konzept" zu zukünftigen Leitlinien zur ProdHaftRL an, dass autonome Fahrzeuge dem Produktbegriff unterfallen.[229]

Neben dem Fahrzeug als Gesamtprodukt findet die Regelung des § 2 ProdHaftG auch auf Software Anwendung, wenn diese nicht zusammen mit dem Fahrzeug in den Verkehr gebracht wurde. Neben den unter E. IV. 2. a. dargestellten Erwägungen wird dies vor allem mit der Vergleichbarkeit der im Zusammenhang mit dem Einsatz in Fahrzeugen wohl allein relevanten Standardsoftware[230] mit technischen Produkten begründet. So bestehen auch im Fall von Softwarevertrieb die Risiken arbeitsteiliger Güterproduktion fort. Der Geschädigte hat zudem auch im Fall des Vertriebs von Software keinen Zugang zu den internen Arbeitsprozessen des Herstellers und steht daher Beweisschwierigkeiten hinsichtlich des Nachweises der Verletzung von Sorgfaltspflichten gegenüber.[231] Unerheblich für die Anwendung des Produkthaftungsrechts ist hierbei schließlich, ob die Software auf konventionellem Wege oder über eine Cloud vertrieben wird. [232]

---

[225] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (714).
[226] Vgl. E. IV. 2. a.
[227] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (714).
[228] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (715).
[229] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 4.1.1. (11) [Stand: 18.9.2018].
[230] Dass nach verbreiteter Auffassung speziell für den Nutzer geschriebene und auf dessen Zwecke zugeschnittene Computerprogramme als Dienstleistung und nicht als Produkt im Sinne des Produkthaftungsgesetzes zu qualifizieren sind, worauf auch die Kommission in ihrem „vorläufigen Konzept" hinweist, dürfte dagegen für den Bereich des Softwareeinsatzes in Fahrzeugen keine Rolle spielen.
[231] Vgl. hierzu *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (717, 718).
[232] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (719).

2. Haftung von Endherstellern und Zulieferern

Der Erläuterung bedarf - über die obigen Ausführungen unter E. III. 3 hinaus -, wer als Haftungssubjekt eines Schadensersatzanspruchs in Betracht kommt. § 1 Abs. 1 ProdHaftG benennt den Hersteller eines Produkts als Anspruchsgegner. Der Begriff des Herstellers findet seine gesetzliche Definition wiederum in § 4 ProdHaftG. Demnach ist als Hersteller anzusehen, wer das Endprodukt, einen Grundstoff oder ein Teilprodukt hergestellt hat. § 4 Abs. 1 S. 2 ProdHaftG erweitert diesen Begriff um den "Quasi-Hersteller", sofern sich dieser durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt. § 4 Abs. 2 ProdHaftG erfasst schließlich auch denjenigen als Hersteller, der das Produkt mit wirtschaftlichem Zweck und im Rahmen seiner geschäftlichen Tätigkeit in den europäischen Wirtschaftsraum einführt.

Angesichts der arbeitsteiligen Fertigung von Fahrzeugen stellt sich auch im Bereich des autonomen/automatisierten Fahrens die Frage des Haftungssubjekts. Nach der Definition des § 4 ProdHaftG kommt als Haftungssubjekt jedenfalls der Endhersteller des autonomen Fahrzeugs in Betracht. Darüber hinaus stellt sich jedoch die Frage nach der Haftung von Zulieferern, gerade auch im Softwarebereich. Nach der Definition in § 4 Abs. 1 S. 1 ProdHaftG sind auch diese als Hersteller im Rahmen des ProdHaftG anzusehen. Dies allerdings nur insoweit, als der haftungsbegründende Fehler das vom Zulieferer hergestellte Teilprodukt betrifft; eine darüber hinausgehende Haftung des Zulieferers für das Endprodukt besteht nicht.[233] Maßgeblicher Zeitpunkt für die Beurteilung der Fehlerhaftigkeit des Produkts ist dabei nicht das Inverkehrbringen des Endprodukts in den Verkehr, sondern die Auslieferung des Zulieferteils an den Endhersteller.[234]

Die Haftung des Zulieferers wird ferner durch die gesetzliche Wertung des § 1 Abs. 3 ProdHaftG begrenzt. Demnach ist dessen Haftung ausgeschlossen, wenn der Fehler durch die Konstruktion des Endprodukts oder die Anleitungen des Endherstellers verursacht worden ist. Die Konstruktionsverantwortung für das Endprodukt liegt folglich in der Regel beim Endhersteller, nicht beim Zulieferer.[235] Mangels fehlender subjektiver Anhaltspunkte im ProdHaftG gilt dies auch für den Fall, dass der Zulieferer eines fehlerfreien Teilprodukts erkannt hat oder hätte erkennen müssen, dass die Verwendung des von ihm produzierten Teiles zu einer Fehlerhaftigkeit des Endprodukts führen wird.[236]

---

[233] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (720).
[234] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (720).
[235] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (721).
[236] *Wagne*r, Produkthaftung für autonome Systeme, AcP 217, 707 (721, 722).

Diese Lücke in der Produkthaftung wird durch die deliktische Produzentenhaftung nach §§ 823 ff. BGB geschlossen. Demnach ist auch ein Unternehmer, der auftragsgemäß nur die Fabrikation einzelner Produkte oder Produktteile für einen anderen Unternehmer übernimmt, für die Verkehrssicherheit dieser Produkte mitverantwortlich.[237] Zwar treffen auch insoweit die Konstruktionspflichten vor allem den Endhersteller; auch der Zulieferer muss jedoch auf den Produktionsbeitrag des anderen achten und bei Kenntnis der Gefährlichkeit der Konstruktion an der Gefahrenabwehr mitwirken.[238] Die Verantwortlichkeit des Endherstellers entlastet den Zulieferer nicht, so dass dieser nach deliktischen Maßstäben neben dem Endhersteller für die Fehler seines Zulieferteils haftet.[239]

Im Bereich des autonomen/automatisierten Fahrens ist aufgrund dieser Erwägungen mit einem Anstieg der gegen Zulieferer gerichteten Haftungsansprüche zu rechnen. Mit fortschreitender Automatisierung und Verselbstständigung der autonomen Fahrzeuge kommt mangels eigener Steuerung durch den Fahrer der dem Betrieb des Fahrzeugs zugrundeliegenden Software eine gesteigerte Funktion zu. Unfälle werden damit in der Regel auf ein Versagen der Steuerungssoftware und nicht mehr auf ein Versagen des Fahrers zurückgeführt werden können. Sofern diese Software nicht durch den Endhersteller des Fahrzeugs selbst, sondern durch einen Zulieferer bereitgestellt wurde, kann auch dieser Zulieferer im Wege der Produzentenhaftung in Anspruch genommen werden. Im Verhältnis der Haftung zwischen Endhersteller und Zulieferer ist daher im Bereich des autonomen/automatisierten Fahrens zu erwarten, dass der Haftung der Zulieferer künftig größeres Gewicht zukommt.

3. Fehlerbegriff

Hinsichtlich der Bestimmung der Fehlerhaftigkeit eines autonomen/automatisierten Fahrzeugs kann zunächst auf die allgemeinen Ausführungen zur Herstellerhaftung unter E. IV. 2. c. Bezug genommen werden.

Auch bei der Betrachtung des autonomen/automatisierten Fahrens scheint die Kategorisierung eines Fehlers des autonomen Fahrzeugs in Konstruktions-, Fabrikations- und Instruktionsfehler sachgerecht.[240]

---

[237] BGH, Urt. v. 9.1.1990 – VI ZR 103/89, NJW-RR 1990, 406.
[238] BGH, Urt. v. 9.1.1990 – VI ZR 103/89, NJW-RR 1990, 406.
[239] MüKo/*Wagner*, BGB, § 823, Rn. 790.
[240] Vgl. hierzu unter E. IV. 2. c.

a. Resistenz gegen Hackerangriffe

Bei der Betrachtung des autonomen Fahrens stellt sich dabei insbesondere im Hinblick auf die Sicherheit der verwendeten Software die Frage nach einem Konstruktionsfehler, sofern die Funktion der Software etwa durch Hackerangriffe beeinträchtigt werden kann. Nach den von der Ethikkommission des Bundesministeriums für Verkehr und digitale Infrastruktur aufgestellten ethischen Regelungen soll ein automatisiertes Fahren lediglich in dem Maße vertretbar sein, in dem denkbare Angriffe oder Systemschwächen nicht zu solchen Schäden führen, die das Vertrauen in den Straßenverkehr nachhaltig erschüttern.[241] Grundsätzlich stellt sich dabei die Frage, ob der erforderliche Sicherheitsstandard durch die Schaffung normativer technischer Standards (etwa im Zulassungsrecht) vorgegeben werden sollte; werden diese Standards nicht erfüllt, so ist das Produkt als fehlerhaft anzusehen und eine Haftung des Herstellers begründet. Sind sie erfüllt, kann der Hersteller davon ausgehen, seinen Sorgfaltspflichten genügt zu haben.

Auch wenn eine derartige Regelung Rechtssicherheit - insbesondere für die Hersteller - schaffen würde, würde sie jedoch nicht der schnelllebigen und äußerst dynamischen technischen Entwicklung Rechnung tragen. So kann ein statischer Standard in der Regel erst reaktiv zur Anwendung kommen, wenn eine Lücke in dem jeweiligen Sicherheitskonzept - gegebenenfalls nach einem erfolgten Hackerangriff - bereits erkannt wurde. Angesichts dessen, dass die IT-Sicherheitsentwicklung nicht langfristig vorausgesagt werden kann[242], scheint dies dem vom Kunden bzw. Verkehrsteilnehmer mit Recht erwarteten Sicherheitsstandard autonomer/automatisierter Fahrzeuge nicht zu genügen. Gerade im Bereich fortschreitender Innovationstechnologie erscheint es möglich, dass sich Risiken realisieren, die zuvor noch nicht normativ adressiert werden konnten.[243] Auch in diesem Sektor ist daher der bereits skizzierte Ansatz der BGH-Rechtsprechung sachgerecht: Normative Sicherheitsstandards, etwa im Zulassungsrecht, bieten als Mindeststandards wichtige Anhaltspunkte für die Bestimmung der Fehlerhaftigkeit bzw. Fehlerfreiheit des Produkts[244], können aber insoweit nicht abschließend sein. Maßgeblich ist vielmehr der Stand von Wissenschaft und Technik zum Zeitpunkt des Inverkehrbringens des Produkts. Der Hersteller eines Produkts muss dabei den Inbegriff der Sachkunde, die im wis-

---

[241] https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile; S. 12, Regel 14. Stand 6.9.2018.

[242] So Prof. Dr. Kargl in seiner Anhörung vom 18. Mai 2018.

[243] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 4.3. (38) [Stand: 18.9.2018].

[244] Zur Diskussion über die Bedeutung des neuen § 1a Abs. 2 S. 1 StVG für die Konstruktionsanforderungen an hoch- und vollautomatisierte Fahrzeugsteuerungssysteme vgl. von Bodungen/Hoffmann, NZV 2018, 97 ff.

senschaftlichen und technischen Bereich vorhanden und allgemein anerkannt ist sowie allgemein zur Verfügung steht, beachten.[245] Dabei hat der Hersteller auch Minder- und Außenseitermeinungen zu berücksichtigen, soweit diese verifizierbar und reproduzierbar sind.[246] Kommt der nicht-statische Standard des Stands der Wissenschaft und Technik statt eines normierten statisch-reaktiven Standards zur Anwendung, ist demnach zu erwarten, dass Hersteller zur Vermeidung potentieller Haftungsrisiken wissenschaftliche und technische Erkenntnisse sorgfältiger auswerten und damit zur Vermeidung bislang unbekannter Sicherheitsschwachstellen beitragen. Eine von der Arbeitsgruppe angehörte Expertin hat hierzu ausgeführt, dass ein sog. Auto-ISAC-Meldesystem (automotive information sharing and analysis center) für Schwachstellen der „Security" des Fahrzeugs – also der Sicherheit des Systems vor Angriffen von außen – in der Diskussion sei.

Angesichts der dynamischen technischen Entwicklung, die fortlaufend zu einer Verbesserung der in den Verkehr gebrachten Produkte führt, ist bei der Bestimmung der deliktsrechtlich relevanten Sicherheitsstandards, die vom Hersteller bei Inverkehrbringen des Produktes berechtigterweise erwartet werden konnten, indes Zurückhaltung geboten. Insbesondere wird den deliktischen Sorgfaltspflichten bereits dann Genüge getan, wenn ein vernünftiges Maß an Sicherheit gefunden wird; die Gewährung absoluter Sicherheit ist demgegenüber nicht erforderlich.[247] Damit geht einher, dass bei der Beurteilung einer vom Hersteller einzuhaltenden Sorgfaltspflicht retrospektiv lediglich der Zeitpunkt des Inverkehrbringens von Relevanz ist.[248] Andernfalls würden den Herstellern nicht erfüllbare Sorgfaltsanforderungen auferlegt und die fortschreitende technische Entwicklung zu einer Ausweitung der deliktischen Haftung führen. Einen Anhaltspunkt bei der Bestimmung der Herstellerpflichten bietet dabei auch das Produktsicherheitsgesetz (ProdSG), das gemäß § 1 Abs. 1 ProdSG bei der Bereitstellung, Ausstellung oder erstmaligen Verwendung von Produkten auf dem Markt im Rahmen einer Geschäftstätigkeit Anwendung findet. So darf nach § 3 Abs. 2 ProdSG ein Produkt nur dann auf den Markt gebracht werden, wenn bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und Gesundheit von Personen nicht gefährdet wird. Einen normativ-reaktiven Standard zur Bestimmung der einzuhaltenden Sicherheitsstandards sieht dabei das ProdSG nicht vor, sondern stellt in § 3 Abs. 2 S. 2 ProdSG lediglich einen nicht abschließenden Katalog abstrakter Kriterien zu deren Bestimmung auf. Auch im Anwendungsbereich des ProdSG ist der maßgebende Zeitpunkt zur Bestimmung

---

[245] BeckOGK/*Seibl*, ProdHaftG, § 1 Rn. 123.
[246] BeckOGK/*Seibl*, ProdHaftG, § 1 Rn. 124.
[247] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (731).
[248] *Wagner* Produkthaftung für autonome Systeme, AcP 217, 707 (731).

der Herstellerpflichten das Bereitstellen des Produkts auf dem Markt, § 2 Abs. 2 S. 3 ProdSG.[249]

b. Vergleich von anthropozentrischen und systembezogenem Lösungsansatz

Zur Ermittlung des erforderlichen Mindestmaßes an Sicherheit wird mitunter vorgeschlagen, auch im Bereich des autonomen/automatisierten Fahrens das hypothetische Verhalten eines sorgfältigen Menschen als Vergleichsmaßstab etwaiger Sorgfaltspflichten heranzuziehen.[250] Ein Produktfehler bestünde demnach dann, wenn ein autonomes Fahrzeug in einer Verkehrssituation nicht derart reagiert, wie dies von einem sorgfältigen menschlichen Fahrer zu erwarten gewesen wäre.

Dieser „anthropozentrische" Sorgfaltsmaßstab wird jedoch von anderen für die Bestimmung der Sorgfaltspflichten des autonomen Fahrens für ungeeignet gehalten. Es wird darauf hingewiesen[251], dass ein potentiell haftungsbegründendes Handeln des Herstellers eines autonomen Fahrzeugs nicht in dem Verhalten des autonomen Fahrzeugs in der jeweiligen Verkehrssituation gesehen werden könne; vielmehr liege dem Fahrverhalten des Fahrzeugs die Programmierung des Steuerungsalgorithmus zugrunde, der ein systemisches Handeln des autonomen Fahrzeugs in jeder denkbaren Verkehrssituation vorgibt. Der Vergleich mit einem sorgfältig handelnden Menschen in der konkreten Verkehrssituation gehe daher fehl. Zwar sei die einem Hersteller obliegende Sorgfaltspflicht jedenfalls dann verletzt, wenn das autonome Fahrzeug bereits nicht den Grad menschlicher Sorgfalt einhalten kann, sondern hinter diesem zurückbleibt. Dabei dürfe jedoch keine isolierte Betrachtung des Verhaltens eines in einen Unfall verwickelten Fahrzeugs erfolgen, da die Feststellung eines Fehlers das in der Fahrzeugflotte eingesetzte technische System als solches sowie dessen Programmierung betreffe.[252] Der Beurteilung deliktischer Sorgfaltspflichten könne aufgrund der technischen Gegebenheiten deshalb in sachgerechter Weise nicht ein individueller Vergleich mit dem Verhalten eines sorgfältigen menschlichen Fahrers in einer einzelnen Verkehrssituation, sondern lediglich eine generalisierende Betrachtung der Programmierung des Steuerungsalgorithmus zugrunde gelegt werden.[253]

---

[249] ProdSG/*Klindt*, ProdSG, § 3 Rn. 39.
[250] *Borges*, Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272 (275 f.); Gomille, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (77).
[251] Vgl. *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (733f.).
[252] Vgl. *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (734).
[253] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (734).

Alternativ zu einem individualisierenden anthropozentischen Sorgfaltsmaßstab wird daher eine systembezogene Betrachtung vorgeschlagen, die dem systemischen Charakter autonomer Fahrzeuge sowie der mangelnden Vergleichbarkeit menschlichen und autonomen Fahrens in einer konkreten Verkehrssituation gerecht werden soll. Nach dem systembezogenen Ansatz ist demnach entscheidend, ob das vom Hersteller programmierte System Unfälle verursacht, die ein "sorgfaltsgemäßer Algorithmus" verhindert hätte.[254] So könnte ein Konstruktionsfehler etwa durch einen Vergleich des beanstandeten Algorithmus mit einem anderen, diesbezüglich fehlerfreien Algorithmus festgestellt werden.[255]

Auch einer systembezogenen Betrachtung etwaiger Konstruktionsfehler seien indes Grenzen gesetzt. Lege man das Kriterium eines "sorgfältigen" Algorithmus zugrunde, käme dem Hersteller mit dem besten Algorithmus selbstlernender, autonomer Fahrzeuge eine faktische Haftungsimmunität zu, während die übrigen Hersteller, die den vom Marktführer gesetzten Algorithmusstandard nicht erreichen, in vollem Umfang die Haftungskosten autonomen Fahrens zu tragen hätten.[256] Um eine solche Teilung des Marktes zu vermeiden, wird vorgeschlagen, die Instruktionspflichten bei der Vermarktung autonomer Fahrzeuge zu erweitern, statt einen weniger sicheren Algorithmus unter die Kategorie des Konstruktionsfehlers zu fassen.

Bei der Bewertung dieser konträren Lösungsansätze ist vom Fehlerbegriff des § 3 ProdHaftG, also den berechtigten Sicherheitserwartungen an das Produkt, auszugehen. Dabei bietet zunächst § 30 Abs. 1 StVZO einen zulassungsrechtlichen normativen Anhaltspunkt. Demnach müssen Fahrzeuge so gebaut und ausgerüstet werden, dass ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet, behindert oder belästigt (Nr. 1) sowie, dass die Insassen des Fahrzeugs insbesondere bei Unfällen vor Verletzungen möglichst geschützt sind und das Ausmaß und die Folgen von Verletzungen möglichst gering bleiben (Nr. 2). Der Gesetzgeber regelt in § 30 StVZO mithin berechtigte Sicherheitserwartungen an die von Fahrzeugen jeder Art zu gewährleistende Verkehrssicherheit.[257] Bauart und Ausrüstung eines Fahrzeugs müssen demnach dem verkehrsüblichen Betrieb entsprechen, was anhand der Umstände des Einzelfalls zu beurteilen ist.[258] Die §§ 32 - 62 StVZO bzw. auch die auf Grundlage von Richtlinie 2007/45/EG anzuwendenden UN/ECE-Regelungen sehen zudem rechtlich normierte technische Mindeststandards vor, die folglich

---

[254] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (736).
[255] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (736).
[256] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (737).
[257] Haus/Krumm/Quarch/*Gutt*, Gesamtes Verkehrsrecht, StVZO, § 30 Rn. 1.
[258] Haus/Krumm/Quarch/*Gutt*, Gesamtes Verkehrsrecht, StVZO, § 30 Rn. 2.

auch von autonomen Fahrzeugen zu erfüllen sind, sodass autonomen/automatisierten Fahrzeugen aus technischer Sicht kein Sonderstatus zukommt.

Auch im Bereich des Betriebs autonomer Fahrzeuge besteht eine gesetzlich intendierte Erwartungshaltung dahingehend, dass die Fahrleistung autonomer Systeme in einer konkret zu betrachtenden Verkehrssituation nicht hinter den Anforderungen an einen sorgfältigen menschlichen Autofahrer zurücksteht. § 1 Abs. 2 StVO normiert insoweit, dass ein Verkehrsteilnehmer sich so zu verhalten hat, dass kein anderer geschädigt, gefährdet oder mehr, als nach den Umständen unvermeidbar, behindert oder belästigt wird. § 1a Abs. 2 S. 1 StVG greift diese Vorschrift auf und ermöglicht eine Anwendung auch auf automatisiert gelenkte Fahrzeuge. Demnach sind Kraftfahrzeuge mit vollautomatisierter Fahrfunktion nämlich solche, die - neben weiteren Anforderungen - in der Lage sind, während der vollautomatischen Fahrzeugsteuerung den an die Fahrzeugführung gerichteten Verkehrsvorschriften zu entsprechen. Weiterhin ergibt sich nach den obigen Ausführungen bereits aus haftungsrechtlichen Erwägungen, dass der Betriebsalgorithmus der Fahrzeuge dem jeweiligen Stand der Technik zu entsprechen hat.[259] Das im Rahmen des systembezogenen Ansatzes angeführte „Argument des Herstellers mit dem besten Algorithmus" kann daher ebenfalls nicht überzeugen. Denn die Anforderung an einen Hersteller innovativer Technik, sein Produkt stets dem Stand der Technik anzupassen, stellt sich bereits als logischer Rückschluss aus dem Produkthaftungsrecht dar.

Unter Beachtung dieser Erwägungen erscheint eine sachgerechte Bestimmung des Fehlerbegriffs auch im Hinblick auf autonome/automatisierte Steuerungssysteme in Fahrzeugen anhand der Definition des Produktfehlers in § 3 ProdHaftG durch eine Kombination aus anthropozentrischen und systembezogenen Lösungsansatz möglich. So muss der in einem autonomen System verwendete Steuerungsalgorithmus den Anforderungen an eine sorgfältige, dem Stand der Technik entsprechende Programmierung gerecht werden. Ebenso dürfte es regelmäßig den berechtigten Sicherheitserwartungen entsprechen, dass der Algorithmus auch in einer konkreten Verkehrssituation nicht hinter den Sorgfaltsanforderungen zurücksteht, die an einen sorgfältigen menschlichen Fahrer gestellt werden können, soweit er bestimmungsgemäß den menschlichen Fahrer ersetzen soll. Die Beurteilung der berechtigten Sicherheitserwartungen im Einzelfall kann der Rechtsprechung überlassen bleiben.

---

[259] Vgl. E. IV. 2. c. (1)

c. Dilemmasituationen

Die schrittweise Einführung autonomen Fahrens wirft schließlich vermehrt die Frage nach einer ethischen Programmierung des Steuerungsalgorithmus des autonomen Fahrzeugs auf. Unter der Prämisse, dass sich Unfälle mitunter nicht gänzlich vermeiden lassen, gilt die Frage hierbei zum Beispiel dem Verhältnis der Rechtsgüter von Fahrzeuginsassen gegenüber fremden Rechtsgütern.[260] Problematisch wird dies insbesondere, sofern einer der Beteiligten Rechtsgüter aufopfern muss.

Für den Themenbereich des autonomen Fahrens hat das Bundesministerium für Verkehr und digitale Infrastruktur zur Erarbeitung konsensfähiger Leitlinien für die Programmierung autonomer Fahrzeuge eine Ethikkommission eingesetzt. Diese hat im Juni 2017 ihren Bericht vorgelegt und darin ethische Regeln für den automatisierten und vernetzten Fahrzeugverkehr aufgestellt.[261] Demnach ist die Technik des autonomen Fahrens derart zu konzipieren, dass Dilemma-Situationen, in denen das Fahrzeug zwischen der Schädigung gleicher Rechtsgüter entscheiden muss, vermieden werden.[262] Sofern eine solche Situation indes nicht zu vermeiden ist, ist der Schutz menschlicher Rechtsgüter als prioritär anzusehen; die Programmierung soll Tier- und Sachschäden vorrangig in Kauf nehmen.[263] Die Abwägung Leben gegen Leben sei hingegen nicht programmierbar, da die technische Programmierung des autonomen Fahrzeugs nicht die Entscheidung des Fahrzeugführers ersetzen könne.[264] Im Falle einer unausweichlichen Unfallsituation ist eine Qualifizierung nach persönlichen Merkmalen ebenso wie eine Aufrechnung von Opfern untersagt. Die an der Erzeugung von Mobilitätsrisiken Beteiligten dürfen Unbeteiligte nicht opfern. Jedoch kann eine Programmierung auf eine Minderung der Zahl von Personenschäden vertretbar sein.[265] Durch die Automatisierung des Fahrens werde die Verantwortung vom Autofahrer auf die jeweiligen Hersteller verschoben.[266] Bei der diesbezüglichen Haftung sollen dann die Grundsätze der Produkthaftung Anwendung finden.[267]

Im Rückschluss könnte sich bei Beachtung der vorstehenden ethischen Regeln daher für den Fehlerbegriff ergeben, dass die Programmierung eines Algorith-

---

[260] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (740).
[261] https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile; Stand 6.9.2018
[262] Ethikkommission, a.a.O., Seite 10, Regel 5; vgl. zur Abwägung Leben gegen Leben BVerfG, Urt. v. 15.2.2006 – 1 BvR 357/05, BVerfGE 115, 118 (152 ff.).
[263] Ethikkommission, a.a.O., Seite 11, Regel 7.
[264] Ethikkommission, a.a.O., Seite 11, Regel 8.
[265] Ethikkommission, a.a.O., Seite 11, Regel 9.
[266] Ethikkommission, a.a.O., Seite 11, Regel 10.
[267] Ethikkommission, a.a.O., Seite 12, Regel 11.

mus dann als fehlerhaft und haftungsbegründend angesehen werden muss, wenn diese der Erhaltung menschlicher Rechtsgüter - unter Berücksichtigung des jeweiligen Gefährdungsgrads - keinen Vorrang gegenüber Tier- oder Sachschäden einräumt. Ebenso könnte die Programmierung der Steuerungssoftware als fehlerhaft angesehen werden, wenn diese bei der Abwägung „Leben gegen Leben" nach deren individuellen Merkmalen entscheidet. Schließlich würde auch ein Algorithmus, der gezielt Rechtsgüter von Unbeteiligten zugunsten der Fahrzeuginsassen opfert, zu einem Produktfehler führen.[268]

In diesem Zusammenhang wird jedoch darauf verwiesen, dass auch die Ethikkommission in ihren Überlegungen keinen Konsens herstellen konnte.[269] In Dilemmasituationen müsse - neben den vorstehenden Erwägungen - insbesondere auch die Herstellerperspektive betrachtet werden. Im Gegensatz zu den ethischen und rechtlichen Fragestellungen, die im sog. Weichenstellerfall diskutiert werden, beherrscht der Hersteller eines autonomen Fahrzeugs nämlich nicht den Kausalverlauf des konkreten Unfallgeschehens, sondern muss bereits in dessen Vorfeld den Steuerungsalgorithmus nach allgemeinen Merkmalen programmieren.[270] Die Programmierung der Steuerung des autonomen/automatisierten Fahrzeugs betreffe ferner nicht ein einzelnes Fahrzeug, sondern die gesamte Fahrzeugflotte des Herstellers, die mit diesem Steuerungsalgorithmus ausgestattet ist.[271] Dementsprechend kann die Software nicht jedes einzelne Unfallgeschehen erfassen, sondern muss eine Unfallsituation anhand abstrakter Regeln bewältigen. Deshalb wird vorgeschlagen, die Software stets so zu programmieren, dass das Risiko des Verlusts von Menschenleben minimiert wird; da sich ein Hersteller andernfalls dem Vorwurf ausgesetzt sähe, dass eine alternative Softwareprogrammierung Todesfälle hätte vermeiden können.[272] Auch hier soll jedoch Persönlichkeitsgütern ein Vorrang vor Eigentumsinteressen eingeräumt werden.[273] Dennoch müsse eine Abwägungsentscheidung unter Beachtung des Grundsatzes der Verhältnismäßigkeit sowie des Rangs und des Grads der Gefährdung der konkreten Rechtsgüter möglich sein; eine Differenzierung mehrerer Menschenleben nach Kriterien wie Alter, Krankheit, etc. solle jedoch nicht erfolgen, da andernfalls die Lebenschancen der nach dieser Differenzierung benachteiligten Personengruppen strukturell beeinträchtigt würden.[274] Im Hinblick auf die Abwägung der Rechtsgüter der Insassen des Fahrzeugs mit den Rechtsgütern unbe-

---

[268] Zu der Problematik eines Wettrüstens: *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (746).
[269] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (741).
[270] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (742).
[271] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (743).
[272] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (743, 744).
[273] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (745).
[274] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (745).

teiligter Dritter solle eine Programmierung nicht systematisch auf den Schutz der Insassen ausgerichtet sein, da dies wiederum der Programmierung zur Minimierung des Risikos des Verlusts von Leben entgegenstünde.[275]

Eine von der Arbeitsgruppe angehörte Expertin hat hierzu ausgeführt, dass der technische Fortschritt eine selbstständige Entscheidung eines autonomen Fahrzeugs bislang ohnehin nicht zulasse und dieses somit nur im Rahmen der Steuerungsprogrammierung reagieren könne. Eine Differenzierung nach dem Alter eines Menschen oder der Anzahl von Personen in einem anderen Fahrzeug sei dem autonomen System aus technischen Gründen bislang ebenfalls nicht möglich. Eine überraschende Situation, die von der Steuerungsprogrammierung nicht vorgesehen ist, könne das Fahrzeug daher zum jetzigen Zeitpunkt nicht bewältigen. Die Expertin schlug zur Entlastung der Hersteller jedoch vor, den Rechtsgedanken des § 34 StGB auch bei automatisierten Fahrzeugen anzuwenden. Dabei wären aber die von der Rechtsprechung zu § 34 StGB aufgestellten Grundsätze zu beachten, wonach eine Abwägung Leben gegen Leben gerade nicht stattfinden kann.[276]

Der fachliche Diskurs zur Bewältigung von Dilemmasituationen durch autonome Fahrzeug erscheint nach dem derzeitigen Stand noch nicht abgeschlossen.[277] Insbesondere der Fehlerbegriff des § 3 ProdHaftG ist bei der Betrachtung der Reaktion der Steuerungsprogrammierung in Unfallsituationen mit erheblichen Unsicherheiten behaftet. Denn die Bestimmung der Anforderungen, die berechtigterweise an die Ausgestaltung der Steuerungssoftware des autonomen Fahrzeugs zu stellen sind, kann in Dilemmasituationen nicht allein nach dem Stand von Wissenschaft und Technik erfolgen; vielmehr sind hier auch ethische Wertungen entscheidend. Gleichwohl ist angesichts des derzeitigen technischen Entwicklungsstandes, der eine Unterscheidung verschiedener Rechtsgüter und Personengruppen durch ein autonomes Fahrzeug ohnehin nicht zulässt, ein zeitnahes gesetzgeberisches Handeln noch nicht erforderlich. Die Möglichkeit der Schaffung von mehr Rechtssicherheit für die Hersteller sollte jedoch - möglichst auf europäischer Ebene - weiter geprüft und verfolgt werden.

d. Beweislast

Sowohl im Bereich der deliktischen Produkthaftung als auch im Anwendungsbereich des Produkthaftungsgesetzes trifft die Beweislast für einen Fehler den

---

[275] *Wagner,* Produkthaftung für autonome Systeme, AcP 217, 707 (745, 746).
[276] Vgl. BGH, Urt. v. 15.9.1988 - 4 StR 352/88 m.w.N.
[277] Weitere Nachweise zum Diskussionsstand bei *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (744 ff.).

Geschädigten.[278] Zum Nachweis eines Fehlers des Steuerungsalgorithmus müsste dieser folglich darlegen und beweisen, dass der Algorithmus des Herstellers, zu dessen Quellcode er keinen Zugang hat, nicht den oben dargestellten Anforderungen genügt.[279] Vor diesem Hintergrund stellt sich bei der Betrachtung der Beweislastverteilung die Frage, ob dem Geschädigten diese Beweisführung gelingen kann oder er sich - angesichts der Komplexität der Materie - unüberwindbaren Beweisschwierigkeit ausgesetzt sieht. Es sollte überlegt werden, ob eine Zulassung autonomer Fahrzeuge nur dann erfolgen sollte, wenn das Fahrzeug über eine Blackbox verfügt.[280]

(1) Vermutung aufgrund Unfallbeteiligung

Eine Abmilderung dieser den Geschädigten treffenden Beweisschwierigkeiten könnte etwa durch die Schaffung einer Vermutungsregelung erreicht werden, wonach die Fehlerhaftigkeit eines autonomen Fahrzeugs auf die Beteiligung an einem Unfall zurückgeführt werden kann. Die Europäische Kommission stellt in ihrem „vorläufigen Konzept“ zu zukünftigen Leitlinien zur Produkthaftungsrichtlinie insoweit klar, dass die Richtlinie der Schaffung von Vermutungsregelungen zwischen Fehlerhaftigkeit des Produkts und eingetretenem Schaden nicht entgegensteht; eine solche Vermutungsregelung dürfe jedoch nicht zu einer Beweislastumkehr führen.[281] Im Falle einer solchen Vermutung müsste der Geschädigte somit nicht mehr die Fehlerhaftigkeit des autonomen Systems, sondern lediglich die Vermutungsbasis, d.h. die Beteiligung an einem Unfall, beweisen. Für die Schaffung einer solchen Vermutungsregel spräche nach den obigen Erwägungen, dass ein Steuerungsalgorithmus mindestens dem Sorgfaltsmaßstab eines vernünftigen menschlichen Fahrers sowie eines dem Stand der Technik und Wissenschaft entsprechenden Algorithmus zu genügen hat, was bei einer Unfallbeteiligung unterschritten sein könnte. Gegen die Schaffung einer Vermutungsregelung spricht jedoch, dass aus dem Geschehen eines Unfalls in der Regel kein Rückschluss auf dessen Verursachung gezogen werden kann. Anstelle der Annahme eines unfallverursachenden Produktfehlers erscheint es dabei ebenso denkbar, dass das autonome Fahrzeug durch das Fehlverhalten anderer Verkehrsteilnehmer in eine Situation gebracht wurde, die weder von einem sorgfältigen menschlichen Fahrer noch von einem sorgfältig programmierten Algorithmus unfallfrei hätte gelöst werden können. Vor dem Hintergrund der Prämisse, dass von autonomen Fahrzeugen gegenüber einem sorgfältigen

---

[278] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (746); *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (78).
[279] Vgl. *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (78).
[280] Vgl. die Entschließung des Europäischen Parlaments mit Empfehlungen an die Kommission zu zivilrechtlichne Regelungen im Bereich Robotik, Ziffer 12 der Entschließung.
[281] Preliminary concept paper for the future guidance on the Product Liability Directive 85/374/EEC, 5. (50) [Stand: 18.9.2018].

menschlichen Fahrer jedoch gerade eine Verbesserung der Verkehrssicherheit zu erwarten ist und der Gesetzgeber auch für die Beteiligung eines menschlichen Fahrers an einem Unfall keine Vermutungsregelung vorgesehen hat, scheint eine gesetzlich normierte Vermutung der Fehlerhaftigkeit eines autonomen Systems aufgrund der Beteiligung an einem Unfall nicht sachgerecht.

(2) Vermutung aufgrund Unfallvermeidung durch sorgfältigen Fahrer

Diskussionswürdig wäre auch eine Regelung, die die Fehlerhaftigkeit eines autonomen Systems für den Fall vermutet, dass das Unfallgeschehen bei Steuerung durch einen sorgfältigen menschlichen Fahrer anstatt eines autonomen Fahrzeugs hätte vermieden werden können. Bei Existenz einer solchen Regelung müsste der Geschädigte als Grundlage der Vermutung beweisen, dass ein autonomes System an einem Unfall beteiligt war und sich das Unfallgeschehen nicht ereignet hätte, sofern das Fahrzeug von einem sorgfältigen menschlichen Fahrer gesteuert worden wäre. Unter Zugrundelegung des oben unter 3. b. gefundenen Ergebnisses brächte die dargestellte Vermutungsregelung jedoch keine Beweiserleichterung für den Geschädigten und kann deshalb als überflüssig betrachtet werden. Ist das autonome System nämlich bereits dann als fehlerhaft zu bewerten, wenn es hinter den Anforderungen, die an einen sorgfältigen menschlichen Fahrer gestellt werden können, zurückbleibt, und beweist der Geschädigte die Vermutungsbasis eines ohne Verwendung des autonomen Systems unfallfreien Alternativverlaufs, kann der Steuerungsalgorithmus ohnehin als produktrechtlich fehlerbehaftet angesehen werden. Einer dahingehenden Vermutungsregelung bedarf es daher nicht mehr.

(3) Notwendigkeit eines Sachverständigen

Nach den vorstehend dargestellten Beweislastregeln hat der Geschädigte den Beweis zu erbringen, dass das Produkt des Herstellers bzw. dessen Steuerungsalgorithmus fehlerhaft war und dieser Fehler zu dem Schaden des Anspruchstellers geführt hat. Angesichts dieser auf erstes Ansehen hin als schwierig zu bezeichnenden Beweisführung ist zu erwarten, dass der Geschädigte sich in der Vielzahl der Fälle der Hilfe eines Sachverständigen bedienen muss. Dieser kann den Unfallhergang daraufhin überprüfen, ob ein menschlicher Fahrer oder Algorithmus den Unfall bei Beachtung der im Verkehr erforderlichen Sorgfalt hätte vermeiden können.[282] Ist dies der Fall, wäre die Fehlerhaftigkeit des autonomen Systems bereits zu bejahen, so dass der Geschädigte eines Zugangs zu dem Quellcode des Herstellers bereits nicht mehr bedarf.[283] Der vermeintlich schwierigen Beweislage, der sich der Geschädigte im Rahmen eines Produkthaftungsprozesses zunächst ausgesetzt sieht, kann daher bereits mit den vorhandenen zi-

[282] Vgl. *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (78).
[283] *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (78).

vilprozessualen Mitteln begegnet werden.[284] Einer über die von der Rechtsprechung im Bereich der Produzentenhaftung bereits entwickelten Grundsätze hinausgehenden weiteren Beweiserleichterung bedarf es demnach im Bereich des autonomen Fahrens nicht.

IV. Ergebnis

Bei einem Fahrzeug mit hoch- oder vollautomatisierter Fahrfunktion hat der Gesetzgeber das bisherige Haftungsregime mit Halter- und Fahrerhaftung als ausreichend erachtet. Dieses Haftungsregime ist auch für das autonome Fahren tauglich und berücksichtigt insbesondere die Interessen von Geschädigten, den Haftenden auf einfache Weise in Anspruch nehmen zu können.

Der Wegfall der Fahrerhaftung nach Maßgabe des § 1b StVG wird beim hoch- oder vollautomatisierten Fahren durch die Verdoppelung der Haftungshöchstbeträge nach § 12 Abs. 1 StVG kompensiert; diese Regelung muss konsequenterweise auch auf das autonome Fahren anwendbar sein.

Mit dem Direktanspruch gegen den Kfz-Haftpflichtversicherer bzw. bei vorsätzlicher Schadensherbeiführung gegen einen Entschädigungsfonds für Schäden aus Kraftfahrzeugunfällen ist sichergestellt, dass der Geschädigte stets einen solventen Schuldner hat; dieser Direktanspruch/Entschädigungsanspruch muss allerdings auch bei durch einen Hackerangriff verursachten Schäden bestehen.

Mit fortschreitender Automatisierung und Verselbstständigung der Fahrzeuge kommt mangels eigener Steuerung durch den Fahrer der dem Betrieb des Fahrzeugs zugrunde liegenden Software eine gesteigerte Funktion zu. Unfälle werden beim automatisierten/autonomen Fahrzeug in der Regel auf ein Versagen der Steuerungssoftware und nicht mehr auf ein Versagen des Fahrers zurückgeführt werden können. Sofern diese Software nicht durch den Endhersteller des Fahrzeugs selbst, sondern durch einen Zulieferer bereitgestellt wurde, kann nicht nur der Fahrzeughersteller, sondern auch der Zulieferer im Wege der Produzentenhaftung in Anspruch genommen werden.

Der in einem autonomen System verwendete Steuerungsalgorithmus muss den Anforderungen an eine sorgfältige, dem Stand der Technik entsprechende Programmierung gerecht werden. Es dürfte den berechtigten Sicherheitserwartungen regelmäßig entsprechen, dass der Algorithmus auch in einer konkreten Ver-

[284] Vgl. auch *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien?, CR 2015, 766 (772).

kehrssituation nicht hinter den Sorgfaltsanforderungen zurücksteht, die an einen sorgfältigen menschlichen Fahrer gestellt werden können, soweit er bestimmungsgemäß den menschlichen Fahrer ersetzen soll. Die Beurteilung der berechtigten Sicherheitserwartungen im Einzelfall kann der Rechtsprechung überlassen bleiben.

In Dilemmasituationen kann die Bestimmung der Anforderungen, die an die Ausgestaltung der Steuerungssoftware des autonomen Fahrzeugs zu stellen sind, allerdings nicht allein nach dem Stand von Wissenschaft und Technik erfolgen; vielmehr sind hier auch ethische Wertungen entscheidend. Angesichts des derzeitigen technischen Entwicklungsstandes, der eine Unterscheidung verschiedener Rechtsgüter und Personengruppen durch ein autonomes Fahrzeug noch nicht zulässt, erscheint ein zeitnahes gesetzgeberisches Handeln noch nicht erforderlich. Die Möglichkeit der Schaffung von mehr Rechtssicherheit für die Hersteller sollte jedoch - möglichst auf europäischer Ebene - weiter geprüft und verfolgt werden.

Es sollte überlegt werden, ob eine Zulassung autonomer Fahrzeuge nur dann erfolgen sollte, wenn das Fahrzeug über eine Blackbox verfügt, um den Geschädigten vor unüberwindbaren Beweisschwierigkeiten zu bewahren.

G. Medizintechnik

I. Einführung

Der Einsatz von Maschinen und Geräten in der Medizin ist prinzipiell nichts Neues und seit vielen Jahren Standard. Innovative Medizinprodukte helfen bei der Diagnose, Entscheidung und Therapie. Es stellt sich aber die Frage, ob und in welchem Umfang aktuell und in absehbarer Zukunft automatisierte und autonome Systeme im medizinischen Bereich zum Einsatz kommen werden und welche rechtlichen Fragestellungen sich daran knüpfen. Dem widmet sich dieses Kapitel.

Die Arbeitsgruppe hat zunächst Experten aus dem Bereich der Medizintechnik befragt, um sich ein Bild über aktuelle und zukünftige Einsatzfelder automatisierter und autonomer Systeme zu machen. Ergebnis dieser Befragungen war, dass zum jetzigen Zeitpunkt im Wesentlichen keine wirklich autonomen - schon gar keine selbstlernenden - Systeme eingesetzt werden. Bei den derzeit und absehbar zum Einsatz kommenden Systemen handelt es sich vielmehr um Assistenzsysteme, die den behandelnden Arzt bei Diagnose und Therapie unterstützen. So werden beispielsweise beim Lesen von Mammographiebildern oder Röntgen-Thorax-Aufnahmen Unterstützungssysteme eingesetzt, die aufgrund des Trainings mit einer Vielzahl von Datensätzen treffsichere Diagnosen vorschlagen können. Sie bieten dem Arzt eine Diagnose oder Therapieempfehlung an, wobei es sich quasi um eine „Zweitmeinung“ handelt und die letztendliche Entscheidung weiterhin beim Arzt verbleibt.

Entscheidend für die weiteren Prüfungen der Arbeitsgruppe war die auf den Angaben von Sachverständigen beruhende Prämisse, dass weder jetzt noch in absehbarer Zeit selbstlernende autonome Systeme zum Einsatz kommen werden. Angesichts der Notwendigkeit der Zulassung solcher Systeme im Bereich der Medizintechnik sei weder möglich noch gewollt, dass diese Systeme nach Inverkehrbringen selbsttätig weiterlernen. Vielmehr werden nur geschlossene - abgekapselte - Systeme in Verkehr gebracht.

Ausgehend davon wird im Folgenden untersucht, ob das geltende Haftungssystem auch für den Einsatz autonomer Systeme in der Medizintechnik sachgerechte Lösungen bereithält oder ob und inwieweit gesetzgeberischer Handlungsbedarf besteht.

II. Betreiberhaftung

1. Vertragliche Haftung

Der Behandlungsvertrag ist in den §§ 630a ff. BGB geregelt. Diese Vorschriften enthalten wichtige Vorgaben dazu, unter welchen Voraussetzungen der Behandelnde, typischerweise ein Arzt, haftet. Im Übrigen gelten freilich die allgemeinen Vorschriften. Es stellt sich die Frage, ob die geltenden Regelungen auch dann zu sachgerechten Ergebnissen führen, wenn ein autonomes System bei der Diagnose oder Behandlung eingesetzt wird. Nur dann, wenn dies nicht der Fall ist, kann sich die weitere Frage stellen, inwiefern ein Handeln des Gesetzgebers geboten ist.

a. Vertragsschluss

Der Behandlungsvertrag kommt zwischen dem Krankenhausträger und/oder dem Arzt auf der einen Seite und dem Patienten auf der anderen Seite zustande (§§ 145 ff. BGB). Hieran ändert sich auch dann nichts, wenn im Rahmen der Diagnostik oder Therapie auf autonome Systeme zurückgegriffen wird. Der theoretisch denkbare Fall, dass vom Patienten von Anfang an kein Arzt, sondern sogleich eine Maschine kontaktiert wird, welche sodann autonom über die weiteren Schritte entscheidet, ist derzeit kein realistisches Szenario und muss hier deshalb nicht weiter vertieft werden; nur in diesem Fall kann sich die Frage nach den Vertragsparteien stellen.

b. Pflichtverletzung

Eine Haftung nach § 280 Abs. 1 S. 1 BGB setzt eine Pflichtverletzung des Behandelnden voraus.

(1) Grundlagen

Die medizinische Diagnostik und Behandlung hängt bereits heute zu einem großen Teil davon ab, welche Güte die dabei herangezogenen Medizinprodukte aufweisen. So wird in der ärztlichen Praxis umfangreich auf automatisierte Medizintechnik zurückgegriffen, wobei die Rechtsprechung es verstanden hat, den sich hieraus ergebenden Besonderheiten durch eine sachgerechte Auslegung des geltenden Rechts angemessen Rechnung zu tragen. So hat sie insbesondere Überwachungs- und Kontrollpflichten entwickelt, um auch in Fällen, in denen fehlerhafte Produkte zum Einsatz kommen, zu interessengerechten Lösungen zu gelangen. Davon abgesehen stellt das Medizinproduktegesetz (MPG) spezielle Anforderungen an Medizinprodukte und deren Betrieb.

Die Besonderheit autonomer Systeme besteht – definitionsgemäß – darin, dass sie Aktionen vornehmen, die in dem Zeitpunkt, in dem sie vorgenommen wer-

den, nicht von einem aktuell gebildeten menschlichen Willen getragen werden; die Entscheidung, welche von mehreren denkbaren Aktionen durchgeführt wird, liegt vielmehr bei dem von Menschenhand programmierten System. Hieraus ergibt sich eine besondere Interessenlage, wenn es zu Fehlern bei der Ausführung kommt. Denjenigen Arzt, der den konkreten Steuerungsverlauf in Gang gesetzt hat, wird man nicht ohne weiteres für einen Ausführungsfehler des autonomen Systems verantwortlich machen können. Dies gilt insbesondere dann, wenn der Ausführungsfehler auf einer fehlerhaften Programmierung beruht. Man wird aber von dem Arzt – wie stets beim Einsatz von Medizinprodukten – verlangen können, dass er die autonom agierende Maschine sachgerecht auswählt, überwacht und – soweit diese Aufgabe nicht beim Krankenhausträger liegt – wartet.

Dies verdeutlicht, dass es beim Einsatz autonomer Systeme zu einer Verlagerung der Pflichten kommt. Je autonomer das System agiert, desto häufiger wird es dazu kommen, dass der Arzt nach den §§ 280 ff. BGB nicht mehr für Ausführungsfehler, sondern allein noch für Fehler bei der Auswahl, Überwachung und Wartung des Produkts sowie hinsichtlich der Aufklärung haftet.

(2) Pflichten des Arztes beim Einsatz autonomer Systeme

Im Ausgangspunkt treffen den Arzt auch in Bezug auf autonome Medizintechnik jedenfalls diejenigen Pflichten, die er auch dann zu erfüllen hat, wenn er herkömmliche Medizinprodukte zum Einsatz bringt. Im Folgenden soll der Frage nachgegangen werden, ob das von der Rechtsprechung in Bezug auf herkömmliche Medizinprodukte herausgearbeitete Pflichtengefüge für den Fall autonomer Systeme einer – ggf. legislativen – Ergänzung bedarf.

(a) Ausgangspunkt: Einhaltung des medizinischen Standards

Der Arzt muss bei der Diagnostik und Behandlung grundsätzlich den medizinischen Standard einhalten. Freilich darf er – vorbehaltlich der aufgeklärten Entscheidung des Patienten – zwischen mehreren Behandlungsmöglichkeiten, die alle dem Standard entsprechen, wählen. Soweit also in einigen Jahren der Fall eintritt, dass der Einsatz einer autonomen Technik dem Standard entspricht, bezieht sich die Wahlmöglichkeit des Arztes auch auf deren Einsatz. Ist dieser Stand noch nicht erreicht, können den Arzt besondere Aufklärungspflichten treffen.

(b) Aufklärungspflichten

Den Arzt treffen bereits nach allgemeinen Grundsätzen unterschiedliche Aufklärungspflichten. Insbesondere muss er den Patienten über die wesentlichen Risiken, die insbesondere mit der von ihm vorgeschlagenen Therapie im Zusammenhang stehen, aufklären. Das gilt auch dann, wenn ein autonomes System

zum Einsatz kommen soll. Von einer ordnungsgemäßen Therapieauswahl und Durchführung kann nur dann die Rede sein, wenn der Arzt dem Patienten vor dem beabsichtigten Einsatz eines autonomen Systems eine nachvollziehbare Nutzen- und Risikoabwägung ermöglicht. Auf dieser Grundlage bezieht sich die ärztliche Aufklärungspflicht zunächst auf die Frage, welches Medizinprodukt zur Anwendung kommen soll. Das gilt insbesondere dann, wenn der Patient für den Arzt erkennbar einen gesteigerten Wert darauf legt, dass ein bestimmtes Produkt angewendet oder gerade nicht verwendet wird. Dann hat der Arzt über die Risiken aufzuklären, die sich aus einer etwaigen Entscheidung des Patienten ergeben. Insbesondere muss er Behandlungsalternativen aufzeigen. All dies gilt ohne weiteres auch dann, wenn es sich bei dem Medizinprodukt, um dessen Einsatz es geht, um ein autonom agierendes System handelt.

Besonderheiten können sich dann stellen, wenn es um ein autonom agierendes Produkt geht, für das sich noch kein Standard entwickelt hat, es sich also um ein neuartiges Produkt handelt. Auch für diesen Fall kann allerdings auf Grundsätze zurückgegriffen werden, die von der Rechtsprechung bereits zu herkömmlichen Medizinprodukten entwickelt wurden. So hat der BGH[285] in seiner sog. Robodoc-Entscheidung klargestellt, dass auch die Anwendung neuer Verfahren für den medizinischen Fortschritt unerlässlich ist; am Patienten dürfen sie aber nur dann angewandt werden, wenn diesem zuvor unmissverständlich verdeutlicht wurde, dass die neue Methode die Möglichkeit unbekannter Risiken birgt. Letztlich muss der Patient in die Lage versetzt werden, für sich sorgfältig abzuwägen, ob er sich nach der herkömmlichen Methode mit bekannten Risiken behandeln lässt oder besser nach einer neuen Methode unter besonderer Berücksichtigung der in Aussicht gestellten Vorteile und der noch nicht in jeder Hinsicht bekannten Gefahren.

Das gilt auch beim Einsatz autonomer Systeme. Der Arzt muss mit dem Patienten die Chancen und Risiken des in Rede stehenden autonomen Systems besprechen und bewerten. Dem Patienten muss eine sachgerechte Entscheidung darüber ermöglicht werden, ob er ein autonomes System zum Einsatz kommen lassen möchte oder nicht. Dabei gilt der Grundsatz, dass die Aufklärungspflicht umso weiter reicht, je stärker der Arzt von etablierten Behandlungen abweicht.[286] Die Beweislast dafür, dass der Arzt seine Aufklärungspflicht ordnungsgemäß erfüllt hat, liegt allgemeinen Regeln entsprechend bei ihm.

---

[285] BGH, Urt. v. 13.6.2006 – VI ZR 323/04, BGHZ 168, 103 = NJW 2006, 2477.

[286] *Koyunco/Dahm-Loraing*, Die Haftung des Arztes und Krankenhauses für Medizinprodukte – Teil 2, PHi 2009, 218 (220).

(c) Pflichten aus § 4 Abs. 1 MPG

Beim Einsatz von Medizinprodukten ist ferner § 4 Abs. 1 MPG zu beachten. Danach ist es insbesondere verboten, ein Medizinprodukt in den Verkehr zu bringen, zu errichten, in Betrieb zu nehmen, zu betreiben oder anzuwenden, wenn der begründete Verdacht besteht, dass es die Sicherheit und die Gesundheit der Patienten, der Anwender oder Dritter bei sachgemäßer Anwendung, Instandhaltung und ihrer Zweckbestimmung entsprechender Verwendung über ein nach den Erkenntnissen der medizinischen Wissenschaften vertretbares Maß hinausgehend unmittelbar oder mittelbar gefährdet. Das gilt selbstverständlich auch dann, wenn es um den Einsatz autonomer Systeme geht. Problematisch sind dabei die Fälle, in denen in der Fachliteratur oder in der Presse ein „begründeter Verdacht" geäußert wird.[287] Dann kann sich die Frage stellen, ob der Arzt schon aus diesem Grunde heraus auf den Einsatz verzichten muss. Hierbei handelt es sich aber nicht um eine Besonderheit, die sich nur oder vorwiegend beim Einsatz autonomer Systemen stellt, sondern um ein Problem, das generell beim Einsatz von Medizinprodukten zum Tragen kommen kann. Es ist derzeit nicht ersichtlich, dass der Gesetzgeber insoweit eine spezielle Regelung für autonome Systeme bereitstellen müsste. Die Lösung etwaiger Probleme, die sich insoweit im Einzelfall stellen können, kann der Rechtsprechung überantwortet werden.

(d) Prüfungspflichten des Arztes

Den Arzt treffen beim Einsatz von Medizinprodukten recht weitgehende Prüfungspflichten. So muss der Arzt sich vor dem Einsatz des Geräts vergewissern, ob das Gerät einsatzfähig ist. Sofern er bei der insoweit vorzunehmenden Prüfung erkennen kann, dass das Gerät fehlerhaft ist, darf er es nicht einsetzen; beachtet er dies nicht, kommt eine Haftung in Betracht. Eine vertragliche Haftung des Arztes für jeden Produktfehler folgt hieraus freilich nicht. Eine solche Haftung ist weder für herkömmliche Medizinprodukte anzuerkennen, noch sollte sie für autonome Systeme begründet werden. Die Interessenlage ist insoweit keine andere.

Unabhängig von der Frage, welche konkrete Prüfung der Arzt vor dem Einsatz einer Maschine durchzuführen hat, muss er während des Einsatzes prüfen, ob das Gerät richtig arbeitet und ob es notwendig wird, einzugreifen und die konkrete Maßnahme ggf. abzubrechen. Den Arzt treffen also Kontrollpflichten.

---

[287] Dazu etwa *Koyunco/Dahm-Loraing*, Die Haftung des Arztes und Krankenhauses für Medizinprodukte – Teil 1, PHi 2009, 172 (176).

Insbesondere dann, wenn ein autonomes System im Rahmen der Diagnose eingesetzt wird, muss der Arzt das von dem System ermittelte Ergebnis kontrollieren. Dabei kann sich allerdings die Frage stellen, welche Prüfungsintensität der Arzt insoweit anzulegen hat. Einerseits könnte man verlangen, dass der Arzt jedenfalls auch diejenigen Untersuchungen durchführen muss, die er veranlassen würde, wenn ein autonomes System nicht zum Einsatz kommt. Andererseits ließe sich die Auffassung vertreten, er sei auf eine Plausibilitätsprüfung beschränkt. Richtigerweise wird man wohl differenzieren müssen. Grundsätzlich wird man annehmen müssen, dass der Einsatz des autonomen Systems nicht zu einer Verringerung der den Arzt treffenden Pflichten führt. Etwas anderes wird man möglicherweise erst dann annehmen können, wenn das Produkt sich über einen längeren Zeitraum in der Praxis bewährt und gesicherte Erkenntnisse darüber vorliegen, dass nur in einer zu vernachlässigenden Anzahl von Fällen die Überprüfung des von der Maschine gefundenen Ergebnisses durch den Menschen zu einem genaueren Ergebnis führt. Nur unter dieser Voraussetzung erscheint es gerechtfertigt, dass der Arzt auf die Leistung des autonomen Systems mit der Folge vertrauen darf,[288] dass sich seine Pflichten verkürzen. Dieser Zeitpunkt dürfte nicht schon mit demjenigen zusammenfallen, in dem der Einsatz des Systems als Standard anzusehen ist; vielmehr dürften hierzu weitere Erkenntnisse nötig sein. Jene schwierigen Fragen müssen jedoch in diesem Bericht nicht abschließend beantwortet werden. Hier soll es allein darum gehen, den gesetzgeberischen Handlungsbedarf zu ermitteln. Dabei kann die Problematik, unter welchen Voraussetzungen der Arzt seinen Kontrollpflichten durch eine bloße Plausibilitätsprüfung genügt, der Rechtsprechung überlassen werden. Letztlich geht es darum, die bereits zu herkömmlichen Medizinprodukten entwickelten Grundsätze weiter auszuformen. Einer speziellen gesetzlichen Regelung bedarf es – jedenfalls derzeit – nicht.

(e) Pflicht zur ordnungsgemäßen Bedienung

Der Arzt ist selbstverständlich dazu verpflichtet, das Gerät richtig zu bedienen. Er hat insbesondere diejenigen Voreinstellungen zu treffen, die für einen ordnungsgemäßen Einsatz erforderlich sind. Soweit ein autonomes System darauf angelegt ist, solche Handlungen vorzunehmen, die bislang ein Arzt durchgeführt hat, ist es dem Arzt auch nicht gestattet, die Pflichten zur Bedienung des Gerätes auf Personen zu delegieren, die keine Ärzte sind. Die Zulässigkeit einer solchen Delegation könnte allenfalls der Gesetzgeber anordnen; hierfür besteht – jedenfalls derzeit – kein Bedürfnis.

---

[288] Zum Vertrauensgrundsatz vgl. auch OLG Saarbrücken, Urt. v. 15.7.1998 – 1 U 859/97, NJW-RR 1999, 749, 750.

(f) Pflicht zur Nachsorge

Den Arzt trifft bereits nach allgemeinen Grundsätzen die Pflicht, den Patienten zu informieren und Kontrolluntersuchungen durchzuführen, wenn nachträglich bekannt wird, dass ein Medizinprodukt, das eingesetzt wurde, fehlerhaft war. Insoweit geht es letztlich um die Pflicht des Arztes zur Nachsorge und Verlaufskontrolle.[289] Diese greift jedenfalls dann ein, wenn der begründete Verdacht besteht, dass durch die Verwendung eines Medizinprodukts die Sicherheit und Gesundheit des Patienten über ein medizinisch vertretbares Maß hinaus gefährdet sind.[290] Es ist nicht erkennbar, dass insoweit beim Einsatz autonomer Systeme andere Grundsätze gelten sollten; ein gesetzgeberischer Handlungsbedarf besteht derzeit auch in diesem Zusammenhang nicht.

(g) Gerätesicherheit und Wartungspflichten

Beim Betrieb eines Medizinprodukts sind die Vorgaben der Medizinprodukte-Betreiberverordnung (MPBetreibV) einzuhalten. Die Pflichten treffen in erster Linie den Betreiber (§ 2 Abs. 2 MPBetreibV). Nach Auffassung der Arbeitsgruppe ist die MPBetreibV auch auf autonom agierende Systeme anwendbar. Dabei spielt es keine Rolle, ob es sich bei dem in Rede stehenden System um eine bloße Software handelt; auch ein solches System wird allgemeinen Grundsätzen entsprechend vom Anwendungsbereich der MPBetreibV erfasst.[291] Es ist nicht erkennbar, dass insoweit in Bezug auf autonome Systeme ein gesetzgeberischer Handlungsbedarf besteht.

Das gilt insbesondere auch für die Frage, welche Regeln für ein Upgrade oder ein Update einzuhalten sind. § 7 Abs. 1 MPBetreibV regelt die Instandhaltung von Medizinprodukten. Diese umfasst Maßnahmen zur Instandhaltung und die Instandsetzung. Dabei zählt nach DIN 31051 unter anderem auch die „Verbesserung" zu den Instandhaltungsmaßnahmen.[292] Im Hinblick auf Upgrades und Updates wird man insoweit wie folgt differenzieren müssen:

Ein Upgrade bringt typischerweise „wesentliche Veränderungen" des Medizinprodukts mit sich; es handelt sich deshalb in der Regel um ein (neues) Inverkehrbringen im Sinne von § 3 Nr. 11 MPG. Es ist also § 6 MPG zu beachten, der nähere Anforderungen an das Inverkehrbringen und die Inbetriebnahme eines Medizinproduktes stellt. Diese Vorschrift richtet sich in erster Linie an den Her-

---

[289] Vgl. *Koyunco/Dahm-Loraing*, Die Haftung des Arztes und Krankenhauses für Medizinprodukte – Teil 1, PHi 2009, 172 (177).
[290] Vgl. *Koyunco/Dahm-Loraing*, Die Haftung des Arztes und Krankenhauses für Medizinprodukte – Teil 1, PHi 2009, 172 (177).
[291] Vgl. *Anhalt/Dieners*, Medizinprodukterecht, § 9 Rn. 8.
[292] *Anhalt/Dieners*, Medizinprodukterecht, § 9 Rn. 33.

steller. Es ist kein Grund erkennbar, weshalb für autonom agierende Systeme insoweit etwas anderes gelten sollte.

Demgegenüber handelt es sich bei einem Update typischerweise darum, dass Schwachstellen oder Produktmängel beseitigt werden, um die Funktionssicherheit oder Verfügbarkeit zu erhöhen.[293] Die Vornahme eines vom Hersteller zur Verfügung gestellten Updates wird man damit als Instandhaltungsmaßnahme im Sinne von § 4 Abs. 1 MPBetreibV qualifizieren können.[294] Somit ist der Betreiber eines Medizinprodukts, also insbesondere auch derjenige eines autonom agierenden Systems, bereits nach der MPBetreibV dazu verpflichtet, die zur Verfügung gestellten Updates zu installieren. Ein weitergehender Handlungsbedarf des Gesetzgebers ist derzeit nicht erkennbar.

(h) Besonderheiten in der Erprobungsphase

Innerhalb der Erprobungsphase eines Medizinprodukts sind in Bezug auf die Haftung nach dem ProdHaftG einige Besonderheiten zu beachten; insbesondere ist umstritten, ob der Produkthersteller eines Medizinprodukts auch in jener Zeit gegenüber den Probanden verschuldensunabhängig haftet. Vergleichbare Probleme stellen sich aber im Rahmen der vertraglichen Haftung des Arztes nicht. Der Arzt hat den Patienten stets sachgerecht aufzuklären; dazu gehört insbesondere auch die Information, dass das Produkt, welches eingesetzt werden soll, möglicherweise noch nicht ausgereift ist. Auf diese Weise soll der Patient dazu in die Lage versetzt werden, eine eigenverantwortliche Entscheidung darüber zu treffen, ob er dem Einsatz des Produkts trotz der hiermit verbundenen Risiken zustimmt. Für den Einsatz eines noch nicht ausgereiften autonom agierenden Systems kann nichts anderes gelten.

c. Vertretenmüssen

Gemäß § 280 Abs. 1 S. 2 BGB haftet der Schuldner nicht, wenn er die Pflichtverletzung nicht zu vertreten hat. Es ist Sache des Arztes darzulegen und ggf. zu beweisen, dass es an einem Vertretenmüssen fehlt. Sofern jedoch eine Pflichtverletzung festgestellt werden kann, dürfte dem Arzt die Exkulpation nur in seltenen Ausnahmefällen gelingen. Es erscheint nicht geboten, dem Arzt die Möglichkeit zu nehmen, sich beim Einsatz autonomer Medizintechnik zu exkulpieren.

---

[293] *Anhalt/Dieners*, Medizinprodukterecht, § 9 Rn. 33.
[294] *Anhalt/Dieners*, Medizinprodukterecht, § 9 Rn. 33.

d. Weitere Beweisfragen

(1) Umkehr der Beweislast für Vorliegen einer Pflichtverletzung

Es stellt sich die Frage, ob es die Besonderheiten autonomer Systeme rechtfertigen, dass im Falle ihres Einsatzes nicht allein das Vertretenmüssen, sondern – de lege ferenda – auch die Pflichtverletzung des Arztes vermutet werden sollte.

Nach dem geltenden Recht hat grundsätzlich der Gläubiger darzulegen und im Bestreitensfall zu beweisen, dass der Schuldner eine Pflicht aus dem Schuldverhältnis verletzt hat.

Eine Ausnahme von jenem Grundsatz sieht § 630h Abs. 1 BGB vor. Nach dieser Vorschrift wird ein Fehler des Behandelnden vermutet, wenn sich ein allgemeines Behandlungsrisiko verwirklicht hat, das für den Behandelnden voll beherrschbar war und das zur Verletzung des Lebens, des Körpers oder der Gesundheit des Patienten geführt hat. Mit dieser Vorschrift hat der Gesetzgeber im Jahre 2013 die von der Rechtsprechung entwickelten Grundsätze kodifiziert. Dabei geht es letztlich um diejenigen Gefahren, die allein dem Herrschafts- und Organisationsbereich des Behandelnden zuzuordnen sind und die unabhängig sind von den Unwägbarkeiten des menschlichen Organismus.[295] § 630h Abs. 1 BGB kommt insbesondere dann zum Tragen, wenn Medizinprodukte eingesetzt werden, die nicht gemäß den gesetzlichen Vorgaben gewartet wurden.

Auf dieser Grundlage wird die Vorschrift auch dann von Relevanz sein, wenn der Betreiber eines autonom agierenden Systems die ihn treffenden Wartungspflichten, insbesondere diejenigen aus der MBetreibV, nicht erfüllt. Dabei spielt es auch keine Rolle, ob das autonome System eine Entscheidung trifft, die der Betreiber – für sich genommen – nicht voraussehen und voll beherrschen kann. Im hiesigen Zusammenhang ist vielmehr allein entscheidend, dass der Betreiber über die Erfüllung der in Rede stehenden Wartungspflichten allein entscheiden und diese deshalb „voll beherrschen" kann. Die Autonomie eines Systems wird also keineswegs dazu führen, dass die in § 630h Abs. 1 BGB geregelte Vermutung nicht zum Tragen kommen kann. Ein Regelungsbedarf ist insoweit derzeit nicht erkennbar.

Von der soeben behandelten Problematik ist die weitere Frage zu unterscheiden, ob und ggf. unter welchen Voraussetzungen der Fehler eines Medizinprodukts vermutet werden sollte. Diese Thematik ist jedoch nicht hier, sondern im Zu-

---

[295] BeckOGK/*Walter*, 1.7.2017, BGB § 630h Rn. 2.

sammenhang zu erörtern, ob die Produkthaftungsrichtlinie oder das Produkthaftungsgesetz (ProdHaftG) angepasst werden sollten.[296]

(2) Vermutung der haftungsbegründenden Kausalität

Den Geschädigten trifft nach allgemeinen Grundsätzen die Beweislast für die sog. haftungsbegründende Kausalität. Das kann zu Ergebnissen führen, die nicht immer als „gerecht" erscheinen. Insoweit ist jedoch kein Problem berührt, das sich nur oder vorwiegend beim Einsatz autonom agierender Systeme stellt. Angesprochen ist insoweit vielmehr eine grundlegende Problematik des Arzthaftungsrechts, die an anderer Stelle untersucht[297] und nicht vom Prüfungsauftrag der hiesigen Arbeitsgruppe umfasst wird. Aus demselben Grund wird hier auch nicht näher auf die Frage eingegangen, ob § 630h Abs. 5 S. 1 BGB, der eine Beweislastumkehr (nur) bei groben Behandlungsfehler vorsieht, überarbeitet werden sollte.

2. Deliktische Haftung

Im Rahmen der deliktischen Haftung ist zwischen der verschuldensabhängigen Haftung (insb. § 823 Abs. 1 und Abs. 2 BGB) und der Gefährdungshaftung zu differenzieren.

a. Haftung aus § 823 Abs. 1 und Abs. 2 BGB

Sofern der behandelnde Arzt die ihn treffenden Verkehrspflichten verletzt, kommt eine Haftung aus § 823 Abs. 1 BGB in Betracht. Der Inhalt und die Reichweite der Pflichten sind im Vertrags- sowie im Deliktsrecht im Wesentlichen deckungsgleich; es kann insoweit auf die obigen Ausführungen verwiesen werden. Zwar wird im Rahmen von § 823 Abs. 1 BGB das für die Haftung erforderliche Verschulden nicht vermutet. Dies führt jedoch nicht dazu, dass die Haftung des Arztes in einer rechtspolitisch unerwünschten Anzahl von Fällen entfällt. Vielmehr folgt aus der Feststellung, dass der Arzt die Verkehrspflichten verletzt hat, in der Regel auch, dass den Arzt ein Verschulden trifft. Es ist nicht erkennbar, dass dies dann, wenn ein autonomes System eingesetzt wurde und der Arzt seine ihn treffenden Pflichten verletzt hat, anders ist. Ein gesetzgeberischer Handlungsbedarf ist also auch insoweit derzeit nicht erkennbar.

Die Haftung aus § 823 Abs. 2 BGB erlangt insbesondere dann praktische Relevanz, wenn der Betreiber eines Medizinprodukts seine aus § 4 MPG folgenden Pflichten nicht erfüllt. Hierbei handelt es sich um ein Schutzgesetz im Sinne je-

---

[296] Dazu III. 2. b.

[297] S. dazu den in 2017 vorgelegten Abschlussbericht der länderübergreifenden AG „Verbesserungen im Arzthaftungsrecht".

ner Vorschrift. In Bezug auf autonom agierende Systeme stellen sich (auch) in diesem Zusammenhang keine Besonderheiten, die spezielle gesetzliche Regelung erfordern würden.

b. Gefährdungshaftung

Es stellt sich die weitere Frage, ob den Betreiber eines autonom agierenden Medizinprodukts eine Gefährdungshaftung treffen sollte. Überzeugend ist eine solche Gefährdungshaftung (nur) dann, wenn ihr Haftungsgrund diesen Fall erfasst. Insoweit kann auf die oben unter E. III. hergeleiteten Kriterien zurückgegriffen werden; diese werden mithin im Folgenden herangezogen.

(1) Existenz einer „besonderen" Gefahr

Wie bereits oben[298] dargestellt, ist der Betreiber eines Produkts, von dem eine besondere Gefahr ausgeht, grundsätzlich ein tauglicher Zurechnungsadressat der Gefährdungshaftung. Der Betreiber ist typischerweise dazu in der Lage, die Gefahr zu beherrschen; er entscheidet insbesondere über den Einsatz des Produkts. Gerechtfertigt ist eine Gefährdungshaftung freilich nur dann, wenn von dem Produkt eine „besondere Gefahr" ausgeht. Zur Beurteilung der Frage, ob dies der Fall ist, lassen sich keine festen Kriterien bestimmen; insoweit kommt dem Gesetzgeber eine Einschätzungsprärogative zu. Der Gesetzgeber hat es also grundsätzlich in der Hand, einzelne Produkte herauszugreifen und an ihren Betrieb eine Gefährdungshaftung zu knüpfen. In Bezug auf autonom agierende Medizinprodukte ließe sich allenfalls noch die Frage stellen, ob eine Gefährdungshaftung deshalb ausscheiden muss, weil das Produkt dazu dienen soll, eine Beeinträchtigung an der Gesundheit zu heilen oder zu lindern; vor diesem Hintergrund könnte man darauf abstellen, dass von einem solchen Produkt keine „Gefahr" ausgehen könne. Eine solche begriffliche Argumentation kann indes nicht überzeugen. Entscheidend ist nicht die Widmung des Produkts, sondern allein, ob aus dem Einsatz des Produkts, das zum Gegenstand einer Gefährdungshaftung gemacht werden soll, weitergehende Schadensrisiken resultieren. Das trifft auf autonom agierende Medizinprodukte zu.

(2) Geschützter Personenkreis und Notwendigkeit einer Gefährdungshaftung

Allein der Umstand, dass von einem Produkt eine besondere Gefahr ausgeht, führt nicht dazu, dass die Einführung einer Gefährdungshaftung zu empfehlen ist. Vielmehr ist darüber hinaus zu prüfen, ob mit den Gefahren des Produkts typischerweise solche Personen in Berührung kommen, die bei normativer Betrachtung den Schutz einer Gefährdungshaftung bedürfen; dies muss, wie bereits

---

[298] Dazu unter E. III. 3. c.

oben[299] dargestellt, produktbezogen geprüft werden. Stellt sich im Rahmen dieser Prüfung heraus, dass nur solche Personen den Gefahren des Produkts ausgesetzt sind, die auf einen solchen Schutz nicht angewiesen sind, so spricht dies gegen die Notwendigkeit, eine Gefährdungshaftung zu begründen.

(a) Was den hier interessierenden Einsatz von autonom agierender Medizintechnik angeht, so ist zu bedenken, dass mit dieser typischerweise keine unbeteiligten Dritten in Berührung kommen. Die Risiken, die von dem Produkt ausgehen, treffen vielmehr allein den Patienten. Der Schutz der Allgemeinheit gebietet es damit nicht, eine Gefährdungshaftung für Medizinprodukte einzuführen.

(b) Zu klären bleibt, ob der Patient, zu dessen Gunsten ein autonom agierendes Medizinprodukt eingesetzt wird, auf den Schutz, den eine Gefährdungshaftung vermittelt, angewiesen ist. Bei dem Patienten handelt es sich um den Profiteur des Produkts. Allgemeine Leitlinien dazu, unter welchen Voraussetzungen der Profiteur eines Produkts den Schutz einer Gefährdungshaftung erhalten sollte, sind bereits oben[300] entwickelt worden; diese sollen im Folgenden auf den hier interessierenden Fall, nämlich den Einsatz autonom agierender Medizintechnik, angewendet werden. Da der Patient typischerweise über das Produkt keine solche Kontrolle erhält, die so stark ist, dass es gerechtfertigt ist, den Betreiber aus seiner Verantwortung zu entlassen,[301] kommt es darauf an, ob ohne eine Gefährdungshaftung eine hinreichend gewichtige Haftungslücke droht.

Soweit ein autonom agierendes System eingesetzt wird, kann in Bezug auf einen etwaigen Ausführungsfehler des Produkts grundsätzlich keine Pflichtverletzung des Arztes gesehen werden. Etwas anderes gilt freilich dann, wenn dieser Fehler auf einer fehlerhaften Auswahl, Bedienung oder Wartung beruht. Allein dies zeigt jedoch deutlich, dass der Einsatz autonomer Medizintechnik eine Verlagerung der Pflichten zur Folge haben kann. Das kann insbesondere dann zu Problemen führen, wenn Produkte eingesetzt werden, die nicht nur autonom, sondern auch selbstlernend agieren. Der Einsatz solcher Produkte ist jedoch jedenfalls für den Medizinbereich nicht in absehbarer Zeit zu erwarten. Dies haben die von der Arbeitsgruppe gehörten Experten übereinstimmend berichtet, so dass dies als Prämisse für die weiteren Überlegungen zugrunde gelegt werden soll. Das wurde insbesondere damit begründet, dass es – jedenfalls für den Bereich der Medizintechnik – bislang kein System gibt, das zuverlässig überprüfen kann, ob die „neuen" Daten in dem Sinne „zutreffend" sind, dass sie zur Grundlage zukünftiger autonomer Entscheidungen gemacht werden können. Die Hersteller verfahren deshalb so, dass dasjenige System, welches in den Markt gelangt, „abgekap-

---

[299] Dazu unter E. III. 4. b.
[300] Dazu unter E. III. 4. b. (2).
[301] Dazu unter E. III. 4. b. (2) (a).

selt“ wird und beim späteren Einsatz allein die Daten verwendet werden, die vom Hersteller – von Beginn an oder im Zuge eines Updates – freigegeben wurden. Vor dem Hintergrund, dass die Arbeitsgruppe sich allein mit solchen Techniken befasst, deren Einsatz in absehbarer Zeit bevorsteht, muss auf Probleme, die sich beim Einsatz selbstlernender Systeme stellen können, hier nicht weiter eingegangen werden.

Die Prüfung kann sich deshalb auf die Frage beschränken, ob beim Einsatz autonom agierender Medizintechnik, die nicht selbstlernend ist, eine Haftungslücke droht, die im Wege der Gefährdungshaftung geschlossen werden sollte. Allein die Feststellung, dass es zu der soeben angesprochenen Verlagerung der Pflichten kommen kann, genügt nicht, um von einem gesetzgeberischen Handlungsbedarf auszugehen; der ggf. drohenden Haftungslücke muss vielmehr ein hinreichendes Gewicht zu kommen. Das ist hier nicht der Fall:

Wie bereits oben[302] dargestellt, kann es gegen eine hinreichend gewichtige Haftungslücke sprechen, dass der Einsatz des Produkts von einer Zulassung abhängig ist. Es kann nämlich grundsätzlich davon ausgegangen werden, dass dann, wenn ein Zulassungsverfahren existiert, die Gefahr schädigender Ereignisse geringer ist, als würde es das Zulassungsverfahren nicht geben. In Bezug auf autonom agierende Medizintechnik spricht jenes Kriterium mithin indiziell gegen eine gewichtige Haftungslücke. Denn ein Medizinprodukt muss, und auch insoweit kann auf die obigen Ausführungen[303] verwiesen werden, vor seinem Einsatz das oben angesprochene[304] Zulassungsverfahren durchlaufen.

Ferner spricht es gegen eine hinreichend gewichtige Haftungslücke, wenn mit dem Produkt typischerweise nur solche Personen in Berührung kommen, die über die Risiken, welche von dem Produkt ausgehen, hinreichend aufgeklärt wurden.[305] Auch dies ist in Bezug auf autonom agierende Medizintechnik der Fall. Der Arzt ist dazu verpflichtet, den Patienten vor dem Einsatz des autonom agierenden Systems sachgerecht aufzuklären.[306] Zwar kann es dazu kommen, dass ein Arzt seine ihn treffenden Pflichten verletzt. In diesem Fall greift aber eine Haftung aus § 280 Abs. 1 BGB. Eine relevante Haftungslücke verbleibt mithin nicht, zumal es dem Arzt im Falle der Verletzung von Aufklärungspflichten nur im Ausnahmefall gelingen wird, sich zu exkulpieren.

---

[302] Dazu unter E. III. 4. b. (2) (b) (bb).
[303] Dazu unter D. III. und E. III. 4. b. (2) (b).
[304] Dazu unter D. III.
[305] Zu diesem Kriterium unter E. III. 4. b. (2) (b) (bb).
[306] Dazu oben unter II. 1. b. (2) (b).

(3) Ergebnis

Nach Auffassung der Arbeitsgruppe bedarf es – jedenfalls derzeit – keiner Gefährdungshaftung des Betreibers von autonom agierender Medizintechnik.

III. Herstellerhaftung

Beim Einsatz von autonomen Systemen, die nicht nur Entscheidungen des behandelnden Arztes umsetzen, sondern algorithmenbasierte eigene „Entscheidungen" treffen und dabei einen Schaden verursachen, ist die Zurechnung zum Behandler problematisch. Wenn ein Behandlungsfehler auftritt, stellt sich daher die Frage nach der Haftungsverteilung zwischen Hersteller und Arzt. Der Arzt wird nach Maßgabe der Ausführungen oben unter II. weiterhin in der Haftung für die Entscheidung bleiben, ob er das autonome System zur Behandlung des Patienten einsetzt, ob er das richtige autonome System für die Behandlung des Patienten ausgewählt hat und ob er mit der Behandlung durch das autonome System die richtige Methode angewandt hat.[307] Der Hersteller haftet für Mängel an Hard- und Software des autonomen Systems.[308] Hierbei wird zwischen der vertraglichen und der deliktischen Haftung zu unterscheiden sein.

1. Haftung aus Vertrag

Der Verkäufer von autonomen Systemen in der Medizintechnik haftet gegenüber seinem Vertragspartner, zumeist dem Träger eines Krankenhauses, für Fehler aus dem abgeschlossenen Vertrag. Für medizintechnische Produkte bestehen oftmals nicht nur bloße Kauf- oder Werkverträge, sondern es liegen längerfristige Vertragsverhältnisse vor, die eine Kombination aus Softwareherstellung und Softwarepflege umfassen. Sofern das Produkt unter die kaufrechtlichen Gewährleistungsvorschriften fällt, dürften insbesondere mangelbezogene Folgeschäden (§§ 437 Nr. 3, 280 Abs. 1 BGB) eine Rolle spielen. Hierfür wäre ein Vertretenmüssen des Verkäufers aus § 280 Abs. 1 BGB zu prüfen. Nach § 280 Abs. 1 S. 2 BGB ist eine Haftung des Schuldners ausgeschlossen, wenn er die Pflichtverletzung nicht zu vertreten hat. Insofern müsste der Geschädigte die Pflichtverletzung beweisen und der Verkäufer des autonomen Systems, dass es bei ihm an einem Vertretenmüssen fehlt. In diesem Rahmen ist eine Haftungsfreizeichnung möglich, soweit kein Vorsatz vorliegt oder eine Beschaffenheitsgarantie übernommen worden ist (§ 444 BGB). Eine weitere Haftungsfreizeichnung für Schäden, die nicht Leben, Körper oder Gesundheit betreffen, bei einer leicht fahrlässigen Pflichtverletzung ist zudem formularmäßig denkbar (Umkehrschluss aus § 309 Nr. 7 lit. b BGB). Inwieweit eine Freizeichnung für Mangelschäden im Einzelnen möglich ist oder ob der Ersatz für mangelbedingte Folge-

---

[307] *Dierks*, Wer haftet für Kollege Roboter?, KMA 2018, 33 (34).
[308] *Dierks*, Wer haftet für Kollege Roboter?, KMA 2018, 33 (35).

schäden ausgeschlossen werden kann, ist zwar umstritten, stellt aber kein spezifisches Problem der Anwendung von künstlicher Intelligenz dar, so dass an dieser Stelle nicht näher darauf eingegangen werden soll. Im Ergebnis kommen vertragliche Ansprüche aber nur zwischen dem Verkäufer des autonomen Systems und seinem Vertragspartner, meist dem Träger des Krankenhauses, in Betracht, die keine Besonderheiten gegenüber sonstigen vertraglichen Verhältnissen bieten.

Eine Haftung aus einem Vertrag mit Schutzwirkung zugunsten Dritter dürfte hingegen ausscheiden. Die Patienten sind typischerweise in den Schutzbereich des Vertrages zwischen dem Verkäufer und dem Arzt oder dem Krankenhausträger nicht einbezogen, da für den Verkäufer der Patientenkreis unabgrenzbar ist und damit zu nicht mehr überschaubaren Haftungsrisiken führen kann.[309]

2. Haftung aus Delikt

Im Bereich der Medizingerätetechnik ergeben sich für eine deliktische Haftung des Herstellers von autonomen Systemen ebenfalls keine Besonderheiten. Hier kommen insbesondere die Ansprüche nach § 823 Abs. 1 und Abs. 2 BGB sowie Ansprüche nach dem Produkthaftungsgesetz in Betracht.

a. Verschuldenshaftung

Bei der Verschuldenshaftung sind zuvorderst Ansprüche aus § 823 BGB zu prüfen; als direkter Anspruch über Abs. 1 und als Anspruch nach Abs. 2 wegen der Verletzung eines Schutzgesetzes, hier im Regelfall das Medizinproduktegesetz.

(1) § 823 Abs. 1 BGB

Soweit ein in der Medizintechnik eingesetztes autonomes System nur fehlerhaft oder gar nicht funktioniert, kann es zu Verletzungen der Rechtsgüter Leben, Körper und Gesundheit kommen, so dass der Anwendungsbereich des § 823 Abs. 1 BGB eröffnet ist. Die für die übliche Produzentenhaftung entwickelten Fehlerkategorien wie Konstruktions- und Fertigungsfehler lassen sich problemlos auf die Entwicklung und Fertigung von autonomen Systemen übertragen. Gleiches gilt für die Produktbeobachtungspflicht. Es lässt sich aber feststellen, dass es mit einem zunehmenden Grad an Automatisierung zu einer Verlagerung der Sorgfaltspflichten vom Arzt als Nutzer der autonomen Systeme zum Hersteller kommt, wobei sich die Auswahl-, Bedienungs- und Überwachungspflichten

---

[309] Vgl. Kullmann/Pfister/Stöhr/Spindler/*Spickhoff*, Produzentenhaftung, 02/17, Haftung für Medizinprodukte, S. 7.

des Nutzers teilweise qualitativ, teilweise quantitativ verändern, die Summe der Pflichten aber im Vergleich zum nicht autonomen System für den Nutzer sinkt.[310]

Für eine Haftung nach § 823 Abs. 1 BGB gelten die allgemeinen Grundsätze der Herstellerhaftung. Autonome Systeme müssen den im Zeitpunkt ihres Inverkehrbringens maßgeblichen Sicherheitsstandard einhalten und Gefahren berücksichtigen, die zu diesem Zeitpunkt bekannt oder erkennbar waren. Wie oben bereits dargestellt,[311] wird in diesem Rahmen zwischen Konstruktionsfehlern, Fabrikationsfehlern und Instruktionsfehlern unterschieden.[312] Weiterentwicklungen der Technik und neue Erkenntnisse, die nach diesem Zeitpunkt aufkommen, spielen für die Feststellung eines Produktfehlers keine Rolle.[313] Bei der Zulassung der Medizinprodukte müssen die Sicherheit und Wirksamkeit nachgewiesen werden. Die Messlatte ist hierbei der Stand der Wissenschaft und Technik.

(a) Konstruktionsfehler

Ein Konstruktionsfehler liegt vor, wenn das autonome System auch bei richtiger Umsetzung der Konstruktion für den gedachten Anwender ein Gefährdungspotential besitzt, das sich nach dem Stand der Wissenschaft und Technik konstruktiv hätte vermeiden lassen.[314] Den Hersteller trifft hierbei die Pflicht, alle Maßnahmen zu ergreifen, die erforderlich und zumutbar sind, um konkrete Gefahren zu vermeiden.[315] Für den Beurteilungsmaßstab, welche Konstruktionsmaßnahmen erforderlich und zumutbar sind, sind die Erwartungen der Nutzer und das Sicherheitsniveau des Produktes, das nach dem jeweiligen Erkenntnisstand von Wissenschaft und Technik möglich und zumutbar ist, maßgebend.[316] Für Medizinprodukte ist in Anhang I der europäischen Medizinprodukteverordnung (Medical Device Regulation - MDR)[317] in den grundlegenden Sicherheits- und Leistungsanforderungen ausdrücklich geregelt, dass der allgemein anerkannte Stand

---

[310] *Horner/Kaulartz*, Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (12/13).
[311] Siehe unter E. IV. 2. c.
[312] *Denga*, Warum die Verschuldenshaftung des BGB auch künftig die bessere Schadensausgleichsordnung bedeutet, CR 2018, 69 (71).
[313] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (750).
[314] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (110).
[315] BGH, Urt. v. 16.6.2009 - VI ZR 107/08, NJW 2009, 2952.
[316] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (110).
[317] Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates; siehe dazu unter Kapitel 1, G.

der Technik zugrunde zu legen ist.[318] Es muss durch technische und organisatorische Maßnahmen gewährleistet werden, dass weder auftretende Fehler, noch neu erlernte Funktionen zu Risiken führen, die diesem Maßstab widersprechen.[319] Nach 17.1 des Anhangs I der MDR sollen Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme, einschließlich Software, gehören, oder Produkte in Form einer Software so ausgelegt werden, dass Wiederholbarkeit, Zuverlässigkeit und Leistung entsprechend ihrer bestimmungsgemäßen Verwendung gewährleistet sind. Für den Fall des Erstauftretens eines Defekts sind geeignete Vorkehrungen zu treffen, um sich daraus ergebende Risiken oder Leistungsbeeinträchtigungen auszuschließen oder sie so weit wie möglich zu verringern. 17.2 des Anhangs I der MDR bestimmt, dass bei Produkten, zu deren Bestandteilen Software gehört, oder bei Produkten in Form einer Software die Software entsprechend dem Stand der Technik entwickelt und hergestellt werden soll, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements einschließlich der Informationssicherheit, der Verifizierung und der Validierung zu berücksichtigen sind.

Insbesondere ist zu beachten, dass im Bereich der Medizintechnik jedes neue Produkt zugelassen werden muss, bevor es in der Praxis eingesetzt werden darf. Für autonome Systeme muss nach Auskunft der von der Arbeitsgruppe angehörten Experten dazu der Algorithmus offengelegt und auch die diesem zugrundeliegenden Daten zur Verfügung gestellt werden, um eine Prüfung durchführen zu können. Von der Zulassungsstelle könne überprüft werden, wie das System zu seinen Entscheidungen gelange. Man sei abgesehen von den Pflichten des Medizinproduktegesetzes über die haftungsrechtliche Produktbeobachtungspflicht hinaus verpflichtet, erhebliche Probleme zu melden. Die Entscheidungsgrundlagen und -prozesse blieben so für die Zulassungsstelle nachvollziehbar.

Beim Einsatz von autonomen Systemen könnten in Bezug auf Haftungsfragen lediglich Probleme auftreten, wenn ein selbstlernendes System im Echtbetrieb eingesetzt würde. Dann könnte nämlich unter Umständen nicht mehr nachvollzogen werden, ob es sich bei einem Fehler um einen Konstruktionsfehler der ursprünglichen Programmierung handelt oder ob der Fehler im Betrieb des selbstlernenden Systems aufgetreten ist und wem dieser gegebenenfalls zuzurechnen wäre. Die von der Arbeitsgruppe angehörten Experten haben hierzu ausgeführt, dass momentan (soweit bekannt) kein selbstlernendes System im Krankenhaus eingesetzt werde, da die Zulassungsstelle das fertige Produkt erst freigeben müsse. Bei autonomen Systemen würden daher sämtliche Daten zu einem Paket zusammenfasst und der Zulassungsstelle zur Beurteilung vorgelegt.

---

[318] Vgl. dazu Fn. 67.
[319] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (110).

Diese habe sodann zu prüfen, ob die Anwendung sicher und effizient sei. Weder die Hersteller noch die Regulierer beabsichtigten, dieses Verfahren in naher Zukunft anders auszugestalten.

Soweit es also weiter eindeutig zuordenbar bleibt, aufgrund welcher Datenbasis das autonome System wie handelt, treten auch bei der Zuordnung von potentiellen Konstruktionsfehlern zum Hersteller keine strukturell neuen Probleme auf. Diese könnten sich erst beim Einsatz von in der medizinischen Anwendung selbstlernenden Systemen ergeben. Ein solcher ist aber noch nicht absehbar.

(b) Fabrikationsfehler

Von einem Fabrikationsfehler wird gesprochen, wenn das Produkt zwar fehlerfrei konzipiert ist, es jedoch im Fertigungsprozess zu einer planwidrigen Abweichung von der vom Hersteller vorgesehenen Soll-Beschaffenheit kommt.[320] Für die Hersteller von autonomen Systemen in der Medizintechnik ergeben sich auch hier keine Besonderheiten zu den Haftungsfragen anderer Produkte. Wie oben bereits beschrieben,[321] kommen bei Produkten mit integrierter Software Fabrikationsfehler insbesondere in Betracht, wenn bei der Übertragung des Programms von einem auf einen anderen Speicherort Fehler erzeugt werden oder sich Schadprogramme einschleichen.[322] Haftungsrechtliche Besonderheiten ergeben sich daraus nicht. Die möglichen Fehlerquellen bleiben vom Prinzip her zuordenbar.

(c) Instruktionsfehler

Es gehört zu den Gefahrabwendungspflichten des Herstellers, auf die Risiken eines Produkts hinzuweisen und dem Endabnehmer eine Anleitung für die risikolose Benutzung zu geben.[323] Ein Instruktionsfehler liegt bei mangelhaften Gebrauchsanweisungen oder nicht ausreichenden Warnungen vor Gefahr bringenden Eigenschaften des an sich fehlerlosen Produkts vor.[324] Für Medizinprodukte gibt es diesbezüglich eindeutige Vorgaben: Gemäß Anhang I Kapitel III der MDR müssen jedem medizinischen Produkt die notwendigen Angaben beigefügt werden, die die Identifizierung des Produkts und des Herstellers ermöglichen, sowie alle für den Anwender oder gegebenenfalls dritte Personen relevanten Informationen über die Sicherheit und Leistung des Produkts. Der Hersteller

---

[320] Staudinger/*Hager*, BGB, Bearb. 2016, § 823 Rn. F 17.
[321] Siehe unter E. IV. 2. c. (2).
[322] *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (78).
[323] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (110).
[324] *Lutz/Tang/Lienkamp*, Die rechtliche Situation von teleoperierten und autonomen Fahrzeugen, NZV 2013, 57 (61).

muss den Produktabnehmer mithin stets über den richtigen Gebrauch seines Gerätes vor der Inbetriebnahme instruieren.

Hieraus entstehen für autonome Systeme auf Herstellerseite Instruktionspflichten gegenüber den Ärzten als Anwender. Zu berücksichtigen ist, dass einerseits solche Instruktionspflichten reduziert sein können, da es sich bei den anwendenden Ärzten um professionelle Nutzer handelt. Andererseits ist zu beachten, dass Ärzte nicht stets über IT-Kenntnisse verfügen müssen.[325] Besonderheiten für autonome Systeme ergeben sich aber nicht.

Eine Problematik könnte sich höchstens ergeben, wenn die autonomen Systeme mit anderen vom Arzt eingesetzten Systemen interagieren sollen. Für das Zusammenspiel verschiedener Produkte kann aber auf den allgemeinen Grundsatz zurückgegriffen werden, dass der Hersteller grundsätzlich nur für diejenigen Gefahren die Verantwortung zeichnet, die er selbst geschaffen hat. Daher dürfte es ausreichen, wenn er den Arzt als den Produktbenutzer dahingehend aufklärt, dass dieser nur vom Hersteller freigegebene oder als unbedenklich eingestufte Zubehörteile gefahrlos nutzen kann und dass die Benutzung von nicht autorisiertem Zubehör auf dessen eigene Verantwortung erfolgt.[326]

(d) Produktbeobachtungspflichten

Auch nach Inverkehrbringen eines Produkts wird der Hersteller nicht vollständig von seiner Verantwortung frei. Er muss sein Produkt auch weiter auf noch nicht bekannte schädliche Eigenschaften hin beobachten und sich über sonstige, eine Gefahrenlage schaffende Verwendungsfolgen informieren.[327] Daher muss er bei Kenntnis von Schäden durch das Produkt die zu diesem Zeitpunkt erforderlichen und ihm zumutbaren Gefahrenabwehrmaßnahmen ergreifen.[328] Hinsichtlich autonomer Systeme und ihrer Subkomponenten, gerade im medizinischen Bereich, dürften sich bereits angesichts deren Komplexität ausgeprägte Produktbeobachtungspflichten der Hersteller ergeben; hierzu eröffnet die fortschreitende Vernetzung derartiger Produkte dem Hersteller völlig neue Möglichkeiten der Produktbeobachtung.[329]

---

[325] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (769).
[326] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (770).
[327] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (111).
[328] *Spindler*, Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (769).
[329] *Gomille*, Herstellerhaftung für automatisierte Fahrzeuge, JZ 2016, 76 (80).

Diese Vernetzungsfähigkeit birgt aber auch die Gefahr, dass durch die zahllosen Kombinationsmöglichkeiten mit anderen (Alltags)Geräten, die weder vom Medizinproduktehersteller hergestellt wurden, noch die er überhaupt kennt, die strengen Anforderungen an die Konformität der Medizinprodukte nicht eingehalten werden und es zu negativen Auswirkungen auf die Wirkungsweise des autonomen Systems kommen kann.[330] Aufgrund der geltenden Rechtsprechung zu Produktbeobachtungspflichten für fremdes Zubehör[331] könnten sich Probleme in der Praxis ergeben, die sich durch Hersteller nicht mehr lösen lassen. Hier muss im Rahmen der Instruktionspflichten des Herstellers mithin eine Anweisung an den Anwender erfolgen, dass nur vom Hersteller freigegebenes Zubehör in Kombination mit dem autonomen System verwendet werden darf (s.o.). Sollte hiergegen verstoßen werden, ergeben sich bei der Zuweisung einer Haftung keine Besonderheiten.

Ferner ist es offensichtlich, dass beim Einsatz komplexer IT-Systeme aus dem Wissen der Unvermeidbarkeit von Programmierungsfehlern („Bugs“) eine Pflicht des Herstellers zur sorgfältigen Produktbeobachtung erwächst.[332] Dies hat auch die durch die Arbeitsgruppe durchgeführte Expertenanhörung bestätigt. Die für autonome Systeme existierenden Produktbeobachtungspflichten seien insgesamt aber nicht anders zu bewerten als für herkömmliche Produkte. Eine Produktbeobachtung der autonomen Systeme sei nach Auskunft der Experten daher im normalen Qualitätsprozess enthalten. Man könne hierzu Lerndatensätze und Validierungsdatensätze schaffen, um im Rahmen der Qualitätssicherung die Güte von Algorithmen zu beurteilen.

(e) Rückrufpflichten

Wie oben dargestellt[333], ist noch nicht abschließend geklärt , ob mit der Rückrufpflicht eines Produktes auch die Pflicht zur kostenlosen Beseitigung der Gefahr einhergeht.[334]

---

[330] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (111).

[331] Nach der Rechtsprechung des BGH kann den Hersteller eine Pflicht zur Produktbeobachtung auch treffen, um rechtzeitig Gefahren aufzudecken, die aus der Kombinierung seines Produkts mit Produkten anderer Hersteller entstehen können, und ihnen entgegenzuwirken (BGH, Urt. v. 9.12.1986 - VI ZR 65/86, BGHZ 99,167 - Honda).

[332] *Spindler*, Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (769).

[333] Unter E. IV. 2. d.

[334] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (770) m.w.N.; *Horner/Kaulartz*, Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (12), sprechen sich zum Beispiel für eine Rückrufpflicht aus.

Um dem Integritätsinteresse des Kunden Genüge zu tun, genügt es grundsätzlich, dass der Kunde gewarnt wird, so dass er das Produkt nicht mehr benutzt. Eine Pflicht für den Hersteller, dass das autonome System und dessen Software stets gepflegt und aktualisiert werden, lässt sich aus dem Produkthaftungsrecht nicht ableiten.[335]

Im Bereich der Medizinprodukte ließe sich eine andere Auffassung für Produkte vertreten, bei denen Warnungen oder Aufforderungen zur Nichtbenutzung oder Stilllegung zur effektiven Gefahrenabwehr nicht ausreichen, da sie zum Beispiel implantiert sind und deshalb nicht einfach unbenutzt bleiben können oder bei denen die Fehlerbehebung für den Hersteller ohne großen Aufwand erfolgen kann.[336] Letztlich trifft die geschilderte Problematik nur auf die Fälle zu, in denen keine weitergehenden Wartungs- oder Aktualisierungsverträge abgeschlossen worden sind. Dies wird auf autonome Systeme oftmals nicht zutreffen, so dass die Problematik eher auf vertraglicher Ebene eine Rolle spielen wird. Unlösbare Haftungsfragen werden dadurch nicht aufgeworfen.

(f) Beweislast

Die von der Rechtsprechung entwickelten Regeln zur Beweislastumkehr zugunsten des Geschädigten im Rahmen der Produkthaftung greifen naturgemäß auch bei der deliktischen Haftung für autonome Systeme in der Medizintechnik ein, da der Geschädigte nicht über hinreichende Einsichtsmöglichkeiten in die Vorgänge in der Sphäre des Schädigers verfügt.[337] Auch hier ergeben sich keine Besonderheiten bei den autonomen Systemen im Rahmen der Medizintechnik.[338]

Dem Geschädigten obliegt der Beweis der Rechtsgutsverletzung, des Produktfehlers sowie der Nachweis, dass der Produktfehler im Organisationsbereich des Herstellers entstanden ist und bereits im Zeitpunkt des Inverkehrbringens vorlag.

---

[335] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (770); *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (111).

[336] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (111).

[337] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (771).

[338] *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (113), vertritt zwar die Auffassung, dass sich ein Produktfehler beim Einsatz intelligenter Medizinprodukte kaum nachweisen lasse, da deren Entscheidungsvorgänge intransparent seien und dadurch eine nachträgliche Überprüfung der maschinellen Aktion nicht möglich sei. Sie verkennt dabei aber, dass auf absehbare Zeit keine selbstlernenden Medizinprodukte zugelassen werden, so dass eine Zuordnung des Produktfehlers zum Hersteller oder Anwender des Produkts weiterhin möglich bleibt.

Anknüpfungspunkte der Haftung sind die Pflichtverletzung und das Verschulden. Von besonderer praktischer Bedeutung ist dabei die Frage, ob der Schädiger fahrlässig gehandelt hat. Fahrlässigkeit (§ 276 Abs. 2 BGB) setzt voraus, dass ein bestimmtes schadensauslösendes Ereignis bei Anwendung pflichtgemäßer Sorgfalt voraussehbar und vermeidbar gewesen wäre. Hinsichtlich der objektiven Pflichtverletzung als auch des Verschuldens greift zugunsten des Geschädigten eine Beweislastumkehr ein, wonach sich der Hersteller in Bezug auf alle seine Hilfskräfte zu entlasten hat.[339] *Wagner*[340] weist darauf hin, dass sich der Hersteller eines fehlerhaften Produktes de facto nicht auf ein mangelndes Verschulden berufen könne; wenn er kein fehlerhaftes Produkt in den Verkehr gebracht hätte, hätte er die im Verkehr erforderliche Sorgfalt eingehalten. In jedem Fall erscheint es, wie hinsichtlich des das autonome System anwendenden Arztes auch,[341] nicht geboten, dem Hersteller von autonomen Systemen generell die Möglichkeit zu nehmen, sich in diesem Bereich der Medizintechnik zu exkulpieren.

(g) Kausalität

Auch die Frage der Kausalität, ob nun der aufgetretene Schaden auf einer fehlerhaften Anwendung des Arztes, einer fehlerhaften Programmierung oder einer Fehlfunktion des autonomen Systems beruht, wirft keine neuen Fragen auf. Dies sind im Ergebnis Fragen des Regresses. Gegenüber dem primär Geschädigten bleiben der Vertragspartner des Patienten und der Hersteller des autonomen Systems in der Haftung, soweit eine Störung des autonomen Systems nachweisbar ist.

Soweit die Haftung des Herstellers des autonomen Systems oder des Arztes als Nutzer in Betracht kommt, indes unklar ist, welches Verhalten beider potentieller Anspruchsgegner den Schaden wirklich verursacht hat, könnte eine Zurechnung über § 830 Abs. 1 Satz 2 BGB erfolgen, soweit bei jedem der beiden möglichen Anspruchsgegner ein anspruchsbegründendes Verhalten vorliegt und nur die konkrete Zurechnung unaufklärbar bleibt.[342]

(2) § 823 Abs. 2 BGB

Bei fehlerhaften Medizinprodukten mit Softwaresteuerung (§ 3 Nr. 1 MPG) können die Vorschriften des MPG als Schutzgesetz des § 823 Abs. 2 BGB zur

---

[339] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (772).
[340] *Wagner*, Produkthaftung für autonome Systeme, AcP 217, 707 (712).
[341] Unter II. 1. c.
[342] *Horner/Kaulartz*, Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (9/10).

Anwendung gelangen.[343] Hierbei wird man sich zwar nicht auf § 1 MPG stützen können, da die Vorschrift kein Schutzgesetz i.S.d. § 823 Abs. 2 BGB ist. Die „Sicherheit, Eignung und Leistung" der Medizinprodukte wird daher vor allem über § 4 MPG gesichert, also durch die medizinprodukterechtliche Generalklausel.[344]

Ausfüllungsbedürftig ist bei § 4 MPG insbesondere der „begründete Verdacht einer Gefährdung". Maßgeblich ist hierbei die Wahrscheinlichkeit des Schadenseintritts. Rechtlich relevant ist der Sachverhalt, wenn die Möglichkeit des Eintritts einer nicht nur geringfügigen nachteiligen Einwirkung auf ein rechtliches Schutzgut besteht, soweit die Einwirkung nicht praktisch ausgeschlossen ist. Begründet ist der Verdacht somit, wenn konkrete Anhaltspunkte dafür vorliegen, dass von einem Medizinprodukt eine Gefahr für Patienten, Anwender oder Dritte ausgeht. Die Anforderungen an die Wahrscheinlichkeit des Eintritts einer Schädigung sind bei § 4 Abs. 1 Nr. 1 MPG umso geringer anzusetzen, je schwerwiegender sich die eintretende Gefahr auswirken kann.[345] Dieser von § 4 Abs. 1 Nr. 1 MPG als Schutzgesetz aufgestellte Prüfungsmaßstab wirft für die Frage der Anwendung von autonomen Systemen gegenüber den herkömmlichen Medizinprodukten keine Besonderheiten auf.

b. Gefährdungshaftung nach Produkthaftungsgesetz

Geht es um eine mögliche Haftung des Herstellers nach dem ProdHaftG, so knüpft diese an einen Fehler der Sache an. Der Hersteller haftet dann nicht, wenn das Produkt fehlerfrei ist. Dies gilt nach den obigen Ausführungen, auf die Bezug genommen wird, auch für autonome Systeme. Angesichts der Entscheidung des Betreibers über den Einsatz des Systems veranlasst allein er die ggf. spezifisch mit der Autonomie des Systems einhergehende Gefahr.

Im Gegensatz zu der in § 84 AMG spezialgesetzlich geregelten Arzneimittelhaftung enthält das 1995 eingeführte Medizinproduktegesetz (MPG) keine spezifischen zivilrechtlichen Haftungsregelungen[346]. Die Haftung des Herstellers richtet sich - von vertragsrechtlichen Schadensersatzansprüchen abgesehen - im Wesentlichen nach § 823 Abs. 1 BGB und § 1 ProdHaftG. Dabei ist die Haftung nach dem Produkthaftungsgesetz faktisch aufgewertet worden, seitdem durch die im Jahr 2002 erfolgte Neufassung von § 253 Abs. 2 BGB ein Anspruch auf

---

[343] *Spindler,* Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (772).
[344] *Bergmann/Pauge/Steinmeyer*, Gesamtes Medizinrecht, 2018, MPG § 1 Rn. 1-3, beck-online.
[345] *Bergmann/Pauge/Steinmeyer*, Gesamtes Medizinrecht, MPG § 4 Rn. 4, beck-online.
[346] *Dahm-Loraing/Koyuncu,* Haftung für Medizinprodukte - Teil 1: Haftung des Herstellers nach dem ProdHaftG, Phi - 3/2010, 108.

Schmerzensgeld nicht mehr nur auf der deliktsrechtlichen Ebene, sondern auch im Falle einer Haftung nach dem Produkthaftungsgesetz zuerkannt werden kann.[347]

Die zivilrechtliche Verantwortlichkeit des Herstellers und des Inverkehrbringers von Medizinprodukten ist nicht dadurch ausgeschlossen, dass ein Produkt vor der Inverkehrgabe die nach MPG geforderte Konformitätsbewertung durchlaufen hat. Vielmehr stellt § 6 Abs. 4 MPG klar, dass die Durchführung dieses Verfahrens die zivil- und strafrechtliche Verantwortlichkeit des Verantwortlichen für das erstmalige Inverkehrbringen unberührt lässt.

Es ist nunmehr zu überprüfen, ob und inwieweit die Regeln der Produkthaftung auch für autonome Systeme im Bereich der Medizintechnik hinreichend sind.

(1) Produkt im Sinne der Produkthaftungsrichtlinie

Autonome Medizinprodukte sind unter den Produktbegriff der ProdHaftRL und des ProdHaftG zu fassen. Unter den Ausnahmetatbestand des Art. 13 ProdHaftRL fällt nur das Arzneimittelrecht nach dem AMG. Danach werden „Ansprüche, die ein Geschädigter (…) aufgrund einer zum Zeitpunkt der Bekanntgabe der Richtlinie bestehenden besonderen Haftungsregelung geltend machen kann, durch diese Richtlinie nicht berührt". Aus dem 13. Erwägungsgrund zur ProdHaftRL wird deutlich, dass das deutsche Arzneimittelhaftungsrecht eine solche „besondere Haftungsregelung" darstellt. Dort heißt es: „Soweit in einem Mitgliedstaat ein wirksamer Verbraucherschutz im Arzneimittelbereich auch bereits durch eine besondere Haftungsregelung gewährleistet ist, müssen Klagen aufgrund dieser Regelung ebenfalls weiterhin möglich sein." Das Arzneimittelhaftungsrecht in Deutschland war die einzige „besondere Haftungsregelung", die zum Zeitpunkt der Bekanntgabe der Richtlinie in den Mitgliedstaaten bestand. Grund für die Aufnahme des besagten Passus' in Art. 13 ProdHaftRL war die Weigerung der damaligen deutschen Bundesregierung, der Richtlinie zuzustimmen, wenn dies eine Anpassung oder gar Aufhebung des erst 1976 neu eingeführten deutschen Arzneimittelhaftungsrechts erforderlich gemacht hätte. Um den deutschen Interessen entgegen zu kommen, bestimmt Art. 13 ProdHaftRL daher, dass eine Haftung nach deutschem Arzneimittelrecht von der ProdHaftRL zunächst unberührt bleibt.

Art. 13 ProdHaftRL wird durch § 15 Abs. 1 ProdHaftG umgesetzt. Die deutsche Umsetzungsnorm schreibt vor, dass die Bestimmungen des ProdHaftG nicht anzuwenden sind, wenn jemand durch ein Arzneimittel geschädigt wird, das in den Anwendungsbereich der Arzneimittelhaftung fällt. § 15 Abs. 1 ProdHaftG statu-

---

[347] *Knoche,* Haftung für Medizinprodukte: Beweisrechtliche Fragen, VersR 2005, 1614.

iert daher ein Exklusivitätsverhältnis zwischen Produkt- und Arzneimittelhaftungsrecht.[348] Dieses Exklusivitätsverhältnis stellt entgegen einigen Stimmen in der Literatur keinen Verstoß gegen Art. 13 ProdHaftRL dar. Vielmehr ist von einer Richtlinienvereinbarkeit des § 15 Abs. 1 ProdHaftG auszugehen.[349]

Das Medizinprodukterecht unterfällt nicht dem Ausnahmetatbestand.

(2) Fehlerbegriff

Wie bereits ausführlich dargestellt, ist wesentliche Haftungsvoraussetzung der verschuldensunabhängigen Haftung nach dem ProdHaftG das Vorliegen eines Fehlers.
Bei der Beurteilung des in § 3 ProdHaftG definierten Fehlerbegriffs ist auf die objektiv berechtigte Sicherheitserwartung abzustellen. Es kommt daher darauf an, ob das Produkt diejenige Sicherheit bietet, die die Allgemeinheit nach der Verkehrsauffassung in dem entsprechenden Bereich für erforderlich hält. Damit ist der Benutzerstandard nach dem Kenntnisstand der in Frage kommenden Benutzer zu bestimmen. Maßgeblich sind die Sicherheitserwartungen desjenigen Personenkreises, an den sich der Produkthersteller mit seinem Produkt richtet. Bei Medizinprodukten ist daher zu differenzieren, ob das Produkt für die Benutzung durch Fachkreise (z.B. Ärzte) und andere professionelle Abnehmer bestimmt ist oder ob es (auch) von Endverbrauchern benutzt werden wird. Diese beiden Personengruppen haben naturgemäß einen unterschiedlichen Erfahrungs- und Wissenstand und damit unterschiedliche Sicherheitserwartungen. Für Patienten, d.h. Endverbraucher, bestimmte Medizinprodukte müssen höheren Sicherheitsanforderungen genügen, um auf das Wissen und Gefahrsteuerungspotenzial dieses Personenkreises Rücksicht zu nehmen.[350]

Allgemein folgt daraus, dass bei Medizinprodukten wegen ihres gesundheitsbezogenen Verwendungszwecks von grundsätzlich hohen Sicherheitserwartungen auszugehen ist. Die Allgemeinheit und insbesondere Patienten und Ärzte erwarten von Medizinprodukten, dass sie keine unvertretbaren Gefahren aufweisen. Dies entspricht im Übrigen auch dem Mindestsicherheitsstandard für Medizinprodukte, wie er explizit in § 4 Abs. 1 Nr. 1 MPG niedergelegt ist.[351]

Gem. § 3 ProdHaftG sind bei der Beurteilung des unbestimmten Rechtsbegriffs „Fehler“ im Sinne des ProdHaftG die Darbietung des Produkts durch den Her-

---

[348] Vgl. BeckOGK/*Franzki*, Stand: 1.7.2018, AMG, § 84 Rn. 9.
[349] Vgl. BeckOGK/*Franzki*, Stand: 1.7.2018, AMG, § 84 Rn. 9 u 10.
[350] Vgl. *Dahm-Loraing/Koyuncu,* Haftung für Medizinprodukte - Teil 1: Haftung des Herstellers nach dem ProdHaftG, Phi - 3/2010, 108 (110).
[351] Vgl. *Dahm-Loraing/Koyuncu,* Haftung für Medizinprodukte - Teil 1: Haftung des Herstellers nach dem ProdHaftG, Phi - 3/2010, 108 (110).

steller, der Gebrauch, mit dem billigerweise gerechnet werden kann sowie der Zeitpunkt des Inverkehrbringens des Produkts als Maßstab heranzuziehen.
Ferner sind hierfür sonstige Umstände, wie z.B. Kriterien, die von der Eigenart des Produkts abhängen oder mit der Erkrankung zusammenhängen, von Relevanz.[352]

Insoweit ist eine richtungsweisende Entscheidung des EuGH nach Vorlagen des BGH[353] bedeutend. Die erste Vorlagefrage des BGH knüpfte an den Fehlerbegriff an und stellte darauf ab, ob ein Produkt, wenn es sich um ein in den menschlichen Körper implantiertes Medizinprodukt handelt, bereits dann fehlerhaft ist, wenn Geräte derselben Produktgruppe „ein nennenswert erhöhtes Ausfallrisiko haben" bzw. „wenn bei einer signifikanten Anzahl von Geräten derselben Serie eine Fehlfunktion aufgetreten" ist, ein Fehler des im konkreten Fall implantierten Gerätes aber nicht festgestellt ist. Zur Konkretisierung der für den Fehlerbegriff relevanten Bewertung der „berechtigen Sicherheitserwartungen" nimmt der EuGH eine zweifache Differenzierung vor, wonach es erstens auf den „Verwendungszweck und die objektiven Merkmale und Eigenschaften des in Rede stehenden Produkts" sowie zweitens auf „die Besonderheiten der Benutzergruppe, für die es bestimmt ist", ankomme. [354] Dies führte in dem konkreten Fall, bei dem es um Herzschrittmacher und Defibrillatoren ging, dazu, dass die „berechtigten Sicherheitserwartungen" in „Anbetracht ihrer [der Geräte] Funktion und der Situation besonderer Verletzlichkeit der diese Geräte nutzenden Personen" sowie auf Grund der „anormalen Potenzialität des Personenschadens, der durch sie verursacht werden könne", als „besonders hoch" eingeschätzt wurden.[355] Im Ergebnis musste ein Fehler des konkreten Produkts daher nicht mehr festgestellt werden. Es reichte für die Annahme eines Fehlers aus, dass ein potenzieller Fehler festgestellt wurde.

Die Auslegung des EuGH ist nach überwiegender Auffassung in der Literatur mit Wortlaut und Zweck der ProdHaftRL vereinbar.[356]

Fraglich ist, ob und inwieweit das Urteil des EuGH auf andere Produkte bzw. Produktkategorien - also z.B. auch autonome Medizinprodukte - übertragbar ist.
Bei genauer Betrachtung wird deutlich, dass auch die allgemeinbezogenen Aussagen des Urteils in einem spezifischen Kontext ergangen sind und nicht ohne Weiteres auf anders gelagerte Fälle übertragbar sind. Wann bei anderen Produk-

---

[352] Vgl. im Detail die Ausführungen bei *Dahm-Loraing/Koyuncu,* Haftung für Medizinprodukte - Teil 1: Haftung des Herstellers nach dem ProdHaftG, Phi - 3/2010, 108 (111 ff.).
[353] BGH, EuGH-Vorlage v. 30.7.2018 - VI ZR 284/12 -, VersR 2013, 1451.
[354] EuGH, Urt. v. 5.3.2015 – C-503/13 und C-504/13 –, NJW 2015, 1163.
[355] EuGH, Urt. v. 5.3.2015 – C-503/13 und C-504/13 –, NJW 2015, 1163.
[356] Vgl. *Timke*, Erhöhtes Ausfallrisiko von Medizinprodukten als Produktfehler, NJW 2015, 3060 (3062).

ten ein erhöhtes Ausfallrisiko zu einem Fehler führt, bleibt somit letztlich eine von den Besonderheiten des Einzelfalles abhängige Wertungsfrage. Denn der Entscheidung des EuGH sind Kriterien, unter welchen Voraussetzungen dieser Fehlerbegriff auch für andere (Medizin-)Produkte gilt, nicht zu entnehmen, insbesondere weil der EuGH den Begriff der „anormalen Potenzialität eines Personenschadens" nicht näher konkretisiert. Dieses Kriterium impliziert zumindest, dass die drohenden Schäden deutlich über ein normales Schadensausmaß hinausgehen müssen. Diese Bewertung kann bei anderen Produkten durchaus anders ausfallen, wenn „nur" eine Gesundheitsbeeinträchtigung, nicht aber Lebensgefahr droht: Je geringer die zu befürchtenden Schäden sind, umso höhere Ausfallquoten wird man verlangen müssen, um einen Produktfehler bei anderen Produkten annehmen zu können.[357]

Teilweise wird jedoch in der Literatur vertreten, dass die Entscheidung des EuGH auf sogenannte mhealth-Produkte, d.h. Produkte, bei denen IT und Medizin in mobilen Geräten verknüpft sind (z.B. blutzuckermessende Kontaktlinsen für Diabetiker), übertragbar sei. Insofern sei bereits ausreichend, dass die Datenübermittlungstechnik fehlerverdächtig sei. Beispielsweise würden die an Diabetes erkrankten Nutzer der Kontaktlinse präzise und aktuelle Informationen über ihren Blutzuckerspiegel erwarten und dürften daher mit Recht hohe Ansprüche an die Zuverlässigkeit des Messgeräts stellen. Denn dessen Ausfall könnte potenziell tödliche Konsequenzen haben. Außerdem sollte eine Verschiebung medizinischer Leistungen hin zu einem Mehr an Automatisierung nicht zu einer Verschlechterung von Patientenrechten führen. Angesichts dessen würde ein bloßer Fehlerverdacht bei einer Produktionsserie der Kontaktlinse ausreichen, um diese als fehlerhaft anzusehen.[358]

Aus Sicht der Arbeitsgruppe kann aber mit Blick auf autonome Medizinprodukte nicht grundsätzlich eine Übertragbarkeit der Entscheidung angenommen werden. Selbst unter der Annahme, dass autonome Medizinprodukte aufgrund ihrer besonderen Eigenarten ggf. ein höheres Schadenspotenzial aufweisen (etwa weil sie aufgrund einer fehlerhaften Programmierung in einer Vielzahl von Fällen zu nicht korrekten Diagnosen gelangen), bedarf es einer Bewertung im Einzelfall, ob die Entscheidung des EuGH Anwendung finden kann. Allein mit der Autonomie eines Medizinprodukts lassen sich die vom EuGH aufgestellten Kriterien jedenfalls nicht begründen. Es kommt vielmehr auf die Eigenart des jeweiligen Produktes an. Die Entscheidung im Einzelfall kann der Rechtsprechung überlassen werden.

---

[357] *Timke*, Erhöhtes Ausfallrisiko von Medizinprodukten als Produktfehler, NJW 2015, 3060 (3063, 3064).

[358] Vgl. dazu *Ortner/Daubenbüchel,* Medizinprodukte 4.0 - Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918 (2922).

(3) Haftender

Haftender nach dem Produkthaftungsgesetz ist der Hersteller des Produkts. Hersteller ist gemäß § 4 ProdHaftG, wer das Endprodukt, einen Grundstoff oder ein Teilprodukt hergestellt hat. Als Hersteller gilt auch jeder, der sich durch das Anbringen seines Namens, seiner Marke oder eines anderen unterscheidungskräftigen Kennzeichens als Hersteller ausgibt. Im Arzneimittelgesetz (§ 84 AMG) ist verantwortlich für den durch einen Entwicklungs-, Herstellungs- oder Instruktionsfehler entstehenden Schaden der pharmazeutische Unternehmer. Bei diesem muss es sich nicht notwendigerweise um den Hersteller des Arzneimittels handeln. Vielmehr ist dies der Inhaber der Zulassung oder Registrierung, aber auch derjenige, der das Arzneimittel in Verkehr bringt und durch die Angabe seines Namens oder in sonstiger Weise kundtut, dass er die Verantwortung für das Inverkehrbringen trägt.
Diese Besonderheit des Arzneimittelrechts ist indes nicht auf das Produkthaftungsrecht betreffend Medizinprodukte zu übertragen. Eine Konkretisierung oder gar Einschränkung des Kreises der haftenden Personen ist - auch mit Blick auf autonome Systeme - nicht veranlasst. Maßstab für die Einordnung als Haftender muss der Gesichtspunkt sein, wer für das Inverkehrbringen des Produkts verantwortlich ist. Dies ist im Arzneimittelbereich der pharmazeutische Unternehmer, der unabhängig vom Herstellungsprozess ein Arzneimittel unter seinem Namen in Verkehr bringt. Im Bereich des Produkthaftungsrechts ist dies wie dargestellt der Hersteller im Sinne des Produkthaftungsgesetzes. Es ist zudem darauf hinzuweisen, dass der Kreis der Haftpflichtigen im AMG zwar auf den pharmazeutischen Unternehmer begrenzt wird. Dies hindert jedoch bei Vorliegen der entsprechenden Voraussetzungen weder die Inanspruchnahme des Herstellers nach §§ 823 ff. BGB noch die Haftung des Herstellers im Innenverhältnis zum pharmazeutischen Unternehmer, falls der Hersteller für die Fehlerhaftigkeit des Arzneimittels verantwortlich ist.[359]

(4) Exkurs: Erprobungsphase

Es ist umstritten, ob der Produkthersteller (auch) während der Erprobungsphase eines Medizinprodukts gegenüber den Probanden verschuldensunabhängig nach dem ProdHaftG haftet. Dessen § 1 Abs. 2 Nr. 1 fordert, dass das Produkt in den Verkehr gebracht worden ist. Nach § 3 Nr. 11 Buchst. a MPG gilt indes die Abgabe von Medizinprodukten zum Zwecke der klinischen Prüfung nicht als Inverkehrbringen. Es wird teilweise argumentiert, dass der Begriff des Inverkehrbringens nach dem ProdHaftG ein anderer sei als der des MPG.[360] Dem ist indes

---

[359] *Rehmann*, AMG, § 84, Rn. 2.
[360] *Koyuncu,* Die klinische Prüfung von Medizinprodukten - Rechtlicher Rahmen, Grundlagen und Haftungsgefüge, MPR 2006, 29 (33 f.).

nicht zu folgen.[361] Denn der Hersteller begibt sich gerade nicht willentlich der tatsächlichen Herrschaft des Produkts. Das Erprobungsverfahren unterliegt vielmehr einem rechtlichen Sonderregime.[362] Zudem sind die Probanden einer Studie nach dem MPG, die ihre Einwilligung jederzeit widerrufen können und die in aller Regel für ein nicht geringes Entgelt tätig werden, nicht so schutzbedürftig wie die Käufer eines gewöhnlichen Produkts, so dass der Schutzzweck des ProdHaftG dessen Anwendbarkeit nicht erfordert.[363] Diese Grundsätze dürften nicht nur für althergebrachte Medizinprodukte gelten, sondern ebenso für autonome Systeme.

(5) Haftungsausschlussgründe

Wie oben bereits dargestellt, sieht das Produkthaftungsgesetz in § 1 Abs. 2 Haftungsausschlussgründe vor, deren Vorliegen eine Ersatzpflicht des Herstellers ausschließt. Der in der Praxis häufig zu Auslegungsschwierigkeiten führende Haftungsausschlussgrund für Entwicklungsrisiken ist in § 1 Abs. 2 Nr. 5 ProdHaftG gesetzlich verankert. Danach sind Produktfehler, die nach dem Stand von Wissenschaft und Technik zum Zeitpunkt des Inverkehrbringens nicht als solche erkennbar waren, von der verschuldensunabhängigen Haftung nach dem ProdHaftG ausgenommen. Ob der Haftungsausschluss auch für nachträglich auftretende Fehler gilt, die auf der Lernfähigkeit von Algorithmen beruhen, ist, wie oben dargestellt, umstritten.[364] In jedem Fall ist zu berücksichtigen, dass der Hersteller verschuldensabhängig nach § 823 Abs. 1 BGB wegen Verletzung von Produktbeobachtungspflichten haften kann, wenn ein ursprünglich nicht erkennbarer Fehler später erkennbar wird und der Hersteller trotz entsprechender Gefährdungslage nicht reagiert.[365]

Der Medizinproduktehersteller ist durch den Haftungsausschlussgrund nach § 1 Abs. 2 Nr. 5 ProdHaftG gegenüber dem Arzneimittelhersteller erheblich privilegiert, da der pharmazeutische Unternehmer nach § 84 AMG gerade auch für Entwicklungsfehler haftet.[366] Es ist fraglich, ob und inwieweit diese Privilegierung gerechtfertigt bzw. geboten ist. Diese Frage spitzt sich angesichts fort-

---

[361] Vgl. *Ortner/Daubenbüchel,* Medizinprodukte 4.0 - Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918 (2921 f.).
[362] Vgl. zu den Einzelheiten insoweit *Ortner/Daubenbüchel,* Medizinprodukte 4.0 - Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918 (2921 f.).
[363] *Ortner/Daubenbüchel,* Medizinprodukte 4.0 - Haftung, Datenschutz, IT-Sicherheit, NJW 2016, 2918 (2922).
[364] Siehe oben unter E. IV. 2. e.
[365] *Dahm-Loraing/Koyuncu,* Haftung für Medizinprodukte - Teil 1: Haftung des Herstellers nach dem ProdHaftG, Phi - 3/2010, 108 (115 f.).
[366] *Dahm-Loraing/Koyuncu,* Haftung für Medizinprodukte - Teil 1: Haftung des Herstellers nach dem ProdHaftG, Phi - 3/2010, 108 (115).

schreitender Autonomie von Medizinprodukten zu, insbesondere für den - derzeit allerdings noch nicht im Raum stehenden - Fall selbstlernender Systeme.

Nach Auffassung der Arbeitsgruppe ist es mit Blick auf autonome Medizinprodukte nicht gerechtfertigt, die für Arzneimittel geltenden Regelungen zu übertragen. Während der Einsatz von Arzneimitteln immer mit einem körperlichen Eingriff verbunden ist und in der Regel sowohl positive als aber auch negative (Neben-)Wirkungen hat, bedeutet der Einsatz von Medizinprodukten nicht immer einen körperlichen Eingriff und negative Wirkungen. Daraus rechtfertigt sich nicht nur die äußerst sorgfältige Zulassung für Arzneimittel, sondern auch die schärfere Haftung. Ferner ist zu berücksichtigen, dass das Arzneimittelgesetz bereits vor Einführung der Produkthaftungsrichtlinie und des Produkthaftungsgesetzes bestand. Die besondere Singularität der arzneimittelrechtlichen Regelungen wird durch einen Blick auf die Historie des in § 84 AMG normierten Gefährdungshaftungstatbestandes deutlich: neben der Zulassungspflicht, Herstellungs- und Vertriebsverboten, einer Dauerüberwachung der Arzneimittel durch Hersteller und Behörden wurde die verschuldensunabhängige Herstellerhaftung nach Bekanntwerden der Contergan-Fälle eingeführt.[367]

Es ist zudem - wie bereits kurz angesprochen - darauf hinzuweisen, dass die Entlastungsmöglichkeit nach § 1 Abs. 2 Nr. 5 ProdHaftG die deliktischen Pflichten des Herstellers für die Post-Inverkehrgabe-Phase unberührt lässt. Wächst die Gefahrerkenntnis in der Zeit zwischen Inverkehrbringen des Produkts und Schadenseintritt, begründet dies zwar nach dem ProdHaftG keine Produktbeobachtungs- oder gar Warn- und Rückrufpflichten für den Hersteller. Kommt er aber dieser Pflicht nicht nach, so setzt er sich gleichwohl einer doppelten Gefahr aus. Erstens wird er sich für Schäden durch spätere Lieferungen der gleichen Produktserie schwerlich auf die Vorschrift des § 1 Abs. 2 Nr. 5 ProdHaftG berufen können, um sich somit von der Haftung zu entlasten. Überdies kann er für das Unterlassen einer Warnaktion ab dem Zeitpunkt des Bekanntwerdens der Produktgefahren deliktisch haftbar gemacht werden.[368]

Es ist aber fraglich, ob etwa die Grundsätze des Gentechnikgesetzes (GenTG) auf autonome Medizinprodukte übertragen werden könnten oder sollten.
Das Gentechnikgesetz enthält in den §§ 32 ff. Regelungen für einen von Rechtswidrigkeit und Verschulden unabhängigen Tatbestand der Gefährdungshaftung, der an Schäden durch gentechnisch veränderte Organismen anknüpft. Die dort geregelte Gefährdungshaftung umfasst auch das Entwicklungsrisiko. Die Schaffung eines derartigen Gefährdungshaftungstatbestandes ist dadurch

---

[367] MüKo/*Freund*, StGB, Band 6 Nebenstrafrecht I, AMG, Vorbemerkung vor § 1, Rn. 5.
[368] *Hoxhaj*, Quo vadis Medizintechnikhaftung? Arzt-, Krankenhaus- und Herstellerhaftung für den Einsatz von Medizinprodukten, S. 173.

motiviert, dass die Wirkungsweise der in ihrer natürlichen Substanz veränderten Organismen nach aktuellem Stand der Wissenschaft nicht mit letzter Sicherheit prognostizierbar ist. Vor diesem Hintergrund ist das mit dem GenTG geschaffene Haftungsrecht ein Mittel zur risikoorientierten Flankierung der sowohl chancenreich als auch als gefahrträchtig angesehenen Gentechnik und soll einen Beitrag zur Sozialverträglichkeit der technischen Entwicklung unter dem Aspekt der Technikfolgenbewältigung leisten, unbeschadet der ebenfalls bestehenden präventiv-verhaltenssteuernden Funktion der gentechnikrechtlichen Schadensersatzhaftung.[369]

§ 37 Abs. 2 S. 1 GenTG bestimmt für die dort genannten Produkte, dass die Haftungsvorschriften des GenTG nicht anzuwenden sind. Gem. § 37 Abs. 3 GenTG, wonach die Haftung aufgrund anderer Vorschriften unberührt bleibt, richtet sich die Haftung deshalb für diese Produkte insbesondere nach dem ProdHaftG. Sofern der Produktfehler auf gentechnischen Arbeiten beruht, ist aber gem. § 37 Abs. 2 S. 2 GenTG die Regelung des § 1 Abs. 1 Nr. 5 ProdHaftG unanwendbar. Diese Vorschrift schließt die Ersatzpflicht aus, wenn der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. Damit stellt auch das Entwicklungsrisiko, das als das eigentliche und primäre Risiko der Gentechnologie angesehen wird[370], einen Haftungsgrund im Rahmen der Produzentenhaftung für gentechnische Produkte dar. Der Hersteller trägt also das volle Risiko für Unvollständigkeiten und Fehler der gentechnischen Wissenschaft und Anwendungstechnik sowie unterlassene Sicherung.[371]

Es stellt sich die Frage, ob angesichts der Unwägbarkeiten, die mit der Technik autonomer - insbesondere selbstlernender - Systeme einhergehen könnten, eine dem GenTG entsprechende Regelung gerechtfertigt wäre, die die Entwicklungsrisiken den Herstellern autonomer Systeme in der Medizintechnik auferlegt.

In der Literatur wird dies vereinzelt überlegt. Denn immerhin habe sich entgegen aller Befürchtungen die Gentechnik bislang als absolut sichere und ungefährliche Technik erwiesen, während bei der Entwicklung von Medizinprodukten die Risikobehaftung klar erkennbar sei. Dieses Entwicklungsrisiko wiederum ließe sich versicherungstechnisch gut abdecken, sodass insgesamt durch die Zuweisung von Entwicklungsrisiken an den Hersteller eines Medizinprodukts eine rechtspolitisch wünschenswerte Lösung erreicht würde.[372] Bemerkenswert ist, dass *Knoche* diese Auffassung für „normale“ Medizinprodukte vertreten hat, und nicht etwa für autonome, selbstlernende Systeme.

---

[369] Staudinger/*Kohler,* BGB, Stand 2017, GenTG, § 37, Rn. 1 m.w.N.
[370] Amtliche Begründung zum GenTG, BT-Drucks 11/5622, S. 36.
[371] Staudinger/*Kohler,* BGB, Stand 2017, GenTG, § 49, Rn. 1 m.w.N.
[372] *Knoche,* Haftung für Medizinprodukte: Beweisrechtliche Fragen, VersR 2005, 1614.

Nach Ansicht der Arbeitsgruppe besteht jedoch kein Anlass, für die nach dem derzeitigen Stand der Technik in absehbarer Zeit zum Einsatz kommenden autonomen (nicht selbstlernenden) Systeme das Entwicklungsrisiko den Herstellern aufzuerlegen. Die Gründe für die im GenTG aufgenommenen Regelungen bestehen darin, dass seinerzeit angesichts eines noch nicht endgültig geklärten Erkenntnisstandes der Wissenschaft bei der Beurteilung von Ursachenzusammenhängen und der langfristigen Folgen des Einsatzes von Gentechnik den Gesetzgeber eine besondere Sorgfaltspflicht getroffen hat, die unter anderem in der Verantwortung gründete, für die künftigen Generationen die natürlichen Lebensgrundlagen zu schützen. So hat auch das Bundesverfassungsrecht mit seiner Entscheidung vom 24.11.2010[373] klargestellt, dass das Gentechnikgesetz verfassungsgemäß ist. In den Gründen der Entscheidung wird unter anderem ausgeführt, dass die Risiken und Chancen der Nutzung der Gentechnik, die in die elementaren Strukturen des Lebens eingriffen, umstritten und nicht abschließend geklärt seien und es ggf. zu unerwünschten Nebenfolgen kommen könne. Die Auswirkungen der Technik könnten unumkehrbar sein.

Derartige unabsehbare Folgen sind jedoch hinsichtlich der nach dem derzeitigen Stand zum Einsatz kommenden autonomen Systeme in der Medizintechnik nicht zu erwarten. Es handelt sich um abgekapselte Systeme, deren „Entscheidungen" absehbar und im Wesentlichen nachvollziehbar sind. Somit sind sie - im Gegensatz zur Gentechnik - letztlich beherrschbar.
Ob dies auch für die ggf. in der Zukunft zum Einsatz kommenden selbstlernenden Systeme gilt, kann mangels faktischer Grundlage zum jetzigen Zeitpunkt offenbleiben.

Am Rande ist noch zu ergänzen, dass eine Herausnahme der Haftung für Entwicklungsrisiken in speziellen Bereichen wie der Medizintechnik zu Wertungswidersprüchen in Bezug auf die Regelungen zum autonomen Fahren führen würde. Während bei Letzterem unter anderem Dritte (mit-)betroffen sein können, steht bei der Medizintechnik „nur" der in der Regel hinreichend durch den Arzt aufgeklärte und in die Behandlung mit dem autonomen System einwilligende Patient im Raum. Eine Änderung der Haftung für Entwicklungsrisiken im Bereich der Medizintechnik hätte zudem ggf. Auswirkungen auf die Innovationsfreudigkeit der Hersteller. Dies wiederum könnte Patienten schaden, deren eventuell letzte Chance auf Heilung oder Besserung des Gesundheitszustandes in der Behandlung mit einem solchen System liegt und die daher bereit sind, das damit ggf. einhergehende Risiko auf sich zu nehmen.

---

[373] BVerfG, Urt. v. 24.11.2010 – 1 BvF 2/05 –, BVerfGE 128, 1-90.

(6) Beweislastverteilung

Nach den allgemeinen beweisrechtlichen Grundsätzen trägt der Geschädigte die Beweislast für das Vorliegen eines Fehlers, für das Vorliegen eines Schadens sowie für die Ursächlichkeit zwischen Fehler und Schadenseintritt. Um einen Anspruch aus § 1 ProdHaftG gerichtlich durchzusetzen, muss der Geschädigte also den Nachweis führen, dass ihm ein Schaden entstanden ist, der durch den Fehler eines Produkts verursacht wurde.
Ob im Zusammenhang mit dem Einsatz autonomer Systeme in der Medizintechnik Beweisschwierigkeiten auftreten werden, ist zum jetzigen Zeitpunkt nicht erkennbar. Es kann daher derzeit keine Aussage dazu getroffen werden, ob und inwieweit Beweiserleichterungen erforderlich sein könnten. Diese Fragen sind zunächst der Rechtsprechung zu überlassen.

4. Ergebnis

Beim Einsatz von autonomen Medizinprodukten kann es zu einer Verlagerung von Pflichten kommen. Je autonomer ein System agiert, desto häufiger wird der Arzt nicht mehr für Ausführungsfehler, sondern nur noch für Fehler bei der Auswahl, Überwachung und Wartung des Produkts haften. Dies gilt insbesondere dann, wenn der Schaden auf einer fehlerhaften Programmierung beruht. Vom Arzt wird aber – wie stets beim Einsatz von Medizinprodukten – weiter verlangt, dass er die autonom agierende Maschine sachgerecht auswählt, überwacht und – soweit diese Aufgabe nicht beim Krankenhausträger liegt – wartet.

Der Arzt muss ferner bei der Diagnostik und Behandlung grundsätzlich den medizinischen Standard einhalten. Hierbei darf er – vorbehaltlich der aufgeklärten Entscheidung des Patienten – zwischen mehreren Behandlungsmöglichkeiten, die alle dem Standard entsprechen, wählen. Soweit also in einigen Jahren der Fall eintritt, dass der Einsatz einer autonomen Technik dem medizinischen Standard entspricht, bezieht sich die Wahlmöglichkeit des Arztes auch auf deren Einsatz. Ist dieser Stand noch nicht erreicht, können den Arzt besondere Aufklärungspflichten treffen. Der Arzt muss daher mit dem Patienten die Chancen und Risiken des in Rede stehenden autonomen Systems besprechen und bewerten, um dem Patienten eine sachgerechte Entscheidung über die zu wählende Behandlungsmethode zu ermöglichen.

Mangels relevanter Schutzlücke ist es nicht geboten, eine Gefährdungshaftung des Betreibers für autonome Medizinprodukte einzuführen. Dabei ist auch zu bedenken, dass mit der autonom agierenden Medizintechnik typischerweise keine unbeteiligten Dritte, sondern lediglich Personen in Berührung kommen, die über die typischen Risiken der eingesetzten Produkte hinreichend aufgeklärt wurden. Zwar kann es dazu kommen, dass ein Arzt seine ihn treffenden Aufklärungspflichten gegenüber dem Patienten verletzt. In diesem Fall greift aber in der Regel die Haftung aus § 280 Abs. 1 BGB.

Auch im Hinblick auf die Haftung des Herstellers von autonom agierender Medizintechnik ist derzeit kein gesetzgeberischer Handlungsbedarf erkennbar. Im Ergebnis kommen vertragliche Ansprüche nur zwischen dem Verkäufer des autonomen Systems und seinem Vertragspartner, meist dem Träger des Krankenhauses, in Betracht, die gegenüber sonstigen vertraglichen Verhältnissen keine besonderen Probleme aufwerfen.

Für eine deliktische Haftung aus § 823 Abs. 1 BGB gelten die allgemeinen Grundsätze der Herstellerhaftung. Autonome Systeme müssen den im Zeitpunkt ihres Inverkehrbringens maßgeblichen Sicherheitsstandard einhalten und Gefahren berücksichtigen, die zu diesem Zeitpunkt bekannt oder erkennbar waren. Die Hersteller verfahren momentan so, dass das verwendete autonome System „abgekapselt" wird und beim Einsatz allein die Daten benutzt werden, die von der Zulassungsstelle – von Beginn an oder im Zuge eines Updates – freigegeben wurden. Soweit es also weiter eindeutig zuordenbar bleibt, aufgrund welcher Datenbasis das autonome System wie handelt, treten auch bei der Zuordnung von potentiellen Konstruktionsfehlern zum Hersteller keine strukturell neuen Probleme auf.

Gegen eine hinreichend gewichtige Haftungslücke spricht auch, dass der Einsatz von Medizinprodukten von einer Zulassung abhängig ist. Es kann nämlich grundsätzlich davon ausgegangen werden, dass dann, wenn ein Zulassungsverfahren existiert, die Gefahr schädigender Ereignisse geringer ist, als würde es das Zulassungsverfahren nicht geben.

Im Gegensatz zum Arzneimittelhersteller, der nach § 84 AMG auch für Entwicklungsfehler haftet, ist der Medizinproduktehersteller, der autonome Systeme herstellt, nach § 1 Abs. 2 Nr. 5 ProdHaftG privilegiert. Momentan besteht aber kein Anlass, für die nach dem derzeitigen Stand der Technik in absehbarer Zeit zum Einsatz kommenden autonomen (nicht selbstlernenden) Systeme das Entwicklungsrisiko den Herstellern aufzuerlegen. Denn derzeit sind durch den Einsatz autonomer Systeme noch keine unabsehbaren Folgen zu erwarten, da es sich um abgekapselte Systeme handelt, die im Wesentlichen nachvollziehbar und letztlich auch beherrschbar sind.

Eine andere Problemlage könnte zukünftig entstehen, wenn Produkte eingesetzt werden, die nicht nur autonom, sondern auch selbstlernend agieren, da hierdurch eine klare Zurechnung von Verantwortlichkeiten nicht mehr gewährleistet sein könnte. Der Einsatz solcher Produkte ist aber jedenfalls für den Medizinbereich in absehbarer Zeit nicht zu erwarten.

IV. Handlungsbedarf

Nach Auskunft der von der Arbeitsgruppe angehörten Experten kommt es im Bereich der Medizinprodukte auf dem europäischen Markt in absehbarer Zeit zwar zum Einsatz autonomer, nicht aber von selbstlernenden Systemen.

Beim Einsatz autonom agierender Medizintechnik bedarf es keiner neuen Gefährdungshaftung des Betreibers, da wegen der Verpflichtung des Arztes zur ordnungsgemäßen Aufklärung des Patienten über den Einsatz zugelassener autonomer Produkte auch ohne eine solche Haftung keine Haftungslücke droht.

Auch beim Einsatz autonomer Systeme in der Medizintechnik kann es dabei verbleiben, dass die Ersatzpflicht des Herstellers nach dem Produkthaftungsgesetz ausgeschlossen ist, wenn der Fehler des Produkts nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte.

Teil 2: „Blockchain“

A. Einführung

Die Blockchain-Technologie ermöglicht es, Daten unter Verzicht auf eine zentrale Instanz weitgehend manipulationsresistent abzuspeichern und bestimmte Informationen auch ohne Einschaltung eines Intermediärs sicher auszutauschen.[374] Sie ist ein Unterfall der Distributed-Ledger-Technologie (DLT), die alle Techniken umfasst, die auf der Dezentralisierung einer Datenmenge beruhen.[375]

Bekanntheit hat die Blockchain-Technologie bisher im Wesentlichen durch die Kryptowährung Bitcoin erlangt. Als Grundlagentechnologie eignet sie sich jedoch für unzählige und vor allem auch unterschiedlichste Anwendungsbereiche.[376] Als Smart Contracts bezeichnete Programme, die in einer Blockchain hinterlegt werden können, eröffnen Möglichkeiten, die Vertragsabwicklung und die Durchsetzung vertraglicher Ansprüche effizienter zu gestalten. Blockchain-basierte Systeme kommen beispielsweise zur automatisierten Auszahlung von pauschalierten Entschädigungs- oder Versicherungssummen, zur Nachzeichnung des Transportverlaufs von Lebensmitteln oder sonstigen Waren, zur Verwaltung von Softwarelizenzen[377] oder als Register für Immaterialgüterrechte[378], zur Regelung der Nutzung von Mobilien oder Immobilien,[379] oder zur Hinterlegung von Herkunftsnachweisen für Diamanten oder sonstige Gegenstände in Betracht. Das Bundesministerium der Finanzen und das Bundesministerium der Justiz und für Verbraucherschutz haben am 7. März 2019 ein Eckpunktepapier zur regula-

---

[374] Vgl. *Leipold*, Hätte, hätte, Datenkette, Chip 2018, 18 (19); *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 56.

[375] *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 36; *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S.14.

[376] Vgl. etwa die Beispiele bei *Müller*, Bitcoin, Blockchain und Smart Contracts, ZfIR 2017, 600 (610 ff.); *Heckmann/Schmid*, Studie Blockchain und Smart Contracts, 2017, S. 7 f.; *Breidenbach/Glatz*, Rechtshandbuch Legal Tech, 2018, S. 73; *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019; *Herrmann*, Was Entscheider wissen sollten: Blockchain - die Chancen und die Risiken, Computerwoche 2019, 14 ff.

[377] Vgl. *Blocher/Hoppen/Hoppen*, Softwarelizenzen auf der Blockchain, CR 2017, 337 ff.

[378] Vgl. *Hohn-Hein/Barth*, Immaterialgüterrechte in der Welt von Blockchain und Smart Contract, GRUR 2018, 1089 ff.

[379] Vgl. *Blocher*, The next big thing: Blockchain - Bitcoin - Smart Contracts, AnwBl 2016, 612 (617).

torischen Behandlung von elektronischen Wertpapieren und Krypto-Token herausgegeben und einen Referentenentwurf angekündigt, mit dem insbesondere die elektronische Begebung von Schuldverschreibungen unter Verwendung der Blockchain-Technologie ermöglicht werden soll.[380] In der Literatur werden auch die Führung von Grundbuch[381] oder Handelsregister[382] auf Grundlage der Blockchain-Technologie diskutiert.

Noch gibt es allerdings nur wenige praktische Anwendungsbeispiele. Den Endverbraucher erreicht haben dürften bislang wohl nur Kryptowährungen wie Bitcoin oder das Angebot einer blockchainbasierten Flugverspätungsversicherung.[383] Soweit ersichtlich haben auch weder Blockchain-Anwendungen noch Smart Contracts bisher die Zivilgerichte beschäftigt. Immer wieder wird auch das Potential der Blockchain-Technologie in Frage gestellt.[384] Es bleibt abzuwarten, in welchen Bereichen sich die Technologie tatsächlich durchsetzt. Für die Arbeitsgruppe galt es ungeachtet dessen zu prüfen, ob bereits heute rechtliche Probleme absehbar sind, deren Lösung nicht der Rechtsprechung überlassen werden kann. Wie in allen anderen zu untersuchenden Bereichen legt die Arbeitsgruppe auch hier die Prämisse zugrunde, dass kein gesetzgeberischer Handlungsbedarf besteht, soweit und solange das geltende („analoge") Recht tragfähige Normen für die Folgen der Digitalisierung bereithält und es den Gerichten überantwortet werden kann, die neuen Sachverhalte durch Subsumtion unter vorhandene Normen sachgerechten Lösungen zuzuführen.

Entsprechend ihrem Auftrag beschränkt sich die Arbeitsgruppe dabei auf eine zivilrechtliche Betrachtung und klammert insbesondere aufsichts-[385] und datenschutzrechtliche[386] Aspekte aus.

---

[380] https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/Eckpunkte_Krypto_Blockchain.pdf;jsessionid=EA2DE194C370E6DA1FC70B0879C6240C.2_cid324?__blob=publicationFile&v=2, letzter Abruf: 25.3.2019.

[381] Insoweit kritisch *Wilsch*, Die Blockchain-Technologie aus Sicht des deutschen Grundbuchrechts, DNotZ 2017, 761 ff.; vgl. a. *Berger*, Blockchain - Mythos oder Technologie für die öffentliche Verwaltung, DVBl 2017, 1271 ff.

[382] Vgl. *Knaier/Wolff*, Die Blockchain-Technologie als Entwicklungsoption für das Handelsregister?, BB 2018, 2253 ff.

[383] Vgl. *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019.

[384] Vgl. etwa *Dworschak*, Nächstes (großes?) Ding, Der Spiegel 2018, S. 118 ff.; *Herrmann*, Was Entscheider wissen sollten: Blockchain - die Chancen und die Risiken, Computerwoche 2019, 14 ff. sowie *Herrmann*, Blockchain - was kommt nach dem Hype?, Computerwoche 2019, 18 ff; *Leipold,* Lasst die Daten von der Kette!, CHIP 2019, 44 ff.

[385] Zur aufsichtsrechtlichen Behandlung virtueller Währungen vgl. etwa *Spindler/Bille,* Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357 (1363 ff.); *Bialluch-von Allwörden/von Allwörden*, Initial Coin Offerings: Kryptowährungen als Wertpapier oder Vermögensanlage, WM 2018, 2118 ff.

[386] Vgl. hierzu etwa *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 ff.; *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain,

B. Technische Grundlagen

I. Grundstruktur

Als Blockchain bezeichnet man eine dezentrale[387] verteilte Datenstruktur, in der von den Teilnehmern verifizierte Transaktionsdaten blockweise gespeichert werden.[388] Die einzelnen Datenblöcke werden dabei kryptografisch so miteinander verkettet, dass jeder folgende Block einen Verweis auf den vorhergehenden Block trägt und eine rückwirkende Änderung bereits gespeicherter Blöcke mit zunehmender Länge der Kette praktisch unmöglich wird.[389] Die einzelnen Teilnehmer (Knoten = *nodes*) sind zumeist über ein peer-to-peer-Netzwerk miteinander verbunden, innerhalb dessen die Blockchain redundant auf den beteiligten Rechnern gespeichert wird, so dass jeder Teilnehmer grundsätzlich[390] ein eigenes Exemplar des Hauptbuches mit der gesamten Transaktionshistorie führt, das stetig fortgeschrieben wird.[391]

Zur Grundidee der Blockchain-Technologie gehört die Gleichberechtigung aller Teilnehmer.[392] An die Stelle einer zentralen Autorität, der Vertrauen entgegengebracht wird, tritt ein Transparenz- und Konsensprinzip: Die Bildung einzelner Blöcke muss durch die Mehrheit der Teilnehmer bestätigt werden. Jeder Teilnehmer kann grundsätzlich die komplette Datenbank einsehen und die Transak-

---

NJW 2017, 1431 (1433-1435); *Quiel*, Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO, DuD 2018, 566 ff.

[387] Der Begriff der Dezentralität meint hier, dass es keine zentrale technische Autorität gibt, die alleine über die Wahrheit der Daten entscheidet.

[388] Vgl. *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 42 ff.; *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S.14; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 42 ff.

[389] *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 37.

[390] Zu der für größere Blockchains wie beispielsweise Bitcoin relevanten Unterscheidung zwischen vollständigen Teilnehmern (*full nodes*) und „leichtgewichtigen" Nutzern (*light-weight nodes*) wird auf die Ausführungen unter C. II. und C.VI verwiesen.

[391] Vgl. *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 24; *Saive,* Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 186, 192; *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1432); https://www.btc-echo.de/tutorial/was-ist-die-blockchain, letzter Abruf: 26.2.2019.

[392] Vgl. *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 74 f.; *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 24.

tionshistorie überprüfen.[393] Abhängig davon, ob die Blockchain für jedermann oder nur für einen bestimmten Kreis von Teilnehmern einsehbar ist und ob man eine gesonderte Berechtigung zur Mitwirkung benötigt, kann man prinzipiell folgende Varianten der Blockchain unterscheiden:[394]

public & permissionless
Der häufigste Anwendungsfall ist die allgemein zugängliche („öffentliche")[395] Blockchain, die für jeden einsehbar ist und an der jeder teilnehmen darf.[396] Hierzu gehören z.B. Bitcoin oder Ethereum.

public & permissoned
Eine für jedermann einsehbare Blockchain kann einer Zugangsbeschränkung in dem Sinne unterworfen sein, dass die Schreibberechtigung auf einen bestimmten Nutzerkreis beschränkt wird.

private & permissionless
Denkbar sind auch private Blockchains, die nur einem bestimmten Teilnehmerkreis zur Verfügung stehen und nicht öffentlich einsehbar sind, bei denen aber alle zugelassenen Teilnehmer die gleichen Rechte haben.

private & permissoned
Meist werden bei privaten Blockchains auch die Schreibrechte eingegrenzt. Neben unternehmensinternen Blockchains sind dies z.B. Blockchains, die von Konsortien gemeinsam betrieben werden.

Ist die Blockchain privat oder mit Zugangsbeschränkungen versehen, gibt es eine zentrale Instanz, die über die Berechtigungen innerhalb der Blockchain wacht; es handelt sich in diesen Fällen nicht um ein reines peer-to-peer-Netzwerk.[397] Auch wenn die Teilnahme an der Blockchain einer besonderen Zulassung unterliegt, hat derjenige, der über die Zulassung entscheidet, regelmäßig

---

[393] Vgl. *Spindler/Bille*, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357 (1358).
[394] Vgl. *Drescher,* Blockchain Grundlagen, 2017, S. 228; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 64 f.; *Saive,* Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 186 (187); teils abweichend *Herrmann*, Was Entscheider wissen sollten: Blockchain - die Chancen und die Risiken, Computerwoche 2019, 14 (17).
[395] Mit einer öffentlichen Blockchain ist hier eine öffentlich einsehbare Blockchain gemeint; nicht aber eine amtliche oder staatliche.
[396] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 58.
[397] *Saive*, Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 186 (191).

aber keine Einflussmöglichkeiten auf die Datenverarbeitung der einzelnen Knoten; er kann insbesondere nicht auf die Version der Datenkette des einzelnen Teilnehmers einwirken.[398]

II. Teilnahme an einer Blockchain

Grundsätzlich kann jeder einen sog. *full node*, d.h. einen „vollwertigen" Knoten, der an der Verifizierung der Transaktionsdaten beteiligt ist und ein vollständiges Abbild der Blockchain vorhält, auf einem Computer mit den notwendigen Minimalanforderungen der jeweiligen Anwendung[399] installieren und betreiben. Im Rahmen der Einrichtung wird eine aktuelle Kopie der Blockchain heruntergeladen und lokal auf dem Computer gespeichert (Initial Block Download). Um andere Knoten im Netzwerk zu finden, sucht die Software zunächst unter bekannten Domain-Namen oder IP-Adressen nach Knoten. Sobald einmal eine Verbindung zum Netzwerk besteht, können darüber bei Bedarf weitere Knoten gefunden werden. Bei Bitcoin hat beispielsweise jeder full node in der Regel acht ausgehende Verbindungen zu anderen Knoten.

Um lediglich Transaktionen in die Blockchain eintragen zu können, genügt es, eine schlankere Version der Blockchain herunterzuladen, die allerdings auch eine geringere Sicherheit bietet, da man nicht alle früheren Transaktionen selbst nachvollziehen und überprüfen kann.[400]

III. Digitales Schlüsselpaar (Public-Key-Verfahren)

Um eine Transaktion innerhalb der Blockchain vornehmen zu können, benötigt man ein digitales Schlüsselpaar (private key und public key), das unter Zuhilfenahme eines Zufallsgenerators erzeugt wird.[401] Mit Hilfe des privaten Schlüssels werden eigene Mitteilungen signiert.[402] Die Geheimhaltung und Sicherung des privaten Schlüssels ist von immenser Wichtigkeit, da man nur mit Hilfe des privaten Schlüssels Verfügungen über Werte, die mit diesem verknüpft worden

---

[398] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1255).

[399] Vgl. z.B. für Bitcoin: 200 GB freier Speicherplatz und 2 GB Arbeitsspeicher: https://bitcoin.org/en/full-node#secure-your-wallet; letzter Abruf: 21.11.2018.

[400] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 27.

[401] *Leipold*, Hätte, hätte, Datenkette, Chip 2018, 18 (20); *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 66.

[402] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 21; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 55.

sind, vornehmen kann und eine Wiederherstellung eines verlorenen Schlüssels ausgeschlossen ist.[403] Der von dem privaten Schlüssel kryptografisch abgeleitete öffentliche Schlüssel wird den anderen Teilnehmern oder auch allgemein bekannt gemacht. Mit ihm können die Knoten Signaturen anderer Teilnehmer überprüfen und eigene Mitteilungen an einen bestimmten Empfänger über dessen öffentlichen Schlüssel oder eine daraus abgeleitete Adresse richten.[404]

IV. Hashing

Die Verschlüsselung von Daten in der Blockchain erfolgt mit Hilfe sog. Hashfunktionen. Diese öffentlich zugänglichen Algorithmen leiten aus Daten unterschiedlichster Art (z.B. Textdokumente, Fotos, Musikdateien etc.) und beliebiger Größe einen alphanumerischen Wert fester Länge ab.[405] Die so erzeugten Hashwerte können einfach und schnell miteinander verglichen werden, erlauben aber keinen Rückschluss auf den Inhalt der zugrundeliegenden Daten.[406] Für Blockchain-Anwendungen werden *kryptografische* Hashfunktionen verwendet, die nicht vorhersagbare Hashwerte erzeugen, die mit an Sicherheit grenzender Wahrscheinlichkeit nicht auf ihren Eingabewert zurückzurechnen (Einwegfunktion) und zudem kollisionsresistent sind.[407] Um die entsprechende Komplexität für eine praktisch unmögliche Rückrechnung zu erreichen, müssen kurze Eingabewerte ggf. verlängert werden.[408] Kollisionsresistent ist eine Hashfunktion,

---

[403] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 52; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 54 ff.; *Spindler*/*Bille*, Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357 (1358).

[404] Vgl. *Brünnler,* Blockchain kurz & gut, 2018, S. 16; *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 21 ff.; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 66.

[405] Vgl. *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 51.; *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.

[406] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 22.

[407] Vgl. *Drescher*, Blockchain Grundlagen, 2017, S. 89 ff.; *Brünnler*, Blockchain kurz & gut, 2018, S. 13.; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 51 ff.; *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.

[408] *Brünnler*, Blockchain kurz & gut, 2018, S. 14.

wenn sie aus verschiedenen Eingabewerten praktisch niemals den gleichen Ausgabewert bildet.[409]

V. Einleitung einer Transaktion[410]

Zur Vornahme einer Transaktion, sendet man die notwendigen Transaktionsdaten (signiert mit dem eigenen *private key*) unter Angabe der Empfänger-Adresse an die verbundenen Knoten.[411] Diese prüfen die Transaktion sodann anhand der jeweiligen Regeln der konkreten Blockchain-Anwendung, verifizieren u.a. die Signatur des Absenders sowie seine Berechtigung, über den Wert nach dem maßgeblichen Blockchainprotokoll zu verfügen, verteilen die Daten weiter und legen die verifizierte Transaktion in einem Zwischenspeicher ab.[412]

VI. Blockbildung

Sobald eine bestimmte Zahl verifizierter Transaktionen im Zwischenspeicher liegt, beginnen die sog. miner mit dem Versuch, einen neuen Block zu bilden und der vorhandenen Kette hinzuzufügen.[413] Die Blockbildung wird dabei künstlich zu einer energie-, zeit- und/oder kostenintensiven Aufgabe gemacht.[414] Denn nur wenn die Blockbildung in einer allgemein und unbeschränkt zugänglichen Blockchain mit einem hohen Aufwand verbunden ist, werden auch Manipulationen, die mit dem gleichen Aufwand je neu zu schreibendem Block verbunden wären, unrentabel.[415]
Die Einzelheiten der Blockbildung unterscheiden sich je nach konkreter Anwendung. Jede Nutzer-Applikation enthält eine Reihe von Regeln, wie Transaktionen und Blöcke aufgebaut, verifiziert und verbreitet werden und wie die maß-

---

[409] *Drescher*, Blockchain Grundlagen, 2017, S. 91; *Brünnler*, Blockchain kurz & gut, 2018, S. 14.
[410] Zum Begriff vgl. im Einzelnen unter D.
[411] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1252).
[412] Vgl. *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 36.
[413] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 36.
[414] Vgl. *Drescher*, Blockchain Grundlagen, 2017, S. 154 und S. 172.
[415] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 40; *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.

gebliche Reihenfolge der Blöcke festgelegt wird.[416] Bei den meisten allgemein zugänglichen Blockchains muss zur erfolgreichen Bildung eines neuen Blocks ein sog. *proof-of-work* erbracht werden.[417] Dazu treten die Teilnehmer in einen Wettbewerb um die Lösung einer kryptografischen Rechenaufgabe (*hashpuzzle*). In einem trial and error-Verfahren muss ein Hashwert ermittelt werden, der ein bestimmtes Kriterium erfüllt, bei Bitcoin beispielsweise unterhalb einer bestimmten Zielvorgabe liegt.[418] Diese Art der Blockbildung wird auch als *mining* bezeichnet, die daran beteiligten Rechner daher als *miner*. Der Schwierigkeitsgrad der Rechenaufgabe wird im Laufe der Zeit immer wieder erhöht, damit die Lösung des Hashpuzzles auch bei zunehmender Leistungsfähigkeit der Rechner nicht weniger aufwändig wird. Sobald ein Rechner das Hashpuzzle gelöst hat, sendet er den neugebildeten Block an die anderen Knoten zur Validierung.[419] Die Kopfzeile (*block-header*) des neu gebildeten Blocks enthält u.a. einen Hash, der über alle im Block enthaltenen Transaktionsdaten errechnet wurde, einen Zeitstempel, die Lösung des Hashpuzzles (*nonce)* und einen Verweis auf den vorangehenden Block.[420] Nach erfolgreicher Validierung eines Blocks fügen die Knoten diesen der auf ihrem Rechner gespeicherten Kette hinzu und verteilen ihn an andere Knoten weiter.[421]

Grundsätzlich steht es bei einer allgemein zugänglichen Blockchain jedem Nutzer frei, sich an der Blockbildung zu beteiligen. Prinzipiell sollten auch alle Teilnehmer eines Blockchainsystems jederzeit über die gleiche Kopie der

---

[416] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 44.

[417] Alternative Konsensfindungsprozesse zu proof-of-work sind beispielsweise proof-of-stake, proof-of-authority, proof-of-service oder proof-of-burn. Vgl. zu näheren Einzelheiten *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 45 ff.

[418] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 41; *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.

[419] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 39.

[420] *Drescher*, Blockchain Grundlagen 2017, S. 155; *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 37.

[421] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 42.

Blockchain verfügen.[422] Aufgrund der dazu benötigten enormen Speicher- und Rechenleistungsressourcen können sich an dem Prozess des Minings bei größeren Blockchains erfolgreich aber nur sehr leistungsstarke Rechner beteiligen. Teilweise werden Mining-Pools gebildet, um Rechenkapazitäten mehrerer Knoten zu bündeln.[423] Bei großen unbeschränkt zugänglichen Blockchains verfügt faktisch auch nur ein kleinerer Teil von full nodes über die komplette Abbildung der Blockchain.[424] Anfang März 2019 betrug z.B. die Größe der gesamten Bitcoin-Blockchain rund 205 GB.[425]

VII. „Gültigkeit" eines Blocks / Verfahren bei Forkbildung

Da regelmäßig mehrere Miner gleichzeitig versuchen, neue Blocks zu bilden, sie dazu beliebige Transaktionen aus dem Zwischenspeicher auswählen können und gewisse zeitliche Verzögerungen bei der Verteilung im Netzwerk auftreten, kommt es immer wieder zur Bildung und Versendung konkurrierender Blöcke, die auf den gleichen Vorgängerblock verweisen.[426] Jeder Teilnehmer schreibt die auf seinem Rechner gespeicherte Blockchain autonom fort und hängt den ältesten bei ihm eingegangenen Folgeblock an die Kette.[427] Die Kette gabelt sich in solchen Fällen in mehrere Zweige auf, es bildet sich ein *fork*. Sobald ein Zweig mehr validierte Folgeblöcke enthält als der andere, setzt sich dieser und damit die längere Kette durch.[428] Derzeit werden Transaktionen als „gültig" angesehen, sobald dem sie enthaltenden Block fünf Nachfolgeblöcke angefügt worden sind[429] - ohne dass damit eine Aussage über die rechtliche Wirksamkeit

---

[422] *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 80.
[423] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 43.
[424] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 16, S. 25.
[425] Vgl. https://www.blockchain.com/charts/blocks-size?, letzter Abruf: 8.3.2019.
[426] *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.
[427] Vgl. *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 39; *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.
[428] *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.
[429] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 36, S. 39.

der jeweiligen Transaktion getroffen wäre. Transaktionen, die sich in einem verwaisten Zweig der Kette befinden, werden zurück in den Zwischenspeicher gelegt und können Gegenstand einer neuen Blockbildung werden.[430]

VIII. Gebühren / Belohnung

Der Knoten, dessen Block letztlich Bestandteil der Hauptkette wird, erhält die Gebühren für die in dem Block enthaltenen Transaktionen.[431] Diese Belohnung stellt den Anreiz für den Aufwand des Minings dar. Eine allgemein zugängliche Blockchain kann nur funktionieren, wenn genügend Teilnehmer ein Interesse daran haben, an der Blockbildung teilzunehmen und die hierzu notwendige Rechenleistung zur Verfügung stellen - andernfalls ist es anfällig für Attacken.[432] Eine solche Blockchain beinhaltet daher regelmäßig auch eine Kryptowährung.[433]

IX. Möglichkeiten zur Änderung der Blockchain

Die Blockchain-Datenstruktur lässt stetige Hinzufügungen, grundsätzlich aber keine rückwirkenden Veränderungen oder Löschungen einmal akzeptierter Blocks zu.[434] Eine nachträgliche Veränderung einer eingetragenen Transaktion ist aufgrund der Verkettung der Blöcke nur möglich, wenn man nicht nur den betroffenen Block, sondern auch alle nachfolgenden Blöcke der maßgeblichen Kette mit dem entsprechenden Aufwand abändert.[435] Um die Blockchain zu manipulieren, muss ein Angreifer daher über 50 Prozent der Rechenleistung des gesamten Netzwerks kontrollieren.[436] Um die Bitcoin-Blockchain anzugreifen, müsste man nach Angaben in der Literatur schätzungsweise rund 1,5 Millionen Spezialrechner betreiben, was einem Hardware-Wert von mehreren Milliarden

---

[430] *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.

[431] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 43.

[432] *Brünnler*, Blockchain kurz & gut, 2018, S. 67 f.; *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 59.

[433] *Brünnler*, Blockchain kurz & gut, 2018, S. 67 f.

[434] *Drescher*, Blockchain Grundlagen, 2017, S. 176.

[435] Vgl. *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 71.

[436] *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 44.

Euro und Stromkosten von täglich mindestens 10 Millionen Euro entsprechen würde.[437]

Es wird immer wieder vorkommen, dass Transaktionen in der Blockchain eingetragen werden, die aus zivilrechtlicher Sicht der Korrektur bedürfen, etwa weil das in der Transaktion enthaltene oder ihr zugrundeliegende Rechtsgeschäft nichtig ist oder aufgrund des Rücktritts eines Vertragspartners eine Rückabwicklung erforderlich wird. Eine Änderung oder Löschung bereits validierter Blöcke stünde in direktem Gegensatz zu dem der Blockchain-Technologie innewohnenden Grundprinzip der Unveränderlichkeit, aus der sich das besondere Vertrauen begründet, das der Blockchain entgegengebracht wird. Solange eine Blockchain nicht von vornherein als veränderlich konzipiert wird (zur sog. redactable blockchain s. unten), ist die nachträgliche Löschung oder inhaltliche Änderung eines Blocks im System nicht vorgesehen, d.h. die Nichtigkeit einer Willenserklärung oder des einer Transaktion zugrundeliegenden Vertrags kann nicht in dem die betroffene Transaktion enthaltenden Block selbst sichtbar gemacht werden.[438]
Soll eine Transaktion im Ergebnis rückgängig gemacht werden, also die in der Blockchain abgebildete Zuordnung korrigiert werden, kann der Empfänger bzw. derjenige, der Zugriff auf den private key hat, dem die transferierten Token zugeordnet sind, eine Transaktion mit umgekehrten Vorzeichen (sog. reverse transaction) ausführen.[439] Ggf. bedarf es der Vornahme mehrerer auf die Wiederherstellung der Ausgangslage gerichteter Transaktionen, um das gewünschte Ergebnis herzustellen. Solche Korrektur-Transaktionen bedürfen - wie jede „normale Buchung“ zur Aufnahme in einen Block - ebenfalls der Zustimmung der Mehrheit der Knoten.
Als Alternative zu einer reverse transaction ist das bewusste Herbeiführen eines forks denkbar, der den betroffenen Block und seine Folgeblöcke nachträglich verwaisen lässt.[440] Hierzu dürfte nur selten die Unterstützung der Mehrheit der Knoten gewonnen werden. Denn der fork hätte zur Konsequenz, dass alle Transaktionen der betroffenen Blöcke wieder als unerledigt in den Zwischenspeicher zurückfallen.
Ein weiterer Ansatz zur Ermöglichung nachträglicher Korrekturen des Blockchaininhalts ist das Konzept der redactable blockchain, in deren Struktur die Möglichkeit einer nachträglichen Veränderung bestehender Blöcke von vornherein vorgesehen ist.[441] Durch den Einbau einer zweiten Hashfunktion in den der

---

[437] *Leipold*, Hätte, hätte, Datenkette, Chip 2018, 18 (20).
[438] Vgl. *Bertram*, Smart Contracts, MDR 2018, 1416 (1420); zur Möglichkeit des sog. Pruning vgl. *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1255).
[439] *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (766).
[440] Vgl. a. *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (766).
[441] Vgl. *Ateniese/Magri/Venturi/Andrade*, Redactable Blockchain - or - Rewriting History in Bitcoin and Friends, https://eprint.iacr.org/2016/757.pdf, letzter Abruf: 15.1.2019; *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (766); *Martini/Weinzierl*,

Blockchain zugrundeliegenden Algorithmus werden über sogenannte chameleon hashes „Falltüren" implementiert, die nachträgliche Änderungen eines Blocks zulassen, ohne dass die Kette infolge der Änderung des Blockheaders gesprengt wird.[442] Mittels eines geheimen Schlüsselpaares wird die bestehende Hash-Verbindung zwischen zwei Blöcken aufgetrennt, so dass der zu ändernde Block durch einen neuen ersetzt werden kann, ohne dass alle nachfolgenden Blöcke ihre Gültigkeit verlieren und neu berechnet werden müssten.[443] Diese Methode ermöglicht die vollständige Entfernung einzelner Inhalte aus der Blockchain.[444] Die Änderung muss entweder von der Mehrheit der Knoten mitgetragen werden oder der Entscheidung einer zentralen Stelle unterstellt werden.[445] Allerdings steht diese Konstruktion in deutlichem Widerspruch zu der Grundidee der Blockchain-Technologie, u.a. durch die Sicherheit vor nachträglicher Veränderung besonderes Vertrauen zu begründen.[446]

X. Vor- und Nachtteile der Blockchain-Technologie (insb. der unbeschränkt zugänglichen Blockchain)

Zu den Vorteilen der Blockchain-Technologie gehören die grundsätzlich hohe Manipulationssicherheit und die Unabhängigkeit von einzelnen Servern und zentralen Instanzen. Durch den Verzicht auf Intermediäre können Zeit und Kosten eingespart werden.

Dem steht der hohe technische Aufwand entgegen, den die verteilte Speicherung der Daten mit sich bringt.[447] Ein ganz wesentlicher Nachteil der Blockchain-Technologie ist jedenfalls bei Einsatz des Konsensverfahrens proof-of-work in einer größeren Blockchain der hohe Strom- und Hardwareaufwand. Das Bitcoin-Mining ist aufgrund des künstlich geschaffenen Schwierigkeitsgrads nur mit teu-

---

Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256); *Marnau,* Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, https://dl.gi.de/bitstream/handle/20.500.12116/3865/B13-1.pdf?sequence=1&isAllowed=y, letzter Abruf: 15.1.2019.

[442] *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (766); vgl. a. M*artini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256).

[443] *Marnau,* Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung, https://dl.gi.de/bitstream/handle/20.500.12116/3865/B13-1.pdf?sequence=1&isAllowed=y, letzter Abruf: 15.1.2019.

[444] *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (767).

[445] Vgl. *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (766); *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256 f.).

[446] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1255).

[447] Vgl. *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019.

ren Spezialrechnern zu leisten; aufgrund des enormen Energieaufwands[448] ist es zudem nur in Ländern mit niedrigen Strompreisen attraktiv und zugleich ökologisch bedenklich.[449] Der hohe Aufwand ist dabei der Preis für die Sicherheit der Technologie, da jede Aufwands- und Kostenminderung auch die Manipulation erleichterte.[450] Der zähe Prozess der Blockbildung begrenzt überdies die Transaktionsrate. Während bei Bitcoin die maximale Transaktionsrate derzeit bei 7 Transaktionen pro Sekunde liegt, können in z.B. in Kreditkartensystemen in Hochphasen rund 56.000 Transaktionen pro Sekunde erreicht werden.[451] Zu beachten ist überdies, dass es keine Garantie für die Aufnahme einer Transaktion in einen Block gibt, mag es auch ein Ausnahmefall bleiben, dass eine Transaktion keinen Eingang in einen Block findet oder eine Abwicklung mittels Smart Contract nicht ausgeführt wird.[452]
Die hohe Transparenz einer für jedermann einsehbaren Blockchain geht außerdem zu Lasten der Privatsphäre oder unternehmerischer Geheimhaltungsinteressen. Trotz der Anonymität der Nutzer können aus einem detailliert abgebildeten Transaktionsverhalten Rückschlüsse auf den Urheber gezogen werden, selbst wenn regelmäßig neue Schlüsselpaare geniert werden. Für unternehmerische Zwecke wird sich vielfach nur eine private oder konsortiale Blockchain anbieten.[453]

Für welche Bereiche sich die Blockchain-Technologie in Anbetracht ihrer Vor- und Nachteile[454] wirklich eignet, muss sich in der Praxis noch erweisen.[455]

---

[448] Vgl. hierzu die Beispiele und statistischen Daten unter https://powercompare.co.uk/bitcoin-mining-electricity-map/; https://digiconomist.net/bitcoin-energy-consumption sowie https://www.faz.net/aktuell/finanzen/digital-bezahlen/bitcoin-eine-transaktion-kostet-30-euro-strom-15282063.html, jeweils letzter Abruf: 28.3.2019, und Leipold, Hätte, hätte, Datenkette, CHIP 2018, 18 (19 f.).

[449] Vgl. *Leipold*, Hätte, hätte, Datenkette, Chip 2018, 18 (19); *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 53.

[450] Vgl. *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 79.

[451] *Kammerer*, IOTA - die nächste Generation der Blockchain?, abzurufen über https://www.heise.de/developer/artikel/IOTA-die-naechste-Generation-der-Blockchain-4208154.html, letzter Abruf: 13.11.2018.

[452] Vgl. *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019.

[453] *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019.

[454] Vgl. a. die Übersicht von *Herrmann*, Was Entscheider wissen sollten: Blockchain - die Chancen und die Risiken, Computerwoche 2019, 14 ff.; *Leipold,* Lasst die Daten von der Kette!, CHIP 2019, 44 ff.

[455] Vgl. a. *Hosp*, Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München, 2018, S. 63, S. 78 f.; *Meinel/Gayvoronskaya/Schnjakin*, Blockchain: Hype oder Innovation, Techni-

C. Begriff des Smart Contracts

Der im Zusammenhang mit der Blockchain-Technologie häufig auftauchende Begriff des „Smart Contract“ ist - aus juristischer Sicht insoweit irreführend - rein technischer Natur und bezeichnet eine Software, welche konkrete Maßnahmen ausführt, wenn bestimme Bedingungen eintreten.[456] Es geht stets um die Ausführung einer vorgegebenen Wenn-Dann-Verknüpfung.[457] Nach der ursprünglichen Definition von *Szabo* ist ein Smart Contract ein computergestütztes Transaktionsprotokoll, das die Bedingungen eines Vertrages ausführt.[458] *Kaulartz/Heckmann* definieren ihn als „Software, die rechtlich relevante Handlungen (insbesondere einen tatsächlichen Leistungsaustausch) in Abhängigkeit von digital prüfbaren Ereignissen steuert, kontrolliert und/oder dokumentiert“.[459] Durch den Programmcode[460] wird sichergestellt, dass ausschließlich solche Transaktionen ausgeführt werden, die in dem Smart Contract zuvor festgelegt wurden.

Smart Contracts verbessern damit vor allem die Möglichkeiten, Verträge ohne größeren bürokratischen und zeitlichen Aufwand automatisiert durchzusetzen.[461] Wird das Programm so gestaltet, dass bei Eintritt einer bestimmten Bedingung (z.B. Kaufpreiszahlung) automatisch die Erfüllungshandlung (z.B. Warenlieferung) veranlasst wird, so kann man vereinfacht davon sprechen, dass der Vertrag sich von selbst erfüllt (auch Self-Executing-Contracts genannt). Smart Contracts

---

sche Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018, S. 56; *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019;

[456] Vgl. etwa *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (433 f.); *Djazayeri*, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016, Anm. 1; *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431; *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019.

[457] *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (86).

[458] Vgl. *Szabo* http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, letzter Abruf: 12.2.2019.

[459] *Kaulartz/Heckmann*, Smart Contracts - Anwendungen der Blockchain-Technologie, CR 2016, 618.

[460] Vgl. *Müller*, Bitcoin, Blockchain und Smart Contracts, ZfIR 2017, 600 (609).

[461] Vgl. *Breidenbach/Glatz*, Rechtshandbuch Legal Tech, 2018, S. 72 f., S. 110 ff.; Breidenbach/Glatz/*Regierer*, Rechtshandbuch Legal Tech, 2018, S. 101; Breidenbach/Glatz/*Sandner/Voigt/Fries*, Rechtshandbuch Legal Tech, 2018, S. 119 f.; *Müller*, Bitcoin, Blockchain und Smart Contracts, ZfIR 2017, 600 (609); *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431; *Fries*, Smart Contracts: Brauchen schlaue Verträge noch Anwälte?, AnwBl 2018, 86; *Börding/Jülicher/Röttgen/v. Schönfeld*, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134 (138).

müssen nicht an eine Blockchain angebunden sein.[462] Der Vorteil, in jenen Fällen die Blockchain-Technologie zum Einsatz zu bringen, liegt aber darin, dass eine zentrale Stelle, welche die Ausführung des Vertrags überwacht, grds. nicht benötigt wird;[463] diese Aufgabe übernimmt die Blockchain, wobei ihr die Vertragsparteien deshalb ein besonderes Vertrauen entgegenbringen können, weil der Datenbestand inhaltsgleich auf allen teilnehmenden Rechnern hinterlegt ist.[464] Schon hieraus wird deutlich, dass es sich beim Smart Contract nicht etwa um einen Vertrag im Rechtssinne handelt[465]; es handelt sich vielmehr um eine „computerbasierte Umsetzung eines Vertrages"[466], die darauf ausgerichtet ist, die Vertragsdurchführung zu vereinfachen. Noch deutlicher wird dies, wenn man sich vor Augen führt, welchen Zweck der „Erfinder" des Smart Contracts, *Nick Szabo*, bei der Entwicklung verfolgt hat. Es ging ihm darum, eine vollautomatische Vertragsdurchführung zu ermöglichen, um zu verhindern, dass nach Vertragsschluss der nach dem Vertrag geschuldete Leistungsaustausch durch einseitiges Handeln verhindert wird.[467] Auf diese Weise sollte ein Vertragsbruch möglichst „zugunsten eines strikten Grundsatzes pacta sunt servanda ausgeschlossen"[468] werden. Bereits dies belegt, dass – jedenfalls nach deutschem Verständnis[469] – zwischen den rechtsgeschäftlichen Fragen und der Frage, nach welchem Muster sich der Leistungsaustausch vollzieht, genau zu differenzieren ist. Diese Erkenntnis wird im Folgenden von wichtiger Bedeutung sein. Damit ist nicht gesagt, dass es nicht auch Anwendungsgebiete von Smart Contracts ge-

---

[462] Vgl. *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505); *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (437).

[463] Es kann allerdings der Einsatz von sog. oracles nötig sein, vgl. unten.

[464] Zu den Vorteilen der Blockchain-Anbindung vgl.a. *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505); *Börding/Jülicher/Röttgen/v. Schönfeld*, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134 (138); *Paulus/Matzke*, Smart Contracts und Smart Meter, Versorgungssperre per Fernzugriff, NJW 2018, 1905; *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505).

[465] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (433 f.); *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505); *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431; *Kaulartz/Heckmann*, Smart Contracts - Anwendungen der Blockchain-Technologie, CR 2016, 618 (619); *Blocher*, The next big thing: Blockchain - Bitcoin - Smart Contracts, AnwBl 2016, 612 (618); *Djazayeri*, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016 Anm. 1 (E.I.); *Söbbing*, Smart Contracts und Blockchain-Technologie 2018, 43 (46).

[466] Treffend *Djazayeri*, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016, Anm. 1.

[467] Vgl. *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85.

[468] *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85.

[469] S. dazu die Hinweise zum anglo-amerikanischem Recht und zur dort geltenden sog. *consideration*-Doktrin von *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (86 Rn. 8).

ben kann, bei denen die für den Vertragsschluss erforderlichen Willenserklärungen automatisiert generiert und abgegeben werden;[470] auch in diesem Fall muss jedoch die rechtsgeschäftliche Ebene, für welche die §§ 145 ff. BGB gelten,[471] von der Ebene der automatisierten Abwicklung unterschieden werden.
Sind Smart Contracts auf einer Blockchain-Anwendung implementiert, stellen sie geschlossene Systeme dar, die grundsätzlich keinen Kontakt zur Außenwelt aufnehmen.[472] Um externe Informationen abrufen zu können, müssen sie über Schnittstellen (sog. Oracles) an andere Systeme angebunden werden, um ggf. den Eintritt bestimmter Ereignisse überprüfen zu können.[473]

Der Einsatz stößt - jedenfalls aktuell - an Grenzen, sobald Wertungen nötig sind, beispielsweise die Auslegung unbestimmter Rechtsbegriffe erforderlich wird oder letztlich richterliche Ermessensentscheidungen ausschlaggebend sind,[474] etwa bei der Bemessung eines Minderungsbetrags wegen eines Mangels der Mietsache.[475] In der Praxis bieten sich Smart Contracts aktuell daher vor allem für einfach gelagerte Massengeschäfte an, bei denen der Leistungsaustausch im Vordergrund steht und Gewährleistungsrechte oder wertende Entscheidungen eine eher untergeordnete Rolle spielen.[476]

D. Begriff der Transaktion

Für die vorliegende Bearbeitung wird der Begriff der Transaktion im Sinne der Verschiebung eines in der Blockchain abgebildeten Werts oder Gegenstands verwendet, ohne dass damit bereits eine rechtliche Einordnung dieses Vorgangs verbunden wäre. Die in einer Blockchain gespeicherten - grundsätzlich für jeden einsehbaren - Transaktionsdaten sind als solche zunächst wirtschaftlich wie rechtlich neutral.[477] Von wirtschaftlicher Bedeutung ist allein der private key, der es demjenigen, der Zugriff auf ihn hat, faktisch ermöglicht, die dem Schlüs-

---

[470] Vgl. *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (88); *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (434, 439); *Börding/Jülicher/Röttgen/v. Schönfeld*, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134 (138); *Söbbing*, Smart Contracts und Blockchain-Technologie 2018, 43 (44 f.).
[471] Zutreffend *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (89).
[472] Vgl. *Spancken/Hellenkamp/Brown/Thiel,* Kryptowährungen und Smart Contracts, S. 59.
[473] *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (87, 91); *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505).
[474] Zum Vorschlag, smart contracts mit einer Schnittstelle zu einer Schiedsstelle zu versehen vgl. *Kaulartz/Heckmann*, Smart Contracts - Anwendungen der Blockchain-Technologie, CR 2016, 618 (624).
[475] Vgl. *Paulus/Matzke*, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769 (772).
[476] *Kaulartz/Heckmann*, Smart Contracts - Anwendungen der Blockchain-Technologie, CR 2016, 618 (620 ff.); *Bertram*, Smart Contracts, MDR 2018, 1416 (1418, 1420 f.).
[477] Vgl. *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 (3280).

sel zugeordneten Gegenstände an andere zu transferieren.[478] Mit einer Transaktion wird also die faktische Herrschaft über einen Datenbankeintrag, z.B. durch Anpassung der Salden, geändert.[479] Theoretisch kann einem private key über eine Blockchain jedes erdenkliche Gut, sei es eine bewegliche Sache, ein Grundstück, ein Recht oder ein sonstiger Gegenstand in Form eines Token zugeordnet werden.[480] Als Token (Wertmarke) wird der den Gegenstand oder Wert repräsentierende Eintrag bezeichnet.[481] Dabei kommt dem Token selbst grundsätzlich keine Rechtsqualität zu.[482] In der Literatur wird allerdings erwogen, Token unter bestimmten Voraussetzungen als Inhaberschuldverschreibungen im Sinne des § 793 BGB einzuordnen.[483]
Ob sich eine Transaktion über eine Blockchain-Anwendung lediglich als Realakt darstellt oder zugleich die Abgabe einer (konkludenten) Willenserklärung beinhaltet und ob sie zu einer Änderung der Rechtslage führt, bedarf der rechtlichen Bewertung nach den konkreten Umständen des Einzelfalls.[484] Der Umstand, dass eine Transaktion in der Blockchain eingetragen ist, besagt jedenfalls noch nichts über die Wirksamkeit des mit ihr in Zusammenhang stehenden Vertrages (vgl. hierzu im Einzelnen unter G.).[485]

E. Vertragsabschluss über eine Blockchain-Anwendung

Blockchain-Anwendungen dürften jedenfalls vorerst weniger der Vertragsanbahnung oder dem eigentlichen Abschluss des Vertrages als eher der Dokumentation des Vertragsschlusses und der Vertragsdurchführung dienen.[486] Nicht jede Transaktion, die über die Blockchain vorgenommen wird, muss als (konkludente) Willenserklärung im Rechtssinne einzuordnen sein. Mangels Sach- oder Rechtsqualität von Bitcoins[487] stellt sich deren „Überweisung" über die Bitcoin-Blockchain beispielsweise nach bislang wohl herrschender Meinung lediglich als Realakt dar,[488] mag dieser Vorgang auch im Einzelfall zugleich als konklu-

---

[478] Vgl. *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht, MMR 2014, 643 (644).
[479] Vgl. *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278.
[480] Vgl. *Müller*, Bitcoin, Blockchain und Smart Contracts, ZfIR 2017, 600 (608); *Breidenbach/Glatz*, Rechtshandbuch Legal Tech, 2018, S. 61, 70.
[481] Vgl. näher zum Begriff des Tokens: *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 ff.; *Breidenbach/Glatz*, Rechtshandbuch Legal Tech, 2018, S. 114.
[482] Vgl. *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278.
[483] Vgl. hierzu *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 (3281 ff.).
[484] Vgl. a. *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 (3280).
[485] *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (449).
[486] Vgl. *Heckmann/Schmid*, Studie Blockchain und Smart Contracts, 2017, S. 22 f.
[487] Zur rechtlichen Einordnung von virtuellen Währungen vgl. a. den Bericht der Arbeitsgruppe Digitaler Neustart vom 15. Mai 2017, S. 261 ff.
[488] *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (451); *Kaulartz*, Die Blockchain-Technologie, CR 2016, 474 (478); *Heckelmann*, Zulässigkeit

dentes Angebot oder als konkludente Annahme eines Angebots auf Abschluss eines Vertrages einzuordnen sein.
Jedenfalls ist kein Grund erkennbar, warum Willenserklärungen nicht über Blockchain-Anwendungen und Smart Contracts abgegeben werden und zugehen können sollten.[489] Ob zwei übereinstimmende Willenserklärungen vorliegen und ein Vertrag geschlossen worden ist, bestimmt sich nach allgemeinen Regeln und ist grundsätzlich losgelöst von der Abbildung einer Transaktion in der Blockchain zu beurteilen.[490]

I. Abgabe einer Willenserklärung

Abgegeben ist eine Willenserklärung, wenn der Erklärende alles getan hat, was für das Wirksamwerden der Willenserklärung erforderlich ist.[491] Für das Wirksamwerden einer empfangsbedürftigen Willenserklärung ist - außer dem Zugehen an den Erklärungsgegner - erforderlich, aber auch ausreichend, dass sie mit Willen des Erklärenden in den Verkehr gelangt ist und der Erklärende damit rechnen konnte und gerechnet hat, dass sie (sei es auch auf Umwegen) den richtigen Empfänger erreichen werde.[492] Soweit in der Vornahme einer Transaktion über eine Blockchain-Plattform auch eine empfangsbedürftige Willenserklärung im rechtlichen Sinne liegt, dürfte es für deren Abgabe darauf ankommen, dass die eingegebenen und signierten Transaktionsdaten unter Angabe des Empfängerschlüssels durch einen Eingabebefehl versendet werden, etwa durch die Betätigung eines Absendebuttons.[493] Allein das Signieren von Daten dürfte demgegenüber jedenfalls bei empfangsbedürftigen Willenserklärungen noch keine Abgabe darstellen,[494] solange mit der Signatur nicht zugleich die Versendung ausgelöst wird. Weitere Bewertungen hängen von der Ausgestaltung der Anwendung im Einzelfall ab.

---

und Handhabung von Smart Contracts, NJW 2018, 504 (508); *Kuhlmann*, Bitcoins, CR 2014, 691 (696).

[489] Vgl. für Smart Contracts: *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (88); *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (434, 439); *Börding/Jülicher/Röttgen/v. Schönfeld*, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134 (138); *Söbbing*, Smart Contracts und Blockchain-Technologie 2018, 43 (44 f.).

[490] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (448).

[491] MüKo-*Einsele*, BGB, § 130 Rn. 13.

[492] BGH, Urt. v. 11.5.1979 – V ZR 177/77 –, Rn. 12, juris sowie Urt. v. 30.1.2018 – X ZR 119/15 –, Rn. 34, juris.

[493] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (445 ff.)

[494] A.A. wohl *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (505).

II. Zugang einer Willenserklärung

Gibt jemand den öffentlichen Schlüssel, den er zur Vornahme von Transaktionen über eine Blockchain-Anwendung generiert hat, anderen bekannt, wird man darin grundsätzlich auch die Widmung der Kommunikationswege der entsprechenden Blockchain-Plattform zum Empfang rechtserheblicher Erklärungen jedenfalls für Geschäfte sehen können, die über die Plattform gerade abgewickelt werden.

Eine empfangsbedürftige Willenserklärung geht (vorbehaltlich einer früheren tatsächlichen Kenntnisnahme) zu, sobald sie derart in den Machtbereich des Empfängers gelangt, dass bei Annahme gewöhnlicher Verhältnisse damit zu rechnen ist, er könne von ihr Kenntnis erlangen.[495] Bei Emails wird angenommen, dass diese in dem Moment in den Machtbereich des Empfängers gelangen, in dem sie der Email-Anbieter im elektronischen Postfach des Empfängers speichert[496] oder sie auf dem Server des Haus-(Access-)Providers des Empfänger eingehen,[497] unabhängig davon, zu welchem Zeitpunkt man eine Kenntnisnahme durch Abruf der Email nach gewöhnlichen Verhältnissen aufgrund der Lebensgewohnheiten oder Geschäftsgepflogenheiten normativ-wertend unterstellen will.[498] Da über Blockchain-Anwendungen nicht bilateral, sondern öffentlich über das gesamte Netzwerk zwischen einer grundsätzlich unbegrenzten Zahl von Knoten kommuniziert wird, ist für die Frage des Zugangs einer Willenserklärung zunächst festzustellen, wann der Empfänger einer über die Blockchain-Plattform abgegebenen Willenserklärung aus technischer Sicht überhaupt (erstmals) die Möglichkeit erhält, eine in einer versendeten Transaktion enthaltene Erklärung zur Kenntnis zu nehmen. In einem zweiten Schritt ist zu prüfen, wann unter Berücksichtigung der technischen Gegebenheiten und Abläufe mit einer Kenntnisnahme sodann gerechnet werden darf. Neu eingegebene Transaktionen werden in der öffentlich zugänglichen Blockchain per Broadcast an alle Knoten des Netzwerkes gesendet.[499] Die bloße Möglichkeit zur Kenntnisnahme dürfte daher ab dem Zeitpunkt bestehen, in dem die Daten auf dem Rechner des Empfängers eingehen. Da jedoch bei jedem Knoten grundsätzlich alle Transaktionen

---

[495] Vgl. BGH, Urt. v. 26.11.1997 – VIII ZR 22/97 –, BGHZ 137, 205-211, Rn. 14.

[496] *Greiner/Kalle*, Ungeklärte Fragen des Wirksamwerdens empfangsbedürftiger Willenserklärungen - im Grundsatz und bei Verwendung digitaler Kommunikationswege, JZ 2018, 535 (538); vgl. Herberger/Martinek/Rüßmann u.a./*Reichold*, jurisPK-BGB, § 130 Rn. 17; MüKo-*Einsele*, § 130 BGB Rn. 18.

[497] *Haug,* Grundwissen Internetrecht, 3. Auflage, S. 274; vgl. a. Palandt-*Ellenberger*, § 130 BGB Rn.7a.

[498] Vgl. insbesondere zu der Frage, ob wegen der Vielgestaltigkeit der Lebens- und Geschäftsgewohnheiten sowie der Kommunikationsgepflogenheiten eine deutlichere Betonung des tatsächlichen Elements innerhalb des Zugangsbegriffs unter Zurückdrängung des normativ-wertenden Elements veranlasst ist, *Greiner/Kalle*, Ungeklärte Fragen des Wirksamwerdens empfangsbedürftiger Willenserklärungen - im Grundsatz und bei Verwendung digitaler Kommunikationswege, JZ 2018, 535 ff.

[499] Vgl. *Spancken/Hellenkamp/Brown/Thiel,* Kryptowährungen und Smart Contracts, S. 12.

unabhängig davon eingehen, an wen sie adressiert sind, und bei größeren allgemein zugänglichen Blockchains fortlaufend neue Transaktionen versendet werden könnten, die sodann automatisiert weiterverarbeitet werden, wird man für eine unterstellte Kenntnisnahme „unter gewöhnlichen Umständen“ jedenfalls nicht immer schon an den Eingang einer Transaktion auf dem Rechner des Empfängers anknüpfen können. Ebenso wenig wird man - jedenfalls bei großen Blockchains - erwarten dürfen, dass jeder Teilnehmer alle gebildeten Blöcke regelmäßig auf eine an ihn adressierte Transaktion hin untersucht. Allgemeingültige Aussagen werden sich hier kaum treffen lassen, da die Beurteilung u.a. von Art, Größe und Ausgestaltung der konkret genutzten Blockchain-Anwendung im jeweiligen Fall abhängen wird.[500] Anhaltspunkte dafür, dass eine Einordnung im Einzelfall auf Grundlage der hinreichend abstrakt gehaltenen Regelung des § 130 BGB sowie der hierzu von Rechtsprechung und Lehre herausgebildeten Grundsätze nicht zu bewerkstelligen wäre, sind jedenfalls nicht vorhanden.

Soweit Willenserklärungen z.B. durch Smart Contracts automatisiert ausgelöst werden, kann im Übrigen, vor allem hinsichtlich der Frage, wem Erklärungen zuzurechnen sind, auf die Ausführungen der Arbeitsgruppe zu Vertragsschlüssen durch Roboter in ihrem Bericht vom 15. Mai 2017[501] verwiesen werden. Blockchainspezifische Besonderheiten, die eine abweichende Beurteilung rechtfertigen oder gar ein gesetzgeberisches Handeln erfordern würden, sind bisher nicht ersichtlich.

F. Pflichten im elektronischen Geschäftsverkehr (§§ 312i, 312j BGB)

Wird ein Smart Contract zum Abschluss eines Vertrages über die Lieferung von Waren oder die Erbringung von Dienstleistungen genutzt, hat der Unternehmer bei dem Einsatz von Telemedien die allgemeinen Pflichten im elektronischen Geschäftsverkehr nach § 312i BGB einzuhalten, also u.a. dem Kunden die nach Art. 246c EGBGB vorgeschriebenen Informationen rechtzeitig vor dessen Bestellung klar und verständlich mitzuteilen und den Zugang der Bestellung unverzüglich auf elektronischem Weg zu bestätigen. Gegenüber Verbrauchern sind zusätzlich die besonderen Pflichten im elektronischen Geschäftsverkehr nach § 312j BGB zu beachten. U.a. hat der Unternehmer in diesen Fällen dafür Sorge zu tragen, dass der Verbraucher mit seiner Bestellung ausdrücklich bestätigt,

---

[500] *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (447), wollen darauf abstellen, dass die in einer Transaktion enthaltene Willenserklärung Eingang in die speziell von dem Empfänger für an ihn adressierte Transaktionen vorgehaltene Wallet findet. *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (506), schlägt vor, an das Anhängen des neuen Blocks an die Blockchain anzuknüpfen.

[501] Arbeitsgruppenbericht „Digitaler Neustart“ vom 15. Mai 2017, S. 102 ff.

sich zur Zahlung zu verpflichten, ggf. über eine eindeutig zu beschriftende Schaltfläche (sog. Button-Lösung). Ein Smart Contract zum Einsatz im elektronischen Geschäftsverkehr mit Verbrauchern wird also über eine entsprechend benutzerfreundlich ausgestaltete Oberfläche verfügen müssen.[502]

G. Wirksamkeit des Vertrags

I. Nichtigkeitsgründe (§ 125, § 134, § 138, § 142 BGB)

Das Gesetz sieht in näher geregelten Fällen vor, dass ein Rechtsgeschäft von Anfang an nichtig ist, so etwa in § 125 S. 1, § 134, § 138 und § 142 Abs. 1 BGB. Es stellt sich die Frage, ob die Rechtsfolge dieser Vorschriften sich auch in den Fällen umsetzen lässt, in denen die Blockchain-Technologie zum Einsatz kommt.

Teilweise[503] wird dies bezweifelt und die Besorgnis geäußert, das deutsche Zivilrecht sei insoweit auf eine Technologie mit einer unveränderlichen Transaktionshistorie nicht vorbereitet. Eine Blockchain sei darauf angelegt, die vorgenommenen Transaktionen dauerhaft zu speichern. Es sei deshalb unmöglich, Nichtigkeitstatbestände von Anfang an zu berücksichtigen und zu vermeiden, dass zivilrechtlich nichtige Transaktionen in der Blockchain niedergelegt würden. Nach heutigem Stand sei es nicht möglich, die Nichtigkeit einer Transaktion maschinell überprüfen zu lassen. Genau dies sei aber das Prinzip der Blockchain: Rechner überprüften aufgrund vorhergehender Transaktionsdaten, ob sie einer neuen Transaktion vertrauten und schrieben diese, wenn das der Fall sei, unveränderlich in die Blockchain.

Jene Bedenken werden von der Arbeitsgruppe nicht geteilt.[504] Es muss stärker berücksichtigt werden, dass zwischen den rechtsgeschäftlichen Fragen auf der einen Seite und der Vertragsdurchführung auf der anderen Seite zu differenzieren ist. Richtig ist zwar, dass die bestätigten Transaktionen nach der Architektur der Blockchain chronologisch und unveränderbar gespeichert werden. Auch ist richtig, dass die Prüfung, ob ein Vertrag nichtig ist, nach heutigem Stand nicht maschinell erfolgen kann. Hieraus lässt sich aber nicht der Schluss ziehen, dass

---

[502] Vgl. zu weiteren Einzelheiten auch *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (458 f.).
[503] Vgl. *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1435); s. auch *Kilian*, Die Zukunft des Juristen, NJW 2017, 3043 (3050).
[504] Wie hier *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (91); *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (435, 460); vgl. auch *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).

die Blockchain-Technologie in einem unauflösbaren Spannungsverhältnis mit den Nichtigkeitsvorschriften des BGB steht. In der Blockchain werden tatsächliche Vorgänge lediglich protokolliert; bei den Einträgen handelt es sich um formelle Statusabbildungen.[505] Der Umstand, dass ein Vertrag in der Blockchain abgebildet wird, besagt nicht, dass der Vertrag als wirksam behandelt werden müsste. Die Blockchain, insbesondere auch ein Smart Contract, vollzieht keine juristischen Wertungen.[506] Der Kontrollprozess innerhalb des Blockchain-Netzwerkes beschränkt sich vielmehr darauf, ob die Informationen den syntaktischen Voraussetzungen des zugrundeliegenden Algorithmus genügen und ob sie in Einklang mit den bereits in der Blockchain gespeicherten Informationen stehen.[507] Das Netzwerk sichert insoweit (nur) die Einhaltung der durch das Anwendungsprotokoll vorgegebenen Regeln.[508] Es prüft, ob eine lückenlose Kette von Transaktionen zu der Empfängeradresse des die neue Transaktion Initiierenden gibt und der zu transferierende Token noch nicht anderweitig weitergegeben wurde.[509] Der Nutzer der Blockchain kann mithin darauf vertrauen, dass alle Informationen in sich korrekt und grds. irreversibel in die Blockchain aufgenommen wurden, etwa dass die dort abgebildeten Erklärungen – in tatsächlicher Hinsicht – abgegeben wurden,[510] nicht aber, dass die Rechtslage auch zutreffend wiedergegeben wird.[511] Rein äußerlich mag die Blockchain zwar an öffentliche Register wie Grundbuch oder Handelsregister erinnern.[512] Öffentliche Register wie Grundbuch oder Handelsregister zeichnen sich jedoch dadurch aus, dass die durch sie verlautbarten Informationen durch staatliche Stellen wie das Grundbuchamt und das Registergericht geprüft werden. Es ist zwar denkbar, in einer Blockchain Rechte zu dokumentieren. Der Blockchain kommt aber vorbehaltlich etwaiger künftiger gesetzlicher Regelungen keine besondere Rechtsscheinwirkung zu.[513] Es verbleibt vielmehr bei den allgemeinen gesetzlichen

---

[505] *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (460).

[506] Zutr. *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).

[507] *Saive,* Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 186 (189 f.).

[508] Vgl. *Breidenbach/Glatz*, Rechtshandbuch Legal Tech, 2018, S. 114.

[509] Vgl. a. *Blocher/Hoppen/Hoppen*, Softwarelizenzen auf der Blockchain, CR 2017, 337 (340); *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379.

[510] Vgl. *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).

[511] Vgl. *Saive,* Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 186 (190); *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (508).

[512] Vgl. *Blocher/Hoppen/Hoppen*, Softwarelizenzen auf der Blockchain, CR 2017, 337 (339); *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379 (382).

[513] Vgl. *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (508); *Bialluch-von Allwörden/von Allwörden*, Initial Coin Offerings: Kryptowährungen als

Regeln hinsichtlich eines gutgläubigen Erwerbs vom Nichtberechtigten, soweit deren Anwendungsbereich eröffnet ist (etwa §§ 932 ff. BGB beim Erwerb beweglicher Sachen).[514]

Mithin kann es jederzeit zu einer Diskrepanz zwischen der in der Blockchain abgebildeten Zuordnung und der tatsächlichen Rechtslage kommen, weil beispielsweise das dem Transfer in der Blockchain zugrundeliegende Rechtsgeschäft nichtig ist.[515] Wird auf der Grundlage der Blockchain-Technologie ein von Anfang nichtiger Vertrag vollzogen, so ändert die Technologie nichts daran, dass die auf der Grundlage des Smart Contracts ausgelöste Erfüllungshandlung ohne Rechtsgrund erfolgt ist und eine Rückgewähr der Leistungen nach allgemeinen Regeln stattzufinden hat. Dem Interesse daran, dass in der Blockchain nur solche Transaktionen protokolliert sind, die auf der Grundlage wirksamer Verträge vollzogen werden, kann dadurch Rechnung getragen werden, dass auch der Umstand, dass eine in der Blockchain angelegte Verfügung rückgängig gemacht wurde, in der Blockchain verlautbart wird. Eine Möglichkeit kann insoweit darin bestehen, in die Blockchain sog. Reverse Transactions einzutragen, die dafür sorgen, dass gegenläufige Transaktionen solange in die Blockchain eingeführt werden, bis der Zustand erreicht ist, welcher der echten Rechtslage entspricht (vgl. hierzu A.IX).[516]

Ein etwaiges Vertrauen des Rechtsverkehrs in die Richtigkeit der Transaktionshistorie wird durch die hier aufgezeigte Gefahr der fehlerhaften Protokollierung jedenfalls nicht in einem solchen Maß erschüttert, dass der Gesetzgeber handeln müsste, zumal der Rechtsverkehr auch abseits der Blockchain-Technologie an die Unsicherheiten gewöhnt ist, die daraus folgen mögen, dass ein Vertrag unerkannt von Anfang an nichtig sein kann.

Wertpapier oder Vermögensanlage?, WM 2018, 2118 (2121); a.A. *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379 ff.

[514] V*gl. Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436); *Bialluch-von Allwörden/von Allwörden*, Initial Coin Offerings: Kryptowährungen als Wertpapier oder Vermögensanlage?, WM 2018, 2118 (2121 f.); *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 (3283) sowie *Kuhlmann*, Bitcoins, CR 2014, 691 (696), der allerdings zu bedenken gibt, der private Schlüssel ersetze in seiner Funktion die physische Übergabe und stünde als Rechtsscheinträger zur Verfügung.

[515] *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (437); *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (508).

[516] Insoweit übereinstimmend *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

Teilweise[517] wird angenommen, es bestehe deshalb ein gesetzgeberischer Handlungsbedarf, weil es an einer tauglichen Kontrollmöglichkeit fehle, ob im Rahmen der Programmgestaltung die Grenzen der Vertragsfreiheit, also etwa § 134 BGB oder § 138 BGB, eingehalten werden. Auch dies überzeugt nicht. Der Umstand, dass die hier interessierenden Verträge sich gleichsam von selbst erfüllen, gebietet es nicht, dass die in der Praxis eingesetzten Smart Contracts einer Vorab-Kontrolle unterzogen werden. Dass Verträge vollzogen werden, die gegen ein gesetzliches Verbot oder gegen die guten Sitten verstoßen, ist dem Gesetz keineswegs fremd. Es hält (insbesondere) in den §§ 812 ff. BGB ein bewährtes Instrumentarium bereit; für die Rückabwicklung des automatisierten Leistungsaustauschs bedarf es freilich „manueller" Maßnahmen.[518]

Die bei dem Einsatz der Blockchain-Technologie möglicherweise steigende Gefahr einer von der materiellen Rechtslage abweichenden Güterzuordnung erhöht die Bedeutung der Vorschriften über die Rückabwicklung und ist kein Umstand, der gegen die generelle Tauglichkeit der Technologie spricht. Es kann freilich sein, dass die Realisierung jener Ansprüche sich mitunter als problematisch erweisen kann, weil diejenigen Personen, welche auf die Blockchain-Technologie zurückgreifen, nicht zwingend unter Preisgabe ihrer Identität agieren, sondern – sofern das Programm, also der jeweilige Smart Contract es zulässt – anonym handeln. Dieses Risiko, das vorwiegend die Anspruchsdurchsetzung betrifft, besteht jedoch immer dann, wenn man sich auf einen Vertragspartner einlässt, dessen Identität man vorab nicht zuverlässig feststellt. Zwar kann auch der Staat ein Interesse daran haben, dass rechtlich nicht zu billigende Verträge, die bereits vollzogen wurden, rückabgewickelt werden, so dass die rechtswidrige Güterzuordnung jedenfalls nicht von Dauer ist. Aber auch dies rechtfertigt keinen Handlungsbedarf auf zivilrechtlicher Ebene. Soweit strafrechtlich relevante Handlungen im Raum stehen, können die strafprozessualen Möglichkeiten genutzt werden, um die Identität zu klären; ob insoweit ein gesetzgeberischer Handlungsbedarf besteht, ist von der hiesigen Arbeitsgruppe nicht zu prüfen. Dasselbe gilt für die Frage, ob die fehlende Möglichkeit, die rechtlich missbilligte und in der Blockchain bereits angelegte Transaktion präventiv zu unterbinden,[519] einen gesetzgeberischen Handlungsbedarf auslöst; dieser würde – wenn überhaupt – auf öffentlich-rechtlichem und ggf. auf strafrechtlichem Gebiet liegen.

---

[517] *Djazayeri*, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016, Anm. 1.

[518] Vgl. *Linartados*, Smart Contracts – einige klarstellende Bemerkungen, K&R 2018, 85 (91), der darauf hinweist, dass – bei der insoweit erforderlichen Gesamtbetrachtung – durch die Notwendigkeit manueller Rückabwicklung derjenige wirtschaftliche Vorteil relativiert wird, der beim Einsatz eines Smart Contracts in eingesparten Transaktionskosten angestrebt wird.

[519] Hierzu *Müller*, Bitcoin, Blockchain und Smart Contracts, ZfIR 2017, 600 (609).

II. Insbesondere: Anfechtung von computererzeugten Willenserklärungen

Es kann sich die Frage stellen, unter welchen Voraussetzungen eine computergenerierte Willenserklärung angefochten werden kann.[520] Dies muss hier nicht weiter vertieft werden; diese Frage wurde bereits an anderer Stelle geprüft. Dass insoweit kein gesetzgeberischer Handlungsbedarf besteht, hat die Arbeitsgruppe in ihrem Bericht vom 15. Mai 2017[521] festgestellt. Die dort angestellten Erwägungen gelten auch dann, wenn die Willenserklärung unter Verwendung der Blockchain-Technologie generiert wurde.

III. Schwebende Unwirksamkeit bei Beteiligung von Minderjährigen

Gem. § 108 Abs. 1 BGB hängt die Wirksamkeit des Vertrags von der Genehmigung des Vertreters ab, wenn der Minderjährige einen Vertrag ohne die erforderliche Einwilligung (vgl. § 107 BGB) des gesetzlichen Vertreters schließt; der Vertrag ist bis zur Genehmigung schwebend unwirksam. Während des Schwebezustands soll – so die Konzeption des Gesetzes – der Vertrag nicht vollzogen werden. Gerade dies stößt aber bei der Verwendung eines Smart Contracts auf Probleme. Dieser lebt davon, dass die veranlasste Transaktion unabhängig von weiteren Umständen und streng nach den zuvor angelegten Wenn-Dann-Verknüpfungen ausgeführt wird; es gibt nur bestätigte oder abgelehnte Transaktionen.[522] Dies führt dazu, dass bei der Verwendung eines Smart Contracts eine höhere Gefahr dafür besteht, dass ein Vertrag, der wegen § 108 Abs. 1 BGB schwebend unwirksam ist, vollzogen wird.[523] Auch dies begründet jedoch keinen gesetzgeberischen Handlungsbedarf. Vielmehr kann zunächst abgewartet werden, ob es in der Praxis tatsächlich zu einer messbaren Verkürzung des Minderjährigenschutzes kommt. So kann heute noch nicht verlässlich vorausgesehen werden, ob die Problematik bereits dadurch entschärft wird, dass die Bedingungen des Smart Contracts einen hinreichenden technischen Schutz bieten oder in den einschlägigen Blockchains von vornherein die Geburtsdaten der potentiellen Transaktionsteilnehmer zu hinterlegen sind.[524] Im Übrigen kann derzeit davon ausgegangen werden, dass die Rechtsprechung auf der Grundlage des geltenden Rechts einen interessengerechten Weg entwickeln wird.

---

[520] Dazu etwa *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (454 ff.).
[521] Arbeitsgruppe „Digitaler Neustart", Bericht vom 15. Mai 2017, S. 105 ff.
[522] Vgl. *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).
[523] Vgl. *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).
[524] Vgl. *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436), der allerdings zugleich auf die verbleibende Problematik zu § 110 BGB hinweist.

IV. Schwebende Unwirksamkeit bei Vertretung ohne Vertretungsmacht

Die obigen Überlegungen zur schwebenden Unwirksamkeit in den Fällen von § 108 Abs. 1 BGB gelten entsprechend in dem Fall, dass für den Prinzipal ein Vertreter ohne Vertretungsmacht agiert; auch in diesem Fall ist der vom Vertreter geschlossene Vertrag zunächst schwebend unwirksam (vgl. § 177 Abs. 1 BGB).

V. Welchen Formanforderungen genügt die Blockchain-Technologie?

Gem. § 125 S. 1 BGB ist ein Rechtsgeschäft, welches der durch Gesetz vorgeschriebenen Form ermangelt, nichtig. Das ist auch dann zu beachten, wenn ein Vertrag mittels eines Smart Contracts abgeschlossen wird, es also um den bereits oben angesprochenen Fall geht, dass die erforderlichen Willenserklärungen, die auf den Abschluss oder die Änderung eines Vertrages gerichtet sind, durch das Programm generiert werden.[525]

Es ist im Einzelfall zu prüfen, ob für das in Rede stehende Rechtsgeschäft ein gesetzliches Formerfordernis gilt. Das ist etwa dann der Fall, wenn – wie gem. § 311b Abs.1 BGB bei Grundstücksgeschäften – die notarielle Beurkundung gefordert wird, aber auch dann, wenn das Gesetz – wie § 492 Abs. 1 S. 1 BGB für die Erklärung des Darlehensnehmers beim Verbraucherdarlehensvertrag – die Schriftform voraussetzt.

Die Schriftform i.S. von § 126 Abs. 1 BGB wird weder durch einen etwaigen Eintrag in der Blockchain noch dadurch gewahrt, dass die automatisierte Willenserklärung in einer sog. Wallet abgespeichert wird;[526] letzteres genügt allerdings grds. den Anforderungen eines Textformerfordernisses gem. § 126b BGB,[527] was nach § 492 Abs. 1 S. 3 BGB beim Verbraucherdarlehensvertrag für die Erklärung des Darlehensgebers von Bedeutung sein kann. Aus demselben Grund kann für Mietverträge, die mithilfe eines Smart Contracts geschlossen werden, keine wirksame Befristung von mehr als einem Jahr vereinbart werden (vgl. § 550 S. 1 BGB i.V.m. § 578 BGB).[528]

---

[525] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (457).
[526] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (457).
[527] *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507); *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (457).
[528] *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (457).

Der Eintrag in einer Blockchain wahrt auch nicht die Anforderungen des § 126a Abs. 1 BGB. Nach dieser Vorschrift kann die schriftliche Form durch die elektronische Form nur dann ersetzt werden, wenn das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen werden kann; derzeit ist dies bei der Verwendung eines Smart Contracts, bei dem die Blockchain-Technologie eingesetzt wird, in technischer Hinsicht wohl nicht möglich.[529] Es ist derzeit nicht erkennbar, dass der Gesetzgeber insoweit handeln sollte. Eine Rechtfertigung dafür, bei der Verwendung der Blockchain-Technologie von den geltenden Anforderungen an die Schriftform abzuweichen, insbesondere von dem Erfordernis einer qualifizierten elektronischen Signatur abzusehen, ist nicht ersichtlich.

Heckelmann[530] weist zutreffend darauf hin, dass trotz jener Ausgangssituation auch bei formgebundenen Rechtsgeschäften die Blockchain-Technologie zum Einsatz kommen kann. Haben die Parteien ein Interesse daran, dass die beabsichtigte Transaktion in der Blockchain abgebildet wird, so können sie die erforderlichen Willenserklärungen formgerecht außerhalb der Blockchain abgeben und sich verpflichten, das Ergebnis ihrer Abrede „zwecks Auslösung der Smart-Contract-Mechanismen anschließend informell in die Blockchain zu überführen."[531]

Den Parteien eines nach dem Gesetz formfreien Vertrages steht es selbstverständlich auch frei, ein rechtsgeschäftliches Formerfordernis zu begründen. Bei der inhaltlichen Ausgestaltung gilt der Grundsatz der Privatautonomie. Aus diesem Grund ist es ihnen auch möglich, die Wirksamkeit des Rechtsgeschäfts davon abhängig zu machen, dass die Abreden in die Blockchain eingetragen und dort abgebildet werden.[532] Auch insoweit stellt sich kein gesetzgeberischer Handlungsbedarf.

H. AGB-Recht

Wie bereits oben dargestellt, ist gedanklich zwischen dem Rechtsgeschäft und dem Smart Contract zu unterscheiden. Bei dem Smart Contract handelt es sich um ein Computerprogramm; Allgemeine Geschäftsbedingungen (AGB) liegen

---

[529] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (457).
[530] *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).
[531] *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).
[532] *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (458).

insoweit nicht vor.[533] Der Smart Contract kann Gegenstand von AGB sein, „nicht jedoch die AGB selbst."[534]

Demgegenüber gelten für das Rechtsgeschäft die allgemeinen Regeln, damit ist auch das AGB-Recht anwendbar. Die vertragliche Abrede, in der vorgesehen ist, dass etwa für die Vertragsdurchführung auf einen Smart Contract zurückgegriffen und wie dieser inhaltlich ausgestaltet wird, muss sich an den §§ 305 ff. BGB messen lassen und damit insbesondere der Inhaltskontrolle gem. §§ 307 ff. BGB standhalten;[535] dasselbe gilt für einen Vertrag, der auf der Grundlage von Willenserklärungen zustande kommt, die von einem Smart Contract generiert werden.[536]

Vor diesem Hintergrund wird es regelmäßig nicht zulässig sein, formularmäßig zu bestimmen, dass einer Transaktion, welche durch den Smart Contract ausgelöst wird, keine Einwendungen entgegengehalten werden können. *Schrey/Thalhofer*[537] führen insoweit das Beispiel an, dass einem Mieter von Wohnraum, der die Miete nicht vollständig entrichtet habe, auf der Grundlage eines Smart Contracts der Zugang zur Mietwohnung verwehrt wird.[538] Eine entsprechende Abrede nimmt dem Mieter etwa die Möglichkeit, eine Mietminderung wegen Mängeln der Mietsache gegen die Mietforderung geltend zu machen; hierin dürfte ein Verstoß gegen § 309 Nr. 2 BGB, jedenfalls gegen § 307 Abs. 1 S. 1, Abs. 2 BGB liegen.[539] Auf diesem Wege werden der automatisierten Durchsetzung von Forderungen bereits nach dem geltenden Recht taugliche Grenzen gesetzt.[540] Es ist derzeit nicht erkennbar, dass der Gesetzgeber diese Grenzen im Hinblick auf die Blockchain-Technologie und den Einsatz von Smart Contracts verschärfen müsste.

Auf ein spezielles Problem im Zusammenhang mit sog. Peer-to-Peer-Krediten weist *Heckelmann*[541] hin. Kennzeichnend für AGB sei, dass sie bei einer Vielzahl von Verträgen zum Einsatz kommen sollen. Ein wichtiger Einsatzbereich von Smart Contracts werde es sein, dass nicht ein Verwender den Vertrag in einer Vielzahl, sondern dass eine Vielzahl von Verwendern den Vertrag einmal nutzt. So führe eine Plattform für Peer-to-Peer-Kredite eine Vielzahl von Transaktionen auf Basis desselben Smart Contracts durch, bei der jeder Darlehens-

---

[533] Zutr. *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (459); insoweit nicht ganz klar *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

[534] *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (459).

[535] Vgl. *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

[536] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB – Viel Lärm um Nichts? –, ZfPW 2018, 431 (459).

[537] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

[538] Zur Frage der verbotenen Eigenmacht vgl. auch die Ausführungen unter K.

[539] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

[540] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

[541] *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).

nehmer nur einen Kredit benötige, die meisten Geber nur ein Darlehen ausreichten und der Plattformbetreiber selbst nicht am Darlehensvertrag beteiligt sei. Hier bestehe die Absicht, die jeweiligen Vertragsbestimmungen vielfach zu verwenden, lediglich bei dem Plattformbetreiber, nicht aber bei den Parteien des Darlehensvertrags. Zwar nehme die Rechtsprechung eine Vielfachverwendungsabsicht auch dann an, wenn der Verwender die von dritter Seite vorformulierten Klauseln selbst nur ein einziges Mal zum Einsatz bringen wolle und bringe.[542] In den hier interessierenden Fällen sei aber gar nicht klar, welche Seite des Darlehensvertrags als Verwender anzusehen sei; aus diesem Grunde heraus scheitere die Anwendbarkeit des AGB-Rechts.[543]

Hier muss nicht abschließend geklärt werden, ob jene Sichtweise überzeugt. Schutzlücken, die der Gesetzgeber schließen müsste, sind nach Auffassung der Arbeitsgruppe nicht absehbar. Es kann vielmehr der Rechtsprechung überlassen werden, ob der Begriff des „Stellens" (vgl. § 305 Abs. 1 S. 1 BGB) unter Berücksichtigung neuer Einsatzformen weiter zu entwickeln ist. Darüber hinaus ist zu bedenken, dass jedenfalls der Teilnahmevertrag zwischen dem Plattformbetreiber und den Nutzern der AGB-rechtlichen Inhaltskontrolle unterworfen sein dürfte. Aus diesem Grund wird der Plattformbetreiber – auch unter Berücksichtigung einer andernfalls drohenden Verbandsklage nach § 1 UKlaG – regelmäßig darauf verzichten, den Inhalt der – im Teilnahmevertrag wohl „vorgegebenen" – Kreditverträge unangemessen zu gestalten; das kann die von *Heckelmann* angenommene Schutzlücke verkleinern. Jedenfalls kann die weitere Entwicklung zu dieser Frage abgewartet werden; ein aktueller Handlungsbedarf des Gesetzgebers ist nicht erkennbar.

I. Beispiel: Smart Contracts im Versicherungswesen

Für Versicherer ist der Einsatz von Smart Contracts zum Beispiel zur effizienten Schadensbearbeitung oder zur Kalkulation und Anpassung von Versicherungsprämien von Interesse.

So wird bereits eine Flugverspätungsversicherung angeboten, die nach Angaben des Anbieters auf Blockchain-Basis verwaltet wird.[544] Der Abschluss des Versicherungsvertrags erfolgt über die Internetseite des Versicherers. Die Daten des versicherten Flugs werden in einem Smart Contract hinterlegt, der nach der Landung die tatsächliche mit der planmäßigen Ankunftszeit abgleicht. Wird für den versicherten Flug eine Verspätung von mehr als zwei Stunden festgestellt,

---

[542] Vgl. BGH, Urt. v. 4.5.2000 – VII ZR 53/99, NJW 2000, 2988 (2989).

[543] *Heckelmann*, Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504 (507).

[544] https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy, letzter Abruf: 25.3.2019; vgl. a. *Skwarek*, Transparente Automatisierung durch Smart Contracts, https://www.it-finanzmagazin.de/automatisierung-smart-contracts-81819/, letzter Abruf: 13.2.2019, der die Frage aufwirft, ob der Einsatz der Blockchain hier überhaupt notwendig und zweckmäßig ist.

wird die dafür vereinbarte Versicherungssumme automatisiert an den Versicherungsnehmer ausgezahlt, ohne dass es einer Schadensmeldung bedürfte.[545]
Smart Contracts könnten künftig zudem im Zusammenhang mit sog. Telematiktarifen eingesetzt werden. Aktuell werden bereits Nachlässe auf die Prämie für die Kfz-Versicherung auf Grundlage der Bewertung der individuellen Fahrweise gewährt („pay as you drive"-Tarife). Es ist jedenfalls vorstellbar, dass die Analyse der erhobenen Daten und die anschließenden Maßnahmen zur Tarifanpassung durch Smart Contracts vereinfacht und beschleunigt werden.
In diesem Zusammenhang stellen sich allgemeine versicherungsvertragsrechtliche und vor allem datenschutzrechtliche Fragen.[546] Die auftretenden zivilrechtlichen Fragen hat die Unterarbeitsgruppe mit Experten für Versicherungsrecht aus der Rechtswissenschaft[547] ausführlich erörtert. Danach bestand Einvernehmen, dass die zu erwartenden Probleme denjenigen entsprechen, die sich generell bei dem Abschluss und/oder der Abwicklung von Versicherungsverträgen unter Einsatz des Internets ergeben. Blockchainspezifische Sonderprobleme sind im Bereich des Versicherungsvertragsrechts hingegen bislang nicht erkennbar. Es kann daher aus derzeitiger Sicht auch hier der Rechtsprechung überlassen werden, angemessene Lösungen für auftretende Streitfälle zu finden.

J. Rücktritt

Gem. § 346 Abs. 1 BGB sind im Falle des Rücktritts die empfangenen Leistungen zurückzugewähren und die gezogenen Nutzungen herauszugeben; der Rücktritt hat also zur Folge, dass ein Rückgewährschuldverhältnis entsteht. Teilweise[548] wird die Auffassung vertreten, dass dann, wenn der Rücktritt sich auf einen Vertrag bezieht, der unter Rückgriff auf die Blockchain-Technologie durchgeführt wurde, eine Rückabwicklung nur über die bereits angesprochenen „Reverse Transactions" in Betracht komme; diese „Reverse Transactions" hätten jedoch „nur wirtschaftlich, aber nicht rechtlich den Effekt einer Rückabwicklung". Das überzeugt in dieser Form nicht. Wird auf der Grundlage von „Reverse Transactions" diejenige Güterzuordnung erreicht, auf die gem. § 346 Abs. 1 BGB ein Anspruch besteht, so wird nicht nur wirtschaftlich, sondern auch in rechtlicher Hinsicht eine Rückabwicklung erreicht.

---

[545] Vgl. zu allen Einzelheiten die Angaben des Versicherers unter https://fizzy.axa/en-gb/faq, letzter Abruf: 13.2.2019.
[546] Vgl. etwa *Armbrüster/Greis*, Telematik in der Kfz-Versicherung aus rechtlicher Sicht ZfV 2015, 457 ff.; *Rudkowski*, Vertragsrechtliche Anforderungen an die Gestaltung von „Self-Tracking"-Tarifen in der Privatversicherung, ZVersWiss (2017) 106, 453 ff.; *Rubin,* Inhalt und versicherungsrechtliche Auswirkungen der Datenschutz-Grundverordnung, r+s 2018, 337 ff.
[547] Prof. Dr. Christian Armbrüster, Freie Universität Berlin, Lehrstuhl für Bürgerliches Recht, Handels- und Gesellschaftsrecht, Privatversicherungsrecht und Internationales Privatrecht, sowie die wissenschaftlichen Mitarbeiter Felix Greis und Adrian Sempf.
[548] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436).

Besteht infolge Rücktritts ein Anspruch auf Rückabwicklung eines vorgenommenen Bitcoin-Transfers wird man in Anlehnung an die Rechtsprechung des Bundesgerichtshofs, dass empfangene Geldleistungen im Rahmen des § 346 BGB durch Rückzahlung des Geldwerts auszugleichen sind,[549] annehmen können, dass es genügt, eine wirtschaftliche Gleichstellung durch den Transfer einer gleich hohen Summe von Bitcoins herzustellen.[550] Davon zu trennen ist die Frage, ob es dem Rückgewähr- oder Bereicherungsschuldner nach § 244 BGB erlaubt sein könnte, seiner Verpflichtung zum Rücktransfer von Bitcoins durch Geldzahlung nachzukommen.[551]

K. Rechtliche Grenzen der Vertragsdurchsetzung mittels Smart Contracts

Der denkbare Einsatz von Smart Contracts zur Fernsteuerung von Türschlössern, vernetzten Geräten oder Stromzählern wirft die Frage nach einem angemessenen Schuldnerschutz vor unzulässiger Selbsthilfe des Gläubigers auf. Denn Smart Contracts vergrößern die faktischen Möglichkeiten des Zahlungsgläubigers, die ihm obliegende Gegenleistung bei Ausbleiben des vereinbarten Entgelts ohne größeren Aufwand zeitnah zu unterbrechen oder einzustellen. Je nach Ausgestaltung eines Smart Contracts ermöglicht der Fernzugriff die Vornahme vollstreckungsähnlicher Handlungen, so dass es zu einem Abschneiden von Einwendungen und Leistungsverweigerungsrechten kommen könnte.[552] Auch wenn es sich hier nicht um blockchainspezifische Fragen im engeren Sinne handelt, soll auf die Problematik zumindest überblicksmäßig eingegangen werden:

I. Insbesondere: Verbotene Eigenmacht (§ 858 BGB)

Bei der oftmals beispielhaft angeführten Fernverriegelung des Schlosses einer Mietsache greift § 858 BGB zum Schutz des Mieters ein. Nicht auszuschließen ist zwar, dass die Hemmschwelle zur verbotenen Eigenmacht faktisch sinkt, wenn nicht mehr der analoge Aufbruch und Austausch des Schlosses nötig ist, sondern die Verriegelung aus der Ferne durch schlichten „Mausklick“ ausgelöst werden kann oder nach entsprechender Programmierung sogar gänzlich automatisiert durchgeführt wird. Nach § 858 BGB handelt aber widerrechtlich, wer dem Besitzer ohne dessen Willen den Besitz entzieht oder ihn im Besitz stört, sofern

---

[549] BGH, Urt. v. 5.10.2005 – VIII ZR 382/04 –, Rn. 25, juris.
[550] Vgl. a. *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379 (384 f.).
[551] Hierzu *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379 (383 ff.).
[552] *Paulus/Matzke*, Smart Contracts und Smart Meter - Versorgungssperre per Fernzugriff, NJW 2018, 1905; *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1436); *Djazayeri*, Rechtliche Herausforderungen durch Smart Contracts, jurisPR-BKR 12/2016, Anm. 1 (E. III.).

nicht das Gesetz die Entziehung oder die Störung (ausnahmsweise) gestattet. Der von *Paulus/Matzke* aufgeworfenen Frage, ob ein digitalisierter Besitzentzug für bestimmte Konstellationen wie etwa zeitlich kurz befristete Mietverhältnisse abweichend von § 858 BGB gerade gestattet werden sollte,[553] soll an dieser Stelle nicht weiter nachgegangen werden.

Allerdings lässt § 858 BGB Spielraum für Fälle, in denen nicht die Sachherrschaft als solche, sondern lediglich der vertragsgemäße Gebrauch der Sache beeinträchtigt wird. Der Bundesgerichtshof hat entschieden, dass die Einstellung oder Unterbrechung von Versorgungsleistungen durch den Vermieter nicht als Besitzstörung zu qualifizieren ist, wenn sie nicht den Zugriff auf die Sache oder die sich aus dem bloßen Besitz ergebene Nutzungsmöglichkeit erschwert, sondern die über den Besitz hinausgehende Verwendung einschränkt.[554] Es erscheint fraglich, ob nach dieser Rechtsprechung in der Unterbindung der vertragsgemäßen Verwendung eines gemieteten oder geleasten Fahrzeugs beispielsweise durch die Fernsperre des Motors ebenfalls noch keine verbotene Eigenmacht im Sinne des § 858 BGB liegt, wenn man das Fahrzeug zwar weiterhin öffnen, den Motor aber nicht starten kann.[555] Für den Schuldner kommt die Nutzungseinschränkung aber jedenfalls in tatsächlicher Hinsicht einer Wegnahme der Sache gleich. Er wird gezwungen, sich gegen eine aus seiner Sicht unberechtigte Nutzungssperre zur Wehr zu setzen, die Leistung des Vertragspartners einzuklagen und ggf. Schadenersatzansprüche geltend zu machen. Die Prozessführungslast verlagert sich mithin faktisch.[556] Zum jetzigen Zeitpunkt ist allerdings noch nicht absehbar, ob und inwieweit der Einsatz von Smart Contracts in der Praxis zu Ergebnissen führt, die einer gesetzgeberischen Korrektur bedürfen. Es bleibt abzuwarten, ob die zunehmenden technischen Möglichkeiten zur Vornahme „vollstreckungsähnlicher Handlungen“[557] zu einem Ungleichgewicht führen, dem durch eine Verschärfung der bestehenden Regelungen Rechnung getragen werden muss. Konkrete blockchainspezifische Probleme sind insoweit zwar nicht erkennbar. Ungeachtet dessen sollte die Gesamtproblematik der „digitalisierten Rechtsdurchsetzung“ im Blick behalten werden.

Entsprechendes gilt für Fälle, in denen die Nutzung digitaler Güter in Frage steht, denen die Sacheigenschaft nach § 90 BGB fehlt, und für die das Verbot der Eigenmacht in § 858 BGB schon deshalb nicht gilt. Überlegungen, ob und inwieweit der Sachbegriff des § 90 BGB erweitert oder das Immaterialgüterrecht

---

[553] *Paulus/Matzke*, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769 (777 f.).
[554] BGH, Urt. v. 6.5.2009 - XII ZR 137/07 - juris Rn. 20 ff.
[555] So *Paulus/Matzke*, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769 (775).
[556] Vgl. *Paulus/Matzke*, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769 (770); *Fries*, Smart Contracts: Brauchen schlaue Verträge noch Anwälte?, AnwBl 2018, 86 (88); *Blocher*, The next big thing: Blockchain - Bitcoin - Smart Contracts, AnwBl 2016, 612 (618);
[557] Vgl. *Paulus/Matzke*, Smart Contracts und Smart Meter, Versorgungssperre und Fernzugriff, NJW 2018, 1905 (1910).

dem Sachenrecht angeglichen werden sollte,[558] würden den Rahmen des Prüfauftrags der Arbeitsgruppe sprengen und soll daher vorliegend nicht weiter nachgegangen werden.

II. Beispiel: Fernsperre im Bereich der Energieversorgung

Auch im Bereich der Energieversorgung könnte es durch Smart Contracts oder sog. Smart Meter (intelligente Messsysteme), die eine elektronische Unterbrechung der Strom- oder Gaszufuhr ermöglichen, zu einer faktischen Verschiebung der Prozessführungslast kommen. Bedurfte es für die Sperre der Versorgung in der Vergangenheit noch analoger Handgriffe und oftmals des ggf. gerichtlich zu erstreitenden Zutritts zur Wohnung des Kunden, wird eine Sperre künftig vielfach auch aus der Ferne und vollautomatisiert ausgelöst werden können.[559]

Die Auslösung einer Energieversorgungssperre ist allerdings nur unter besonderen Voraussetzungen (z.B. nach einer vorherigen Androhung der Versorgungsunterbrechung) zulässig, welche in den jeweiligen Rechtsverordnungen (StromGVV, GasGVV, NAV, NDAV) zum Schutz des Nutzers als besondere Ausgestaltung der Leistungsverweigerungsrechte nach §§ 273, 320 BGB[560] aufgestellt werden.

Die Vornahme einer in § 19 Abs. 2 StromGVV/GasGVV vorgeschriebenen Verhältnismäßigkeitsprüfung hat das Energieversorgungsunternehmen selbstverständlich auch sicherzustellen, wenn es digitale Systeme einsetzt. Dass Härtefälle regelmäßig nur berücksichtigt werden könnten, wenn der Kunde das Energieversorgungsunternehmen über die in seiner Sphäre liegenden besonderen Umstände informiert, ist ebenfalls keine Besonderheit der „digitalen Welt".

Paulus/Matzke weisen darauf hin, dass ein Richtervorbehalt nur für den Fall besteht, dass der Wohnungszutritt zur Durchführung einer Sperre erforderlich ist und der Kunde diesen verweigert, und werfen insoweit die Frage auf, ob die Fälle der Versorgungssperre hinsichtlich des Richtervorbehalts nicht harmonisiert werden sollten und die Aktivierung einer Sperre durch Smart Meter generell der vorherigen gerichtlichen Kontrolle unterworfen werden sollte.[561] Auch bisher kann die Stromzufuhr aber auch ohne vorherige richterliche Kontrolle unterbrochen werden, wenn z.B. der Zutritt zu den im Keller eines Mietshauses befindlichen Stromzählern genügt und der Vermieter diesen gewährt. Denn der Richter-

---

[558] S. hierzu *Paulus/Matzke*, Digitalisierung und private Rechtsdurchsetzung, CR 2017, 769 (776 ff.).

[559] *Paulus/Matzke*, Smart Contracts und Smart Meter, Versorgungssperre und Fernzugriff, NJW 2018, 1905 (1906).

[560] Vgl. BGH, Urt. v. 3.7.1991 - VIII ZR 190/90 - juris Rn. 10 zu § 33 Abs. 2 Satz 1 AVBEltV a.F.

[561] *Paulus/Matzke*, Smart Contracts und Smart Meter, Versorgungssperre und Fernzugriff, NJW 2018, 1905 (1911).

vorbehalt dient dem besonderen Schutz der Wohnung als höchstpersönlichem privatem Bereich, nicht aber dem Schutz vor einer möglicherweise unzulässigen Unterbrechung der Storm- oder Gasversorgung. Solange keine Anhaltspunkte dafür bestehen, dass Versorgungsunterbrechungen nicht nur ausnahmsweise ohne Vorlage der rechtlichen Voraussetzungen vorgenommen werden, dürfte für einen generellen Richtervorbehalt daher keine Veranlassung bestehen, auch weil ein Gerichtsverfahren dann meist zu unnötigen zusätzlichen Kosten für den auch im Prozess häufig säumigen Verbraucher führen würde.[562]
Im Übrigen ist noch nicht abzusehen, ob sich aus dem praktischen Einsatz digitaler Systeme im Bereich der Energieversorgung ein Bedürfnis zur Anpassung bestehender Rechtsvorschriften ergibt. Derzeit sieht die Arbeitsgruppe hier keinen Handlungsbedarf.

L. Zwangsvollstreckung

Bereits in ihrem Bericht vom 15. Mai 2017 hat sich die Arbeitsgruppe mit Fragen der Zwangsvollstreckung im Zusammenhang mit Bitcoin befasst.[563] Die dort getroffenen Aussagen lassen sich auch auf andere Blockchain-Anwendungen erstrecken:

I. Zwangsweise Durchsetzung einer Änderung der Blockchain

Ist zur Rechtsdurchsetzung, etwa zur Rückabwicklung eines Vertrages, die Änderung der Blockchain erforderlich, bedarf es hierzu nach der technischen Grundkonstruktion der Blockchain-Technologie regelmäßig sowohl der Mitwirkung desjenigen, der über den auf den betroffenen Transaktionsgegenstand bezogenen private key verfügt, als auch der Validierung der reverse transaction durch die Mehrheit der Knoten.[564]
Ohne Kenntnis des zugehörigen private key ist ein (Rück-)Transfer überwiesener Token nicht möglich.[565] Mangels anderer Möglichkeit des Gläubigers, auf den private key des Schuldners zuzugreifen, kommt eine Vollstreckung dann nur nach § 888 ZPO in Betracht, um den Schuldner zur Vornahme der Rückabwicklung zu zwingen.[566] Ist der private key verloren gegangen, ist die Vollstreckung

---

[562] *Paulus/Matzke*, Smart Contracts und Smart Meter - Versorgungssperre per Fernzugriff, NJW 2018, 1905 (1911).
[563] Bericht der Arbeitsgruppe Digitaler Neustart vom 15. Mai 2017, S. 267 ff.
[564] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (463); *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (766).
[565] Vgl. *Kaulartz*, Die Blockchain-Technologie, CR 2016, 474 (479).
[566] Vgl. *Paulus/Matzke*, Smart Contracts und das BGB - Viel Lärm um nichts? -, ZfPW 2018, 431 (463 f.); *Kaulartz*, Die Blockchain-Technologie, CR 2016, 474 (479); *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht, MMR 2014, 643 (645); *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379 (386); *Saive*, Rückabwicklung von Blockchain-Transaktionen, DuD 2018, 764 (767).

unmöglich, und der Gläubiger ist auf die Verfolgung von Schadenersatzansprüchen beschränkt.
Über die Vornahme der Transaktionseinleitung hinaus hängt der tatsächliche Erfolg der Vollstreckung auch davon ab, ob und inwieweit die Aufnahme der Transaktion in die Blockchain im Wege der Zwangsvollstreckung erzwungen werden könnte. Da die Verifizierung anhand der Regeln des jeweiligen Blockchain-Protokolls automatisiert erfolgt, vor allem in der Prüfung liegt, ob die Transaktion mit dem Inhalt der Blockchain in Einklang steht, der Vornehmende also nach der bisherigen Transaktionshistorie zu ihr befugt ist, dürfte die reverse transaction meist nicht an der Zustimmung der Mehrheit der Knoten scheitern. Ob und wie im Einzelfall aber die Aufnahme einer Transaktion in einen Block und dessen Validierung im Wege der Zwangsvollstreckung durchgesetzt werden könnte, ist äußerst fraglich,[567] da die Zahl und Identität derjenigen, die Knoten oder miner betreiben, bei einer unbeschränkt zugänglichen Blockchain einem stetigen Wechsel unterworfen sein kann, grundsätzlich keine Verpflichtung zur (weiteren) Mitwirkung an einer Blockchain-Anwendung begründet wird, nicht ohne Weiteres vertragliche Beziehungen zwischen den Betreibern der Knoten bestehen und eine zentrale Instanz, die zur Durchsetzung einer Änderung herangezogen werden könnte, gerade fehlt.[568]

Es bleibt abzuwarten, ob und welche Probleme sich bei einzelnen Blockchain-Anwendungen in der Praxis insoweit tatsächlich ergeben. Aktuell ist ein Bedürfnis für ein gesetzgeberisches Einschreiten jedenfalls nicht festzustellen.

II. „Blockchain-Vermögen“ als Vollstreckungsgegenstand?

Die Vollstreckung wegen einer Geldforderung „in die Blockchain“ kommt - mangels Verkörperung der Token und mangels der Existenz eines Drittschuldners - nach geltendem Recht allenfalls über § 857 ZPO in Betracht. Anders als § 111b Abs. 1 StPO[569] erlaubt die Zivilprozessordnung nur die Beschlagnahme von Sachen und Rechten, nicht aber sonstiger Gegenstände. Ein Vorgehen nach § 857 ZPO wäre also nur möglich, wenn es sich bei den in der konkreten Blockchain eingetragenen Token um Vermögensrechte im Sinne dieser Vorschrift handelt. Von § 857 ZPO nicht erfasst werden rein tatsächliche Verhältnisse, aufgrund derer der Schuldner eine wirtschaftlich wertvolle Stellung einnimmt, oder bloße Befugnisse im Sinne von Handlungsmöglichkeiten, die nicht als verkehrsfähige, pfändbare Rechte ausgestaltet sind.[570] Solange der Eintrag in der

---

[567] Vgl. *Saive,* Haftungsprivilegierung von Blockchain-Dienstleistern gem. §§ 7 ff. TMG, CR 2018, 186 (190).
[568] Vgl. a. *Spindler/Bille,* Rechtsprobleme von Bitcoins als virtuelle Währung, WM 2014, 1357 (1360).
[569] Zur strafprozessualen Bewertung vgl. *Greier*, Möglichkeiten strafprozessualer Sicherung von Bitcoins gemäß §§ 111b ff. StPO, wistra 2016, 249 ff.
[570] MüKo-*Smid*, § 857 ZPO Rn. 9.

Blockchain bzw. der ihm zugeordnete private key lediglich die faktische Verfügungsmacht[571] über den Token vermittelt, jedoch kein weiteres Recht begründet, sind entsprechende Token daher auch nicht als Vermögensrechte nach § 857 ZPO pfändbar.[572] Nach überwiegender Auffassung ist eine Einzelvollstreckung „in Bitcoins" auf Grundlage der Zivilprozessordnung nach geltendem Recht nicht möglich.[573] Entsprechendes muss für vergleichbare andere Token gelten.
Selbst wenn man aber zu einer Pfändbarkeit - in analoger Anwendung des § 857 ZPO oder auf Grundlage einer entsprechenden Neuregelung - käme,[574] wären der Effektivität der Vollstreckung faktisch Grenzen gesetzt, da der Inhaber des private key ein Veräußerungsverbot jederzeit umgehen und die ihm zugeordneten Token aufgrund seiner faktischen Zugriffsmöglichkeit selbst weitertransferieren kann. Wegen der diesbezüglichen Einzelheiten wird auf den Bericht der Arbeitsgruppe vom 15. Mai 2017 Bezug genommen.[575] Die Ausführungen gelten gleichermaßen für andere Blockchain-Anwendungen als Bitcoin.
Da Bitcoin und auch andere Token eine erhebliche Kaufkraft beinhalten können, stellt sich dieses Ergebnis für einen Gläubiger, dem eine andere Vollstreckungsmasse im Einzelfall möglicherweise nicht zur Verfügung steht, als sehr unbefriedigend dar. Gleichwohl hält die Arbeitsgruppe daran fest, dass vorerst kein gesetzgeberischer Handlungsbedarf besteht. Denn es ist derzeit nicht feststellbar, dass sich in der Praxis tatsächlich Vollstreckungshindernisse ergeben, die durch eine gesetzgeberische Maßnahme adäquat behoben werden könnten. Diesbezüglich gilt es allerdings, die Problematik im Blick zu behalten und die weitere Entwicklung zu verfolgen.

M. Befassung auf EU-Ebene

Die EU-Kommission hat am 1. Februar 2018 mit Unterstützung des Europäischen Parlaments eine Beobachtungsstelle und ein Forum für die Blockchain-Technologie („EU Blockchain Observatory and Forum") auf den Weg gebracht, die „auf wichtige Entwicklungen der Blockchain-Technologie aufmerksam […] machen, europäische Akteure […] fördern und das europäische Zusammenwirken mit den verschiedenen an Blockchain-Aktivitäten beteiligten Interessenträ-

---

[571] Vgl. *Kaulartz/Matzke*, Die Tokenisierung des Rechts, NJW 2018, 3278 (3281); *Kuhlmann*, Bitcoins, CR 2014, 691 (696).
[572] Vgl. a. *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht, MMR 2014, 643 (644).
[573] Vgl. *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht, MMR 2014, 643 (644); *Ammann*, Bitcoin als Zahlungsmittel im Internet, CR 2018, 379 (385 f.); *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung, MMR 2014, 75 (78); *Kaulartz*, Die Blockchain-Technologie, CR 2016, 471 (479).
[574] *Greier*, Möglichkeiten strafprozessualer Sicherung von Bitcoins gemäß §§ 111b ff. StPO, wistra 2016, 249 (256), schlägt vor, auch „faktisch exklusive Rechte" der Pfändbarkeit zu unterwerfen.
[575] Bericht der Arbeitsgruppe Digitaler Neustart vom 15. Mai 2017, S. 268 f.

gern […] verstärken“ sollen.[576] Bisher hat die Stelle die folgenden drei Berichte[577] veröffentlicht:

„Blockchain for Government and Public Services“;
„Blockchain and the GDPR“;
„Blockchain innovation in Europe“.

Die EU finanziert außerdem verschiedene Forschungsprojekte zum Thema Blockchain, etwa „DECODE - blockchain for privacy“[578] oder „MyHealthMyData - blockchain for ehealth“.[579]

Am 10. April 2018 gründeten 21 Mitgliedstaaten der EU und Norwegen die „European Blockchain Partnership“, der sich zwischenzeitlich fünf weitere Mitgliedstaaten der EU angeschlossen haben. Ziel der Partnerschaft ist es, eine Europäische Infrastruktur für Blockchain-Dienste aufzubauen, die die Erbringung grenzüberschreitender digitaler öffentlicher Dienstleistungen mit höchsten Sicherheits- und Datenschutzstandards unterstützt.[580]

Das Europäische Parlament hat am 3. Oktober 2018 eine Entschließung[581] zu Distributed-Ledger-Technologien und Blockchains gefasst und u.a. das breite Spektrum DLT-basierter Anwendungen betont, die tiefgreifende Auswirkungen auf die Struktur der öffentlichen Verwaltung und die Rolle der Institutionen haben und potenziell alle Wirtschaftssektoren betreffen könnten. Das Parlament hat die Kommission u.a. aufgefordert, in Bezug auf Smart Contracts eine eingehende Prüfung der einschlägigen Möglichkeiten und der damit verbundenen rechtlichen Auswirkungen durchzuführen, u.a. den bestehenden Rechtsrahmen in den einzelnen Mitgliedstaaten in Bezug auf die Durchsetzbarkeit von Smart Contracts zu untersuchen und für den Fall, dass sich bei dieser Analyse mögliche Hemmnisse für die Nutzung von Smart Contracts im digitalen Binnenmarkt ergeben, angemessene Maßnahmen zu ergreifen.

---

[576] Vgl. Pressemitteilung der EU-Kommission vom 1.2.2018, http://europa.eu/rapid/press-release_IP-18-521_de.htm, letzter Abruf: 22.2.2019, sowie die näheren Informationen unter https://www.eublockchainforum.eu/, letzter Abruf: 22.2.2019.

[577] https://www.eublockchainforum.eu/reports, letzter Abruf: 24.2.2019.

[578] https://decodeproject.eu/what-decode, letzter Abruf: 24.2.2019.

[579] https://ec.europa.eu/digital-single-market/en/news/blockchain-enable-medical-data-be-stored-and-transmitted-safely-and-effectively, letzter Abruf: 24.2.2019.

[580] https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership, letzter Abruf: 24.2.2019.

[581] Vgl. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0373+0+DOC+PDF+V0//DE, letzter Abruf: 25.2.2019.

Teil 3:

„Leistungsschutzrechte an maschinengenerierten Daten“

A. Vorbemerkung

Ausgehend von dem Arbeitsauftrag der Frühjahrskonferenz Justizministerinnen und Justizminister am 21. und 22. Juni 2017 in Deidesheim hat sich die Arbeitsgruppe mit dem Thema „Leistungsschutzrecht an Daten“ auseinandergesetzt. Da maschinengenerierte Daten nicht dem Urheberrechtsschutz von Datensammlungen zugänglich sind und sich auch nicht als Geschäftsgeheimnisse schützen lassen, wird in der Literatur vorgeschlagen, die Zuordnung der Daten auf der Grundlage eines neuen Leistungsschutzrechts vorzunehmen und demjenigen zuzuordnen, der ihre Erhebung, Speicherung und Einteilung veranlasst hat (in der Regel der Hersteller).

Ausgehend von dieser Fragestellung soll nach einer Einführung in die Problematik und der Erläuterung der grundlegenden Begrifflichkeiten (unten B.) der Schutz maschinengenerierter Daten nach geltender Rechtslage dargestellt werden (unten C.). Hieran anschließend soll der Frage nachgegangen werden, ob die Zuordnung von maschinengenerierten Daten anhand eines neuen Leistungsschutzrechts geboten ist (D.).

B. Einführung in die Thematik und Begrifflichkeiten

Der jüngst entflammte Streit zwischen der Lufthansa, Airbus und Boeing um „das Gedächtnis von Flugzeugen“[582], also den Zugang zu und das Nutzungsrecht an in Flugzeugen erhobenen Daten, macht deutlich: Maschinendaten kommt eine immense wirtschaftliche Bedeutung zu. Wenn schon nach vorsichtigen Schätzungen der Wert von Mobilitätsdaten in einem privaten Pkw etwa 350 Euro im Jahr beträgt[583], wird die Bedeutung der Auseinandersetzung in der Luftfahrtbranche offenbar: Moderne Flugzeuge verfügen über 24.000 Messpunkte, die Triebwerksdrehzahlen, Treibstoffverbrauch, Kabinendruck etc. aufzeichnen und täglich etwa 1,5 Terabyte Daten - also ein Vielfaches eines privaten Pkw -

[582] Die Welt, veröffentlicht am 21. Juli 2018, abrufbar unter https://www.welt.de/wirtschaft/article179728238/Luftfahrt-Der-erbitterte-Streit-um-das-Gedaechtnis-von-Flugzeugen.html, letzter Abruf: 21.2.2019.
[583] BMVI, „Eigentumsordnung“ für Mobilitätsdaten?, S. 73.

erheben.[584] Sowohl für die Fluggesellschaft als auch für die Flugzeughersteller sind diese Daten gleichermaßen wertvoll, unter anderem weil deren Auswertung eine vorausschauende Wartung ermöglicht. Die Hoheit über die Daten gibt Zugriff auf die daraus gewonnenen Erkenntnisse. Der Streit zwischen Lufthansa, Airbus und Boeing steht damit paradigmatisch für die Frage, ob die europäische und die deutsche Rechtsordnung die für das Funktionieren der Datenwirtschaft notwendigen Regeln bereithalten, ob und gegebenenfalls wem diese Daten zugewiesen sind und wer Zugang zu ihnen hat.

I. Der Begriff des Leistungsschutzrechts

Der Begriff des Leistungsschutzrechts wird im deutschen Recht für unterschiedliche Sachverhalte mit zum Teil sehr unterschiedlichen Rechtsfolgen verwendet. Er taucht namentlich im Urheberrecht und im Wettbewerbsrecht auf. Leistungsschutzrechte können zunächst immaterialgüterrechtlicher Natur sein. Dann gewähren sie einen den Sonderschutzrechten[585] wesensgleichen Schutz geistiger Güter aufgrund geistig-schöpferischer oder wirtschaftlicher Leistungen und gegen unbefugten Zugriff Dritter. In diesem Sinne sind sie Ausschließlichkeitsrechte, die dem Inhaber ein positives Benutzungsrecht und ein Ausschlussrecht gegenüber unberechtigten Benutzern gewähren.

Beispiele für Leistungsschutzrechte im Sinne von Ausschließlichkeitsrechten sind die im Urheberrechtsgesetz geregelten „verwandten Schutzrechte“, die dem kulturellen Schaffen dienen, jedoch eine unternehmerische Leistung zum Gegenstand haben. Sie sind ihrer Natur nach unterschiedlich und rechtssystematisch nicht eindeutig zu klassifizieren.[586] So sind für die Verfasser wissenschaftlicher Ausgaben (§ 70 UrhG) und die Hersteller von Lichtbildern (§ 72 UrhG) die Vorschriften über das Urheberrecht sinngemäß anzuwenden, sodass diese Leistungsschutzrechte einen persönlichen und verwertungsrechtlichen Kern haben. Gleiches gilt für den Inhalt des Leistungsschutzrechts für ausübende Künstler (§ 73 UrhG). Im Urheberrechtsgesetz finden sich aber auch Anwendungsfälle reinen Investitionsschutzes, namentlich das *sui-generis*-Leistungsschutzrecht des Datenbankherstellers (§ 87a UrhG), dem in der Untersuchung ein breiter Raum eingeräumt werden wird. Sie sind auf den Schutz unternehmerischer, nichtinnovativer Leistungen gerichtet, weil diese mit einem wirtschaftlichen Aufwand verbunden sind.[587]

---

[584] Angaben aus Behördenspiegel, Oktober 2018, S. 27.

[585] Als Sonderschutzrechte werden die in den zum gewerblichen Rechtsschutz zählenden Gesetze gewährte Rechte bezeichnet.

[586] Schricker/Loewenheim/Loewenheim/*Leistner*, Urheberrecht, Einleitung Rn. 39.

[587] Möhring/Nicolini/*Ahlberg*, Urheberrecht, Einführung Rn. 70 ff.; Dreier/Schulze/*Dreier*, UrhG, Vorbemerkung zu § 87a Rn. 1.

Der Begriff des Leistungsschutzrechts wird zum anderen für die rechtliche Missbilligung und Ahndung von Handlungen verwendet, ohne dass damit eine konkrete Rechtezuweisung einherginge. Dies gilt für den „wettbewerbsrechtlichen Leistungsschutz", der das Leistungsergebnis eines Mitbewerbers schützen soll und auch als „lauterkeitsrechtlicher Nachahmungsschutz" oder „ergänzender wettbewerbsrechtlicher Leistungsschutz" bezeichnet wird.[588]

Allen Begrifflichkeiten ist immanent, dass jeweils das Ergebnis einer erfinderischen, schöpferischen oder unternehmerischen Tätigkeit geschützt wird. Dieses Begriffsverständnis soll auch im Folgenden zugrunde gelegt werden. Leistungsschutz soll in seiner Bandbreite von Innovationsschutz bis hin zum reinen Investitionsschutz untersucht werden. Wenn daher von „Leistungsschutzrecht an Daten" die Rede ist, geht es um den Schutz der berechtigten Interessen an einem wirksamen Investitions- und Innovationsschutz im Spannungsverhältnis zur Gemeinfreiheit. Dieser Untersuchungsgegenstand klammert die Betrachtung des Integritätsschutzes (§§ 823 Abs. 2 BGB, 303a StGB), des Vertraulichkeitsschutzes (§§ 17 UWG, 202a StGB) und des persönlichkeitsrechtlichen Datenschutzes (BDSG, DSGVO) aus.

II. Datenbegriff, maschinengenerierte Daten

Unabhängig von den in der Literatur geführten Kontroversen um Einzelheiten des Begriffs der Daten[589] werden in der folgenden Untersuchung Daten definiert als „Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen, vorrangig zum Zweck der Bearbeitung oder als deren Ergebnis".[590] Untersuchungsgegenstand sind digitale Daten, die nach einem bestimmten Code dargestellt sind und

---

[588] Köhler/Bornkamm/Feddersen/*Köhler*, Gesetz gegen den unlauteren Wettbewerb, § 4 Rn. 3.4.; Fezer/Büscher/Obergfell/*Götting/Hetmank*, Lauterkeitsrecht: UWG, § 4 Nr. 3 Rn. 1.

[589] Das deutsche Recht verwendet an verschiedenen Stellen den Datenbegriff, weist aber keine diesbezügliche Definition auf. Verwendet wird der Begriff etwa im Datenschutz oder im Strafrecht unter „Ausspähen von Daten" (§ 202a StGB); „Daten" in diesem Sinn sind „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."

[590] *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 29 unter Bezugnahme auf DIN 4430, Teil 2 Nr. 2.1.13, zitiert nach Hoeren/*Hoeren/Völkel*, Big Data und Recht, S. 11. Nach ISO sind Daten „a reinterpretable representation of information … in a formalized manner suitable for communication, interpretation, or processing" (ISO/IEC 2382-1 (1993)), vgl. hierzu *Wiebe,* Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken*,* GRUR 2017, 338.

die deshalb von Computern und anderen Geräten zur digitalen Datenverarbeitung gelesen oder verarbeitet werden können.[591]

Der Begriff des „maschinengenerierten Datums", der Eingang in zahlreiche Arbeitspapiere der EU-Kommission gefunden hat[592], ist mittlerweile weit verbreitet und lässt sich definieren als von einer Datenverarbeitungsanlage automatisch erzeugtes und verarbeitetes Datum.[593] Er beschreibt Sachverhalte, in denen Maschinen Daten ohne unmittelbare Mitwirkung eines Menschen erzeugen. Gängige Beispiele sind - neben dem bereits genannten Beispiel der Datenerzeugung im Flugzeug - vernetzte Thermostate, die anhand detaillierter Verbrauchsdaten der Raumnutzer die Temperatur regulieren - mit dem Effekt der Heizkostenersparnis.[594] In der Vision einer Fabrik der Industrie 4.0 koordinieren intelligente Maschinen durch Kommunikation miteinander selbstständig Fertigungsprozesse und kümmern sich eigenständig um Logistik und Materialfluss.[595] In der Landwirtschaft kann eine Analyse der aktuellen Wetter- und Bodendaten dazu beitragen, den Pflanzenanbau zu optimieren.[596] Landmaschinen, die laufend die Bodengüte und die ausgebrachte Menge an Bodendünger ermitteln und bei der Ernte kleinteilig Erträge messen, sind in der Lage, die effektivste Route auf der zu bewirtschaftenden Fläche und die optimale Düngermenge zu ermitteln.[597]

In der Regel weisen diese Daten einen Personenbezug auf, sei es, indem sie menschliche Handlungen aufzeichnen (GPS-Systeme die Ortsveränderungen; smarte Küchengeräte das Verbrauchsverhalten etc.), sei es, indem sie Informationen über die Maschine selbst geben und damit Rückschlüsse auf menschliches Verhalten zulassen. So kann die Analyse von maschinengenerierten Daten beispielsweise einen Bedienungsfehler einer Maschine zu einem bestimmten Zeitpunkt offenlegen, der sich einem bestimmten Arbeitnehmer zuordnen lässt.[598] In

---

[591] Zum Begriff des digitalen Datums: *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 29 m.w.N.

[592] Vgl. etwa Mitteilungen der EU-Kommission „Aufbau einer europäischen Datenwirtschaft", COM(2017) 9 final und „Aufbau eines gemeinsamen europäischen Datenraums", COM(2018) 232 fin.

[593] Sassenberg/Faber/*Sattler*, Rechtshandbuch Industrie 4.0 und Internet of Things, S. 29; *Becker* in: FS Fetzer, S. 815 (816 f.).

[594] Beispiel nach *Schwartmann/Hentsch,* Eigentum an Daten - Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221.

[595] BMWi, Digitale Transformation in der Industrie, abrufbar unter https://www.bmwi.de/Redaktion/DE/Dossier/industrie-40.html (letzter Abruf: 21.2.2019)

[596] Mitteilung der EU-Kommission „Aufbau eines gemeinsamen europäischen Datenraums", COM(2018) 232 final.

[597] Beispiel nach *Zech,* Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137; *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 75.

[598] Beispiel nach Sassenberg/Faber/*Sattler*, Rechtshandbuch Industrie 4.0 und Internet of Things, S. 30.

diesen Fällen können die gewonnenen Daten zusätzlich dem Datenschutzrecht und den Vorschriften anderer Rechtsgebiete unterliegen. Maschinengenerierte Daten stellen also nicht das Gegenstück zu personenbezogenen Daten dar, weshalb die für personenbezogenen Daten geltenden rechtlichen Beschränkungen bei weitergehenden Überlegungen hinsichtlich künftiger Regelungen für die Datenwirtschaft einbezogen werden müssen.[599]

Um den Untersuchungsgegenstand sinnvoll zu begrenzen, müssen die durch sogenannte „künstliche Intelligenz" generierten Daten ausgeklammert bleiben. Für diese stellen sich immaterialgüterrechtliche Sonderprobleme, etwa auf dem Gebiet des Patentrechts.[600] Hinzu treten weitere Probleme, deren Klärung für die Beantwortung des Arbeitsauftrags nichts Erhellendes beitrüge: Es besteht schon keine Einigkeit, ob „künstliche Intelligenz" überhaupt Daten generiert. Dies wird zum Teil mit dem Argument bestritten, dass die generierten Daten für den Menschen unverständlich seien und aus diesem Grund keinen Informationsgehalt enthielten. Ebenso wenig wurde eine trennscharfe Definition für das Phänomen der künstlichen Intelligenz gefunden[601] (wie auch für den Begriff der Intelligenz selbst[602]). Es erscheint daher gerechtfertigt, diese spezifisch bei „künstlicher Intelligenz" auftretenden Probleme, die sich im Übrigen bei maschinengenerierten Daten nicht stellen, einer gesonderten Untersuchung vorzubehalten.

---

[599] Morik/Krämer/*Scheuch*, Daten, S. 58 f.

[600] Siehe hierzu instruktiv *Hetmank/Lauber-Rönsberg,* Künstliche Intelligenz - Herausforderungen für das Immaterialgüterrecht, GRUR 2018, 574 ff.

[601] Testimony of Dr. Amir Khosrowshahi, Artificial Intelligence Products Group, before the U.S. House of Representatives, Committee on Oversight and Government Reform, Subcommittee on Information Technology, Hearing "Game Changers: Artificial Intelligence Part I", February 14, 2018; *Wichert*, Künstliche Intelligenz, https://www.spektrum.de/lexikon/neurowissenschaft/kuenstliche-intelligenz/6810 (letzter Abruf: 21.2.2019). Teilweise wird im Rahmen einer Definition darauf abgestellt, ob ein System Aufgaben ausführen kann, die typischerweise von Menschen ausgeführt werden. Andere stellen auf den im Jahr 1950 von A.M. Turing publizierten Aufsatz "Computing Machinery and Intelligence" ab, in welchem der Autor ein intelligentes Programm als ein solches definierte, das auf die Fragen eines intelligenten Wesens reagieren könne.

[602] *Wichert*, Künstliche Intelligenz, https://www.spektrum.de/lexikon/neurowissenschaft/kuenstliche-intelligenz/6810 (letzter Abruf: 21.2.2019).

C. Schutz maschinengenerierter Daten nach geltendem Recht

In dem folgenden ersten Teil wird der Leistungsschutz an maschinengenerierten Daten nach geltendem Recht dargestellt. Dabei wird zunächst das Bürgerliche Recht in den Blick genommen. In der Diskussion um die Einführung eines Leistungsschutzrechts wird zudem immer wieder auf das Urheberrecht verwiesen, dem zum Teil sogar eine Vorbildfunktion zugeschrieben wird.[603] Der Schaffung von Immaterialgüterrechten, insbesondere der Leistungsschutzrechte im Urheberrechtsgesetz, habe der Gedanke zugrunde gelegen, dass die Investition (technische bzw. geistige Leistung) belohnt werden müsse. Ähnlich, so heißt es, verhalte es sich mit Daten, die sich zu einem immateriellen Gut entwickelt hätten. Daher läge es nahe, dass demjenigen, der in die Erzeugung dieses Gutes investiert habe, dessen Verwertung nach der Rechtsordnung gebühre. Dieser Frage soll nachgegangen werden, wobei im Mittelpunkt das *sui-generis*-Leistungsschutzrecht des Datenbankherstellers stehen wird.

Abschließend wird der lauterkeitsrechtliche Leistungsschutz in den Blick genommen werden. Dessen Untersuchung ist nicht zuletzt deshalb geboten, weil ihm als enges Bindeglied zu den Immaterialgüterrechten vielfach eine „Schrittmacherfunktion“ für die Entwicklung neuer Leistungsschutzrechte zugeschrieben wird.

I. Leistungsschutz im Bürgerlichen Gesetzbuch

Ein ausdrückliches Leistungsschutzrecht an Daten existiert im Bürgerlichen Recht nicht. Gleichwohl haben die Gerichte und das Schrifttum in der Vergangenheit die offen formulierten Tatbestände der gesetzlichen Schuldverhältnisse in einer Weise angewendet, dass mit der Gewährung von Ansprüchen gegen die unerlaubte Nutzung „neuer“ Güter, die durch wirtschaftliche und technologische Entwicklungen hervorgebracht worden sind, Befugnisse an diesen Gütern zugunsten einer bestimmten Person herausgebildet werden.[604] So haben das Reichsgericht und der Bundesgerichtshof viele inzwischen normierte Immaterialgüterrechte auf allgemein bürgerlich-rechtlicher aber auch lauterkeitsrechtlicher Grundlage vorweggenommen, indem bestimmten Personen Ansprüche etwa gegen die Vervielfältigung und sonstige Übernahme von Tonträgern, Computerprogrammen und Datenbanken gewährt wurden.[605] Dies führt zu der Frage, ob sich dem Bürgerlichen Recht ein geltendes (nicht im Wege der Rechtsfortbil-

---

[603] *Schwartmann/Hentsch*, Eigentum an Daten - Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221, sprechen von „Pate für ein Datenverwertungsrecht“.
[604] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 474, S. 136 ff. und S. 237 ff.
[605] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 4 f.; *Schröer,* Der unmittelbare Leistungsschutz, S. 11 ff.

dung zu entwickelndes) Rechtsprinzip entnehmen lässt, das gebietet, ein Leistungsschutzrecht an dem „neuen“ Gut der maschinengenerierten Daten anzuerkennen. Vor allem das Deliktsrecht ist der Bereich, in dem sich die Anerkennung neuer Güter als Erstes zeigt.

1. Leistungsschutz nach Deliktsrecht

Maschinengenerierte Daten genießen nach geltendem Recht in vielerlei Hinsicht deliktsrechtlichen Schutz. Der unbefugte Zugriff auf Daten kann eine vorsätzliche sittenwidrige Schädigung des Berechtigten darstellen und damit eine Haftung nach § 826 BGB auslösen. In den §§ 202a ff., 303a StGB finden sich Straftatbestände, die Daten unabhängig von einem Speichermedium und ihrem Inhalt schützen. Geschützt sind auch solche Daten, die keine persönlichkeitsrelevanten Informationen enthalten, jedoch von wirtschaftlichem Wert sind. Diese Strafgesetze sind ebenso wie andere Vorschriften zum Schutz des Dateninhalts (z.B. Vorschriften des BDSG und der DSGVO; §§ 17 ff. UWG zum Schutz von Geschäftsgeheimnissen) Schutzgesetze im Sinne von § 823 Abs. 2 BGB.[606] Dieser deliktsrechtliche Schutz greift indes nur bei vorsätzlichen Handlungen und gewährt allein Integritäts- und Vertraulichkeitsschutz, während das allgemeine Persönlichkeitsrecht zudem als Rechtsgut im Sinne von § 823 Abs. 1 BGB geschützt ist. Eine konkrete Rechtezuweisung ist damit nicht verbunden, sondern wird von den Normen vorausgesetzt.

a. Leistungsschutzrecht nach § 823 Abs. 1 BGB

Damit stellt sich die Frage, ob sich dem Tatbestand des § 823 Abs. 1 BGB, insbesondere dem Tatbestandsmerkmal des „sonstigen Rechts“, die Zuweisung eines Rechts an Daten entnehmen lässt. Das Deliktsrecht schützt Ausschließlichkeitsrechte durch § 823 Abs. 1 BGB. Die in dieser Norm erwähnten „sonstigen Rechte“ sind neben Leben, Körper, Gesundheit, Freiheit und Eigentum ebenfalls als Ausschließlichkeitsrechte zu verstehen.[607]

Die rein faktische Möglichkeit des Datenerzeugers, Maschineninhabers oder Maschinennutzers, andere von der Nutzung der Daten auszuschließen, begründet für sich genommen, kein sonstiges absolutes Recht im Sinne von § 823 Abs. 1 BGB. Daten sind mangels Sachqualität auch nicht „Eigentum“ im Sinne von § 823 Abs. 1 BGB, denn es handelt sich bei gespeicherten Daten lediglich um ein bestimmtes Muster magnetischer Spannung.[608] Es fehlt an der von § 90 BGB vorausgesetzten Körperlichkeit, darüber hinaus aber auch an der für Sacheigentum charakteristischen Rivalitätsbedingung. Informationen können von mehre-

---

[606] OLG Dresden, Beschl. v. 5.9.2012 – 4 W 961/12 –, NJW-RR 2013, 27 (28).
[607] Jauernig/*Teichmann*, BGB, § 823 Rn. 12; MüKo/*Wagner,* BGB, § 823 Rn. 267 f..
[608] *Zech,* Information als Schutzgegenstand, S. 326 ff.

ren Personen gleichzeitig genutzt und mit geringem Aufwand ohne Verlust vervielfältigt werden.[609] Sachen im Sinne von § 90 BGB sind hingegen die Datenträger, also Disketten, Festplatten und Bänder, auf denen Informationen gespeichert sind, indem deren Oberfläche in bestimmter Weise magnetisiert ist. Nur wenn der Datenträger beschädigt, zerstört oder - etwa durch Veränderung oder Löschung der Dateninhalte - in seiner Beschaffenheit verändert wird, liegt ein Eingriff in das Sacheigentum (am Datenträger) vor.

An diesem Befund ändert auch die technische Entwicklung nichts. Zwar verliert der durch das Eigentum am Datenträger vermittelte Rechtsschutz an elektronisch gespeicherten Informationen durch den Fortschritt der Informationstechnologie an Bedeutung. Der durch den Sachbegriff vermittelte Schutz versagt, wenn Daten körperlos durch das Netz übermittelt und nicht mehr auf dem Computer des Nutzers, sondern in der sog. Datenwolke (cloud) gespeichert werden. Hieraus folgern zahlreiche Stimmen in der Literatur ein praktisches Bedürfnis, das Recht an den eigenen Daten als „sonstiges Recht“ im Sinne von § 823 Abs. 1 BGB anzuerkennen.[610] Diese Auffassung hat sich jedoch bislang nicht durchgesetzt und auch die Arbeitsgruppe hat sich in ihrem Bericht vom 15. Mai 2017 mit eingehender Begründung gegen die Anerkennung von maschinengenerierten Daten als sonstiges Recht im Sinne von § 823 Abs. 1 BGB ausgesprochen.[611] Der ausschließliche Zugriff auf digitale Daten beruht auf faktischen, technischen Gründen und schuldrechtlichen Ansprüchen. Die Einordnung als deliktsrechtlich geschütztes Recht erfordert hingegen eine absolute, gegenüber jedermann wirkende, von der Rechtsordnung eingeräumte Rechtsposition. Ein solches Recht lasse sich inhaltlich kaum fixieren und einer Person zuordnen. Probleme ergäben sich insbesondere bei kollidierenden Rechtspositionen am Dateninhalt.[612]

Schließlich eröffnet das Tatbestandsmerkmal „sonstiges Recht“ auch nicht die Möglichkeit, Leistungsschutzrechte an für schutzwürdig befundenen Rechtsgütern aus § 823 BGB selbst heraus herzuleiten. Denn das Deliktsrecht des Bürgerlichen Gesetzbuchs enthält keine allgemeine Generalklausel nach dem Prinzip des *neminem laedere*, wonach für jeden Schaden gehaftet wird, es sei denn, der Schuldner habe ein besonderes Recht ausgeübt oder in einer mit den guten Sitten übereinstimmenden Ausübung der natürlichen Freiheit gehandelt.[613] Vielmehr tritt eine Ersatzpflicht für Schäden nur ein, wenn ein Tatbestand der abschlie-

---

[609] MüKo/*Wagner,* BGB, § 823 Rn. 219.
[610] *Zech*, Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (143) m.w.N.
[611] *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 48 ff. und S. 82 f.
[612] Zur Begründung im Einzelnen, *Arbeitsgruppe „Digitaler Neustart“*, Bericht vom 15. Mai 2017, S. 48 ff.
[613] BeckOK/*Förster*, BGB, Stand: 1.11.2018, § 823 Rn. 2.

ßend aufgezählten gesetzlichen Haftungsregelungen erfüllt ist; der Zweck des Deliktsrechts ist also von vornherein auf bestimmte Verletzungshandlungen beschränkt (Enumerationsprinzip).[614] Aus diesem Grund entspricht es herrschender Auffassung, dass eine deliktische Haftung nur bei der Verletzung absoluter, aus dem allgemeinen Vermögen herausgehobener Rechtsgüter in Betracht kommt.[615] Vor diesem Hintergrund kann ein solches Rechtsgut nicht aus § 823 Abs. 1 BGB selbst heraus entwickelt werden, sondern wird vielmehr von dieser Haftungsnorm vorausgesetzt.

b. Leistungsschutzrecht nach § 826 BGB

Der Tatbestand von § 826 BGB gewährt einen Ersatzanspruch für die Zufügung von Schäden auch ohne Verletzung eines der in § 823 BGB genannten Rechtsgüter und kann grundsätzlich, etwa bei Ausnutzung fremder Leistungen, Grundlage für Leistungsschutz sein. Die Vorschrift war bis zur Einführung des Gesetzes gegen den unlauteren Wettbewerb (UWG) und der Kartellverordnung als Vorläufer des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) das zentrale Instrument zur Steuerung des Wettbewerbsverhaltens der Marktteilnehmer. Wenngleich ihre Bedeutung zurückgegangen ist[616], sind Fälle denkbar, in denen etwa gegen den Missbrauch wirtschaftlicher Macht aufgrund von „Datenherrschaft“ einerseits oder zur Abwehr sittenwidriger Schädigungen durch unberechtigte Datennutzung andererseits auf § 826 BGB zurückgegriffen werden kann. [617] Erforderlich ist insoweit neben der vorsätzlichen Zufügung eines Schadens nach der sog. Verwerflichkeitsformel des Bundesgerichtshofs, dass besondere Umstände hinzutreten, die das schädigende Verhalten wegen seines Zwecks oder wegen des angewandten Mittels oder mit Rücksicht auf die dabei gezeigte Gesinnung nach den Maßstäben der allgemeinen Geschäftsmoral und des als „anständig“ Geltenden verwerflich machen.[618] Soweit sich danach etwa der unbefugte Zugriff auf Daten im Einzelfall als verwerflich darstellt, stünden dem Geschädigten Abwehrrechte nach § 826 BGB zu. Dabei ist es eine weitere Frage des Einzelfalls, wer als Geschädigter und damit als Gläubiger eines Anspruches nach § 826 BGB anzusehen ist. Auch wenn hierfür die Verletzung eines Schutzrechts im Sinne von § 823 Abs. 1 BGB nicht erforderlich ist, weil § 826 BGB auch reine Vermögensschäden erfasst[619], muss jedenfalls eine schützenwerte Position des Anspruchstellers beeinträchtigt sein, die dessen Vermögen zuzurechnen ist.

---

[614] MüKo/*Wagner,* BGB, Vorbemerkung zu § 823 Rn. 25.
[615] Palandt/*Sprau*, BGB, § 823 Rn. 11; MüKo/*Wagner,* BGB, § 823 Rn. 370.
[616] Zum verbleibenden Anwendungsbereich von § 826 BGB allgemein MüKo/*Wagner,* BGB, § 826 Rn. 198.
[617] Bericht der Arbeitsgruppe „Digitaler Neustart“, S. 55.
[618] BGH, Urt. v. 3.12.2013 - XI ZR 295/12, NJW 2014, 1098 (1099) m.w.N.
[619] MüKo/*Wagner,* BGB, § 826 Rn. 41.

Durch die Rechtsprechung wurde in der Vergangenheit die Nutzung „neuer" Güter in zahlreichen Fällen unter Rekurs auf das Verbot sittenwidriger Schädigungen bestimmten Personen auch exklusiv im Sinne eines Ausschließlichkeitsrechts vorbehalten. So wurden damit auf der Grundlage von § 826 BGB Schutzrechte an neuen Gütern entnommen, die nicht selten Pate für spätere gesetzliche Normierungen im Urheberrechtsgesetz standen.[620] Den insoweit ergangenen Gerichtsentscheidungen ist gemein, dass es aufgrund der technologischen Entwicklung erstmals möglich geworden war, bestimmte Produkte zu geringen Kosten zu reproduzieren. Die ursprünglichen Hersteller der jetzt reproduzierbaren Information gingen gegen diese technische Übernahme vor, weil sie ihre bis dato automatische Exklusivität verloren hatten.[621] Da zuvor kein Schutzbedürfnis bestanden hatte, war keines der Güter spezialgesetzlich zugeordnet, so dass sich die Betroffenen auf § 826 BGB, allgemeine Rechtsgrundlagen und Prinzipien beriefen. Ähnliche Szenarien sind auch in Bezug auf maschinengenerierte Daten denkbar.

Die Gerichte beriefen sich seinerzeit überwiegend auf naturrechtlich geprägte Rechtfertigungen, indem die Übernahme eines fertigen Arbeitsprodukts durch technische Mittel als „Schmarotzen an fremder Leistung" sanktioniert wurde, weil dieses Verhalten dem ursprünglichen Investor die Möglichkeit nehme, seine Herstellungskosten angemessen zu amortisieren und damit am Markt konkurrenzfähig zu sein. Argumentiert wurde ferner mit Erklärungen zur Schutzwürdigkeit des Gutes, der Behauptung einer allgemeinen Überzeugung zugunsten des Schutzes oder wettbewerbspolitischen Motiven.[622] Niemand dürfe um die „Früchte der eigenen Arbeit" gebracht werden, künstlerische und andere Leistungen seien Ausdruck der Persönlichkeit, die dem „Schöpfer" so gehören, wie dieser sich selbst gehört.[623] Wenn für das Hervorbringen eines kommerziell verwertbaren Arbeitsergebnisses ein erheblicher Aufwand an Finanzkraft notwendig war, und auf diese Weise eine Position geschaffen wurde, die üblicherweise erhebliche Ertragschancen bietet, sei das ein ausreichender Grund für einen schützenswerten Besitzstand. Denn der Kopist erspare sich die versunkenen

---

[620] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 152 ff.; *Schröer,* Der unmittelbare Leistungsschutz, S. 11 ff.

[621] Eine detaillierte Übersicht über die Rechtsprechungsentwicklung liefert *Schröer,* Der unmittelbare Leistungsschutz, S. 11 ff.

[622] RG, Urt. v. 31.1.1928 – II 77/27 –, RGZ 120, 94 (97 ff.) - Huthaken; BGH, Urt. v. 6.11.1963 – Ib ZR 37/62 –, BGHZ 41, 55 (57 ff.) - Klemmbausteine I; BGH, Urt. v. 19.1.1973 – I ZR 39/71 –, BGHZ 60, 168 (169 ff.) - Modeneuheit; BGH, Urt. v. 28.1.1988 – I ZR 34/86 –, GRUR 1988, 385 (387); BGH, Urt. v. 7.2.2002 – I ZR 289/99 –, GRUR 2002, 820 (822).

[623] RG, Urt. v. 31.1.1928 – II 77/27 –, RGZ 120, 94 (97 ff.) - Huthaken.

Herstellungskosten, so dass der Anreiz zur Schaffung von Waren und Dienstleistungen verloren gehe.[624]

Ohne auf die schwierige und umstrittene Frage einzugehen, ob der Rechtsprechung die Befugnis zusteht, Leistungsschutzrechte aus den bestehenden Regelungen heraus rechtsschöpferisch zu entwickeln[625], lässt sich *de lege lata* dem Tatbestand des § 826 BGB ein bei sittenwidriger Schädigung im Einzelfall bestehender Rechtsschutz, jedenfalls aber kein Leistungsschutzrecht im Sinne eines Ausschließlichkeitsrechts an maschinengenerierten Daten entnehmen. Denn der Tatbestand erfasst nur sittenwidrige und damit trotz der Offenheit des Tatbestands nur qualifiziert rechtswidrige Handlungen und setzt damit eine bereits bestehende Güterzuordnung voraus, ohne sie selbst zu schaffen.[626] Die angedeuteten Argumente der Rechtsprechung für die Gewährung von Leistungsschutz liefern aber wertvolle Entscheidungshilfen für die Beurteilung eines gesetzgeberischen Handlungsbedarfs, weshalb auf sie an anderer Stelle erneut zurückgegriffen werden soll.[627]

2. Leistungsschutz nach Bereicherungsrecht

Auch dem Bereicherungsrecht ist kein mit einer Güterzuweisung verbundener Leistungsschutzgedanke zu entnehmen. Der Bereicherungsschuldner erlangt im Sinne von § 812 Abs. 1 S. 1 2. Alt. BGB etwas auf Kosten des Bereicherungsgläubigers, wenn er in eine Rechtsposition eingegriffen hat, die nach der Rechtsordnung dem Gläubiger zu dessen ausschließlicher Verfügung und Verwertung zugewiesen ist.[628] Durch diese Vorschrift wird dem Bereicherungsgläu-

---

[624] Eingehend *Peukert,* Güterzuordnung als Rechtsprinzip, S. 152 ff.

[625] Die Rechtsprechung nimmt für sich die Befugnisse „angesichts des beschleunigten Wandels der gesellschaftlichen Verhältnisse und der begrenzten Reaktionsmöglichkeiten des Gesetzgebers sowie der offenen Formulierungen zahlreicher Normen“ in Anspruch, weil „in einer solchen Situation (…) das Gesetz seine Fähigkeit verloren haben (kann), für alle Fälle, auf die seine Regelung abzielt, eine gerechte Lösung bereit zu halten.“, BVerfG NJW 2006, 3409; BVerfGE 82, 6 (12); BVerfGE 84, 212 (226 f.) Zustimmend gerade für die hier behandelten Konstellationen des Datenrechts (für § 3 UWG) *Becker,* Lauterkeitsrechtlicher Leistungsschutz für Daten, GRUR 2017, 346 (347): Der unmittelbare Leistungsschutz nach UWG ist in der Lage, die Ausnutzung fremder Leistungen mit Rücksicht auf die Besonderheiten des Einzelfalls zu verhindern. Dies ermöglicht es, zunächst Erfahrungen auf dem neuen Gebiet zu sammeln und Geschäftsmodelle entstehen zu lassen, die gegebenenfalls mit der Zeit gesetzlich geregelt werden könnten. In einer solchen Findungsphase des Rechts spielt Rechtssicherheit eine geringere Rolle. Ein unmittelbarer Leistungsschutz nach UWG dürfte aus diesem Grund auch der Gemeinfreiheit zuträglicher sein als eine verfrühte gesetzliche Regelung.

[626] Näher hierzu *Peukert,* Güterzuordnung als Rechtsprinzip, S. 284.

[627] Siehe unten unter D. II.

[628] BGH, Urt. v. 13.7.2012 – V ZR 206/11 –, NJW 2012, 3572 Rn. 9; BGH, Urt. v. 9.3.1989 – I ZR 189/86 –, BGHZ 107, 117 (120 f.).

biger Schutz jedoch nur gewährt, soweit ihm eine Rechtsposition durch andere Rechtsvorschriften zugewiesen ist. Die Rechtsposition selbst kann dem Bereicherungsrecht nicht entnommen werden. Dementsprechend haben der Bundesgerichtshof[629] und mit ihm die ganz herrschende Lehre[630] den Gedanken eines selbständigen Leistungsschutzes aus Bereicherungsrecht verworfen.

3. Leistungsschutzrecht nach den Vorschriften über die Geschäftsführung ohne Auftrag

Leistungsschutzrechte an Daten lassen sich auch nicht aus den Vorschriften über die Geschäftsführung ohne Auftrag (§§ 677 ff. BGB) herleiten. Dies wäre nur dann der Fall, wenn die Vorschriften aus sich heraus Rechte an maschinengenerierten Daten zuwiesen oder Investitionsschutz gewährten. Beides ist nicht der Fall: Die Regelungen zur Geschäftsführung ohne Auftrag nehmen selbst keine Zuordnung bestimmter Geschäfte als „fremd" im Sinne von § 677 BGB oder bestimmter Geschäftsbehandlungen als unberechtigt im Sinne von § 687 Abs. 2 S. 1 BGB vor. Sie stellen vielmehr nur Blankettnormen zur Verwirklichung vorausgesetzter Rechte bzw. gesetzlicher Wertungen dar. Ob eine Leistung oder eine Erwerbsmöglichkeit dem Geschäftsherrn rechtlich zugewiesen ist, lässt sich anhand der Vorschriften der §§ 677 ff. BGB nicht klären.[631]

4. Leistungsschutzrecht nach §§ 950, 951 BGB analog

In der rechtswissenschaftlichen Literatur ist vereinzelt der Vorschlag unterbreitet worden, in Anlehnung an §§ 950, 951 BGB Leistungsschutz für den mit der Datenerhebung erforderlichen Aufwand zu gewähren.[632] Diese Konzeption weist Ausschließlichkeitsrechte an den Daten nicht dem Datenerzeuger, sondern dem Datenspeicherer zu, und gewährt dem Datenerzeuger lediglich Investitionsschutz durch Entschädigung.

Nach § 951 Abs. 1 S. 1 BGB kann, wer infolge der Vorschriften der §§ 946 bis 950 BGB (Verbindung, Vermischung, Verarbeitung) einen Rechtsverlust erleidet, von demjenigen, zu dessen Gunsten die Rechtsänderung eintritt, Vergütung

---

[629] BGH, Urt. v. 9.3.1989 – I ZR 189/86 –, BGHZ 107, 117 - Forschungskosten.
[630] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 439 Fn. 186 m.w.N.
[631] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 473 ff. Aus diesem Grund hat der Bundesgerichtshof einen Anspruch auf Umschreibung eines Domainnamens aus § 687 Abs. 2 BGB und § 812 Abs. 1 S. 1 (2. Alt.) BGB verneint, weil der Eintrag eines Domainnamens nicht im Sinne eines ausschließen Rechts einer Person zugewiesen ist.
[632] *Ensthaler*, Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473 (3476); vgl. auch *Hoeren*, Dateneigentum - Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (490); *Zech*, Information als Schutzgegenstand, S. 270 ff.

in Geld nach den Vorschriften der §§ 812 ff. BGB fordern. Ein Rechtsverlust nach § 950 BGB kann durch Verarbeitung oder Umbildung eines oder mehrerer Stoffe in eine neue bewegliche Sache eintreten, auch etwa durch Beschreiben, Bedrucken eines Stoffes (§ 950 Abs. 1 S. 2 BGB). Der Hersteller der neuen Sache erwirbt hieran das Eigentum, sofern nicht der Wert der Verarbeitung oder Umbildung erheblich geringer ist als der Wert des Stoffes bzw. des Rohmaterials. Die Vorschrift des § 950 BGB könnte in zweierlei Hinsicht auf Daten Anwendung finden: zunächst in direkter Anwendung mit Blick auf den Datenspeicherungsvorgang auf ein Speichermedium („Beschreiben des Mediums"), ferner in einer analogen Anwendung für den Vorgang der Datenverarbeitung.

a. Direkte Anwendung von § 950 BGB: „Beschreiben" des Speichermediums als Verarbeitung (§ 950 BGB)

Der Wortlaut von § 950 BGB erfordert, dass durch die Verarbeitung oder Umbildung eines oder mehrerer Stoffe eine neue bewegliche Sache herstellt wird. Bei weiter Auslegung könnte man darunter den Vorgang subsumieren, bei dem Daten auf einem körperlichen Gegenstand (etwa einem Tonband, einer Diskette) durch Aufspielen elektromagnetischer Signale verkörpert werden. Dies legt § 950 Abs. 1 S. 2 BGB nahe, nach welchem auch das Schreiben, Zeichnen, Malen, Drucken, Gravieren oder eine ähnliche Bearbeitung der Oberfläche als Verarbeitung gelten. Beim Beschreiben etwa eines Magnetbandes kommt es auf diesem zu einer körperlichen Veränderung. Das Band wird von Ort zu Ort unterschiedlich stark magnetisiert, was später beim Abtastvorgang wieder sichtbar gemacht werden kann. Die Substanz des Magnetbandes wird also in der Weise (revisibel) verändert, dass die Substanz an den verschiedenen Stellen unterschiedlich stark magnetisiert ist.

Nach § 950 BGB ist allerdings weiterhin erforderlich, dass durch die Verarbeitung eine „neue Sache" hergestellt wird. Ob eine neue Sache hergestellt wird, bestimmt sich maßgeblich nach der Verkehrsauffassung unter Berücksichtigung wirtschaftlicher Gesichtspunkte.[633] Eine neue Sache liegt dann vor, wenn sie eine eigenständige, gegenüber den einzelnen verarbeiteten Sachen weitergehende Funktion erfüllt. Hat sich durch die Verarbeitung der wesentliche wirtschaftliche Verwendungszweck geändert und hat der Ausgangsstoff nach der Verkehrsauffassung durch die vorgenommenen Handlungen eine Wesensänderung erfahren, spricht dies für das Entstehen einer neuen Sache. Entscheidend ist, dass zwischen Ausgangsstoff und Verarbeitungsprodukt keine Identität mehr besteht. In diesem Zusammenhang ist ein wesentliches Indiz für das Entstehen einer neuen Sache, wenn das Ergebnis der Verarbeitung im allgemeinen Sprachgebrauch mit einem anderen Begriff bezeichnet wird als der verarbeitete

---

[633] MüKo/*Füller,* BGB, § 950 Rn. 7 f.; Jauernig/*Berger*, BGB, § 950 Rn. 3.

Stoff.[634] Hieran wird es bei der Speicherung digitaler Daten in der Regel fehlen. Der Bundesgerichtshof differenziert danach, ob das Speichermedium seine Funktion verloren hat oder ob es weiterhin als Speicherort für Daten zur Verfügung steht. Das eingangs beispielhaft genannte Speichermedium „Magnetband" wird demnach auch dann nicht zu einer neuen Sache, wenn es etwa wegen der historischen Bedeutung der aufgenommenen Inhalte nur einmal bespielt werden soll.[635] Dagegen soll ein Ton- bzw. Datenträger dann zu einer neuen Sache werden, wenn z.B. ein CD-Rohling mit Musiktiteln bespielt wird, die in dieser Form vertrieben werden sollen. Der CD-Rohling verliert durch das kommerzielle Bespielen gleichsam seine Funktion als Speichermedium und wird dadurch zum Absatzprodukt, also zu einer neuen Sache.

Wenn schon das körperliche „Beschreiben" eines Magnetbandes oder das Beschreiben einer CD-ROM nicht oder nur unter engen Voraussetzungen zur Herstellung einer neuen Sache führt, so kann dies umso weniger beim Abspeichern von Daten auf einer Festplatte gelten. Durch das Generieren, Abspeichern, Sammeln und Verarbeiten von Daten wird zwar auf den entsprechenden Speichermedien (Festplatte, Server etc.) eine Veränderung herbeigeführt. Im Gegensatz zu einer CD können Speicherkapazitäten auf einer Festplatte und einem Server aber immer wieder gelöscht, modifiziert und neu genutzt und mithin die Veränderungen auf dem Speichermedium rückgängig gemacht werden.

b. Analoge Anwendung von § 950 BGB: Daten als Rohmaterialien, die verarbeitet werden

Eine analoge Anwendung der (in direkter Anwendung nur körperliche Gegenstände erfassenden) Vorschrift des § 950 BGB käme unter dem Blickwinkel in Betracht, dass nicht das zu beschreibende Speichermedium als Rohmaterial angesehen wird, sondern die Daten selbst. Digitale „Rohmaterialien" werden bei der Datenverarbeitung bearbeitet und zu einer „neuen Sache geformt".[636]

Die analoge Anwendung von § 950 BGB auf Daten als Rohmaterial, die zu einer neuen „Sache" (Datengesamtheit) verarbeitet werden, ist jedoch aus mehreren Gründen rechtsdogmatisch bedenklich: Die Vorschrift des § 950 BGB setzt zunächst eine „alte" Sache (Rohmaterial) voraus, an der Eigentum besteht.[637] Ein solches Eigentumsrecht an den bloßen Rohdaten kennt die Rechtsordnung aber

---

[634] BeckOK/*Kindl,* BGB, § 950 Rn. 5.
[635] BGH, Urt. v. 10.7.2015 – V ZR 206/14 –, NJW 2016, 317 - Tonbänder Helmut Kohl; anders noch OLG Karlsruhe, Beschl. v. 6.10.1986 – 6 U 160/86 –, CR 1987, 19; LAG Chemnitz, Urt. v. 17.1.2007 – 2 Sa 808/05 -, MMR 2008, 416; OLG Köln, Urt. v. 1.4.2016 – I-6 U 182/15 –, GRUR-RR 2016, 419.
[636] *Ensthaler,* Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473 (3476).
[637] Vgl. *Drexl*, Neue Regeln für die Europäische Datenwirtschaft?, NZKart 2017, 339 (341).

bislang nicht.[638] Die analoge Anwendung von Spezialvorschriften zum gesetzlichen Eigentumserwerb an Sachen auf nicht zugeordnete Güter erscheint indes problematisch, wenn nicht gar ausgeschlossen.[639] Durch die „Verarbeitung" der Rohdaten entsteht auch keine „neue Sache". Vielmehr sind sowohl die Rohdaten als auch die verarbeiteten Daten digitale Daten. Wenngleich die Rohdaten nunmehr verarbeitet und geordnet Schlüsse zulassen, erscheint es schwerlich möglich, diesen Unterschied bzw. diese „Verarbeitungshöhe" mit der sachenrechtlichen Kategorie der „neuen Sache" einzufangen. Die Rohdaten gehen durch ihre Verarbeitung auch nicht in der Weise „verloren", wie das Rohmaterial bei direkter Anwendung von § 950 BGB untergeht. Sie werden nicht in der Weise „be- bzw. verarbeitet" wie etwa eine ungebrauchte Leinwand oder ein CD-Rohling, der nach dem Bearbeitungsprozess als solcher nicht mehr vorhanden ist und auch nicht wieder hergestellt werden kann. Daher besteht auch gar kein Bedürfnis, für einen erlittenen „Rechtsverlust" nach § 951 BGB einen Ausgleich zu schaffen. Schließlich erscheint es nicht zwingend, dass die zusammengetragenen und verarbeiteten Daten in jedem Fall „wertvoller" sind als die Rohdaten selbst. In der Regel sind die „Rohdaten" (häufig als Öl des 21. Jahrhunderts bezeichnet) schon für sich genommen ein wertvolles Gut, das aufwändig zu beschaffen ist, während die Verarbeitung der Daten automatisiert durch einen Algorithmus erfolgen kann.

Entscheidend ist, dass mit einer analogen Anwendung von § 950 BGB auf die digitale Datenverarbeitung der Normzweck dieser Vorschrift verfehlt würde. Deren Ziel ist die klare und nachvollziehbare Eigentumszuordnung.[640] Der Eigentumserwerb durch Verarbeitung dient in erster Linie der Rechtsklarheit und soll einfach subsumierbare Eigentumsverhältnisse schaffen. In den hier untersuchten Fällen bliebe stets im Unklaren, ab welchem Grad eine „neue Sache" hergestellt ist und wer der „Verarbeiter" der Rohdaten ist. § 950 BGB nimmt dem Rechtsanwender diese Wertungsfragen gerade nicht ab, sondern setzt deren Beantwortung voraus. Dann ist aber für die Frage der Güterzuordnung durch § 950 BGB nichts gewonnen. Ob beispielsweise die natürliche Person, die beim Autofahren Rohdaten produziert, oder das Unternehmen, welches diese Daten sammelt, (ursprünglicher) Inhaber dieser konkreten Daten ist, ist eine Vorfrage, welche § 950 BGB nicht klärt. Nach den Grundsätzen der herkömmlichen Praxis wird im Rahmen von § 950 BGB als Hersteller angesehen, wer das wirtschaftliche Risiko des Verarbeitungsvorgangs trägt. Ob dies das Unternehmen ist, das die technischen Vorrichtungen zur Erfassung der Daten an der jeweiligen Maschine anbringt[641] oder aber der Autofahrer, ist eine offene Frage, zu deren Klärung § 950 BGB nichts beiträgt.

---

[638] Bericht der Arbeitsgruppe „Digitaler Neustart", S. 98.
[639] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 855.
[640] MüKo/*Füller,* BGB, § 950 Rn. 1.
[641] So *Ensthaler,* Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473 (3476).

Neben der Rechtsklarheit dient die Vorschrift dazu, den Interessenkonflikt hinsichtlich der Güterzuordnung zwischen dem Stofflieferanten und dem Verarbeiter bzw. Hersteller zu entscheiden. Ein solcher, die Zuordnung von Ausschließlichkeitsrechten betreffender Interessenkonflikt besteht mangels Rivalität der Daten nicht. Auf der anderen Seite würde eine analoge Anwendung von § 950 BGB die Auflösung eines durch die bewirkte Güterzuordnung herbeigeführten anderen Normenkonflikts erschweren, wenn nicht unmöglich machen: Die Schaffung eines Leistungsschutzrechts konfligiert nahezu zwangsläufig mit Rechtszuweisungen anderer Rechtsgebiete, etwa dem Geheimnisschutz oder dem Datenschutz (wenn die Maschinendaten Rückschlüsse auf personenbezogene Merkmale zulassen); dies deshalb, weil eine güterrechtliche Zuweisung anderen Wertungen folgen kann als etwa die datenschutzrechtliche. Dieser Zuweisungskonflikt würde durch eine entsprechende Anwendung von § 950 BGB auf Daten verschärft, weil diese zur Folge hätte, dass der gesetzliche Rechtserwerb an den verarbeiteten Daten indisponibel wäre, wie dies von Rechtsprechung und überwiegender Ansicht im Schrifttum für den gesetzlichen Eigentumserwerb an Sachen vertreten wird.[642]

Schließlich erscheint der Rückgriff auf den Gedanken von § 950 BGB bei der Betrachtung des gesamten Untertitels der §§ 946 ff. BGB als wenig naheliegend. Dem Vorgang der Datenverarbeitung im Sinne einer Erkenntnisgewinnung aus der Datenmenge geht in der Regel das Zusammentragen von Rohdaten unterschiedlicher Herkunft voraus. Der „Eigentumsverlust“ folgt nicht aus der Strukturierung der Daten und der Informationsgewinnung, sondern vielmehr aus der Zusammenführung der Rohdaten unterschiedlicher „Urheber“ zu einer Datenmenge. Dann entsteht eine Datengesamtheit. Es kommt - bildlich gesprochen - unter Umständen zu einer untrennbaren „Vermischung“ und „Vermengung“ von Daten, wenn man diese nicht mehr nachträglich auftrennen kann. Diesen Gedanken konsequent fortgeführt, läge eine analoge Anwendung von § 948 BGB (Vermischung von Sachen) näher als eine solche von § 950 BGB mit der Folge des Entstehens einer Bruchteilsgemeinschaft. Für einen Leistungsschutz in Form der Entschädigung nach § 951 BGB analog bliebe in diesem Fall kein Raum.

---

[642] BGH, Urt. v. 15.6.1989 - IX ZR 167/88, NJW 1989, 3213; MüKo/*Füller,* BGB, § 950 Rn. 15 f. mit zahlreichen weiteren Nachweisen; *Wadle*, Das Problem der fremdwirkenden Verarbeitung, JuS 1982, 477 (478 f.); *Westermann/Gursky/Eickmann*, SachenR, § 53 Rn. 10; *Zeuner,* Arbeitnehmer, Verarbeitung durch A. (Eigentumserwerb), Eigentumserwerb, durch Verarbeitung, Verarbeitung, Eigentumserwerb durch V., JZ 1955, 195 (196).

5. Zusammenfassung und Zwischenergebnis

Nach alledem kann festgehalten werden, dass das Bürgerliche Recht maschinengenerierte Daten nicht im Sinne eines Leistungsschutzrechts ausschließlich zuweist und außerhalb von § 826 BGB auch keinen Investitionsschutz gewährt.

II. Urheberrechtsschutz an maschinengenerierten Daten

Das Urheberrecht schützt Werke der Literatur, Wissenschaft und Kunst, insbesondere in den in § 2 Abs. 1 UrhG genannten Formen. Werkschutz für maschinell generierte Daten scheidet schon begrifflich aus. Die nach dem Urheberrechtsgesetz geschützten Werke sind nur persönliche geistige Schöpfungen (§ 2 Abs. 2 UrhG), während es sich bei den untersuchten Daten um Erzeugnisse einer Maschine handelt. Auch in Fällen, in denen die Datengenerierung mittelbar auf menschliches Handeln zurückzuführen ist (Heizverhalten, Rasiergewohnheiten, Fahrverhalten etc.), fehlt den Aufzeichnungen des menschlichen Verhaltens jedenfalls das Merkmal der geistigen Schöpfung. Die generierten Daten bringen für sich genommen keinen geistigen Inhalt gedanklicher Art zum Ausdruck.

Dies gilt auch für „Schöpfungen“, die ohne gestalterische Tätigkeit eines Menschen von Maschinen hervorgebracht werden, etwa eine Übersetzung oder eine Graphik.[643] Es ist weithin anerkannt, dass dem Inhaber eines Urheberrechts an einer entsprechenden Software (z.B. Übersetzungssoftware) nicht das Urheberrecht an dessen Erzeugnissen zuzuordnen ist, jedenfalls dann nicht, wenn das Erzeugnis nicht durch die menschlich-gestaltende Tätigkeit seine Prägung erhält.[644] Das Urheberrecht kennt - im Gegensatz zum Patentrecht[645] - keine Ausdehnung des Schutzbereichs auf Erzeugnisse menschlicher Schöpfungen im Sinne eines derivativen Schutzes, weshalb ein Schutz für die mittels Maschinen ohne prägende menschliche Beteiligung geschaffenen maschinellen Daten nicht in Betracht kommt.

Urheberrechtsschutz genießen gemäß § 4 UrhG auch Datenbankwerke. Hierbei handelt es sich um eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind (§ 4 Abs. 2 S. 1 UrhG). Ein Schutz als Datenbank*werk* kommt schon begrifflich nur in Betracht, wenn die Auswahl oder Anordnung der enthaltenen Elemente auf einer

---

[643] Von einer näheren Betrachtung von Schöpfungen durch sogenannte „künstliche Intelligenz“ soll hier abgesehen werden.
[644] Schricker/Loewenheim/*Loewenheim*, Urheberrecht, § 2 Rn. 39.
[645] Hierzu *Hetmank/Lauber-Rönsberg,* Künstliche Intelligenz - Herausforderungen für das Immaterialgüterrecht, GRUR 2018, 574 (576 ff.).

schöpferischen Leistung beruht.[646] Maßgeblich ist, dass die Struktur der Datenbank auf freien und kreativen Entscheidungen des Urhebers beruht und schöpferische Fähigkeiten in eigenständiger Weise zum Ausdruck bringt. Hieran fehlt es bei den hier untersuchten Daten, weil sie Maschinenerzeugnisse sind. Da deren Auswahl und Anordnung nicht auf individueller Kreativität beruhen, liegt ein Datenbankwerk im Sinne von § 4 Abs. 2 UrhG nicht vor.[647]

III. Leistungsschutz nach dem *sui-generis*-Schutz des Datenbankherstellers

Bei der Untersuchung, ob nach geltendem Recht Leistungsschutzrechte an Maschinendaten bestehen, kommt der Auslotung des Anwendungsbereichs des Schutzrechts für Datenbanken Bedeutung zu. Die Europäische Kommission hat jüngst gar die Frage aufgeworfen, ob das Schutzrecht *sui generis* nach Art. 7 ff. der Richtlinie über den rechtlichen Schutz von Datenbanken[648] (im Folgenden: Datenbankrichtlinie) breiter angewandt werden könnte als bislang angenommen.[649] Es erscheint daher lohnenswert näher zu untersuchen, ob das Leistungsschutzrecht des Datenbankherstellers Rechte an einzelnen maschinengenerierten Daten zuweist. Im Anschluss soll darlegt werden, ob und gegebenenfalls welche Rolle dem *sui-generis*-Leistungsschutzrecht des Datenbankherstellers beim Schutz maschinengenerierter Daten zukommt (unten 2.).

1. Immaterialgüterschutz an Daten kraft Datenbankherstellerschutz?

Das durch §§ 87a ff. UrhG umgesetzte Schutzrecht des Datenbankherstellers ergänzt den bereits früher bestehenden Schutz von Sammelwerken und Datenbankwerken nach § 4 UrhG, indem er die Voraussetzung einer persönlichen geistigen Schöpfung durch das Merkmal der wesentlichen Investition ersetzt.[650] Das Recht nach §§ 87a ff. UrhG erwirbt derjenige, der in die Herstellung einer Datenbank, das heißt in die Beschaffung, Überprüfung oder Darstellung ihres Inhalts, eine nach Art und Umfang wesentliche Investition getätigt hat. Das Recht liegt in der ausschließlichen Befugnis, die Vervielfältigung, Verbreitung

---

[646] Schricker/Loewenheim/*Leistner*, Urheberrecht, § 4 Rn. 50; *Rehbinder/Peukert,* Urheberrecht, Rn. 336.

[647] Statt vieler *Zech,* "Industrie 4.0" - Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1157); *Specht*, Ausschließlichkeitsrechte an Daten - Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288 (293).

[648] Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, Amtsblatt der EG Nr. L 77/20.

[649] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau eines gemeinsamen europäischen Datenraums“, COM(2018) 232 final, S. 7.

[650] *Zech,* Information als Schutzgegenstand, S. 360; Dreier/Schulze/*Dreier*, Urheberrechtsgesetz, vor §§ 87a ff. Rn. 1.

oder öffentliche Wiedergabe der Gesamtheit oder eines wesentlichen Teils des Inhalts der Datenbank zu untersagen.[651] Schutzgegenstand des Herstellerrechts ist damit nur die Datenbank als Gesamtheit oder der nach Art und Umfang wesentliche Teil der Datenbank. Nur diese Gesamtheit, nicht aber die in der Datenbank enthaltenen Daten selbst, stellt ein immaterielles Gut dar und wird dem Datenbankhersteller im Sinne von § 87a Abs. 2 UrhG zugeordnet. Eine Rechtezuweisung an Einzeldaten ist damit nicht verbunden.

Zwar wird in der Literatur zu Recht darauf hingewiesen, dass den in die Datenbankstruktur aufgenommenen Einzeldaten (mittelbar) Leistungsschutz insoweit zukommt, als ein wesentlicher Teil der Datenbank nicht vervielfältigt, verbreitet oder öffentlich wiedergegeben werden darf.[652] Dass dieser mittelbare Schutz Ausschließlichkeitsrechte an den Einzeldaten vermittelt, wird hingegen einhellig verneint.

2. Reichweite des *sui-generis*-Leistungsschutzes des Datenbankherstellers

Über die Anwendung des *sui-generis*-Leistungsschutzes des Datenbankherstellers auf maschinengenerierte Daten besteht Unsicherheit.[653] Einigkeit besteht weitestgehend darüber, unter welchen Voraussetzungen Daten in Datenbanken strukturiert sind (hierzu unten a.). Im Hinblick auf maschinengenerierte Daten bereitet das Erfordernis einer wesentlichen Investition in die Beschaffung, Überprüfung oder Darstellung der Daten besondere rechtlichen Schwierigkeiten (hierzu unten b.). Abschließend wird gezeigt, wem das Leistungsschutzrecht zugewiesen ist (hierzu unten c.).

a. Sammlung von (unabhängigen) Daten

Der Begriff der Datenbank wird in § 87a Abs. 1 UrhG legaldefiniert als „eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert." Der Begriff der Sammlung setzt voraus, dass es sich jedenfalls um eine Vielzahl von Elementen handelt, ohne dass sich eine konkrete Mindestanzahl verbindlich

---

[651] Dreier/Schulze/*Dreier*, Urheberrechtsgesetz, vor §§ 87a ff. Rn. 1; Wandtke/Bullinger/*Thum/Hermes*, UrhG, vor §§ 87a ff. Rn. 24.

[652] *Wiebe,* Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338 (345); Dreier/Schulze/*Dreier*, Urheberrechtsgesetz, vor §§ 87a ff. Rn. 1.

[653] So die Einschätzung der EU-Kommission in ihrer Evaluierung der Datenbankrichtlinie vom 25. April 2018, SWD(2018) 146 fin., S. 24 ff. nach Auswertung von Rechtsprechung und wissenschaftlicher Literatur in den EU-Mitgliedstaaten und Anhörung verschiedener Interessenvertreter.

bestimmen ließe.[654] Da bei einer automatisierten Datengenerierung, etwa durch Messung und erst recht beim Zusammenführen von Daten mehrerer Geräte, Sammlungen mit einer Vielzahl von Einzeldaten entstehen, scheitert der Schutz maschinell generierter Daten durch §§ 87a ff UrhG jedenfalls regelmäßig nicht am Merkmal der Datensammlung.[655]

Diese in der Sammlung zusammengestellten Daten sind, wie § 87a Abs. 1 S. 1 UrhG verlangt, regelmäßig auch voneinander unabhängig. Mit dem Merkmal der Unabhängigkeit werden Gestaltungen aus dem Datenbankbegriff ausgegrenzt, die von vornherein auf ein Ganzes geschaffen sind, inhaltliche Wechselbeziehungen aufweisen und so in ihrer Verschmelzung eine einheitliche Aussage bilden.[656] Zwar wollen die Beteiligten der Datengenerierung regelmäßig aus den generierten Einzeldaten einen Mehrwert schaffen. Dies ändert jedoch nichts an dem Umstand, dass die Einzeldaten für sich genommen einen selbständigen Aussagewert haben (Luftdruck y im Zeitpunkt x) und bei Trennung einen eigenen, wenn auch verminderten, Aussagewert behalten. Von eher akademischer Bedeutung ist die Frage, ob bereits die gesammelten, noch unverarbeiteten „Rohdaten" den Schutz von § 87a UrhG genießen. Deren Unabhängigkeit im Sinne der genannten Vorschrift wird teilweise verneint, weil diese nicht nach vorgegebenen Ordnungskriterien zusammengestellt seien[657], wobei auch diese Autoren konzedieren, dass „Datenhaufen" Element einer Datenbank sein können. Unbestritten ist, dass die bei der Datenerhebung gewonnenen Primärdaten (z.B. Messwerte) unabhängige Elemente sein können, wie dies für Wetterdaten[658], geografische Daten[659] oder bloße Verkaufszahlen[660] höchstrichterlich entschieden wurde. Solange diesen „Rohdaten" (irgend)ein selbständiger Informationswert bis zur Grenze der Inhaltslosigkeit[661] des Einzelzeichens zukommt, reicht dies für die Unabhängigkeit[662] des Datums aus. Da es gerade Kennzeichen der Auswertung von großen Datenmengen ist, dass jedes noch so scheinbar un-

---

[654] EuGH, Urt. v. 9.11.2004 – C-444/02 –, GRUR 2005, 254 f. - Fixtures-Fußballpläne II; Wandtke/Bullinger/*Thum/Hermes*, Urheberrecht, § 87a Rn. 10 f.

[655] *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (418).

[656] LG München I, Urt. v. 30.3.2000 – 7 O 3625/98 –, NJW 2000, 2214 (2215); *Wiebe,* Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338.

[657] Schricker/Loewenheim/*Vogel* , Urheberrecht, § 87a Rn. 22; Dreier/Schulze/*Dreier*, Urheberrechtsgesetz, § 87a Rn. 7.

[658] OLG Köln, Urt. v. 15.12.2006 – 6 U 229/05 –, MMR 2007, 443; ebenso *Gaster*, Der Rechtsschutz von Datenbanken, 1999, Rn. 66.

[659] EuGH, Urt. v. 29.10.2015 – C-490/14 –, AfP 2016, 33 - Verlag Esterbauer; LG München I, Urt. v. 9.11.2005 – 21 O 7402/02 –, GRUR 2006, 225.

[660] BGH, Urt. v. 21.7.2005 – I ZR 290/02 –, GRUR 2005, 857 - HIT BILANZ; BGH, Urt. v. 21.4.2005 – I ZR 1/02 –, GRUR 2005, 940 (941) - Marktstudien.

[661] Schricker/Loewenheim/*Vogel* , Urheberrecht, § 87a Rn. 12 m.w.N.

[662] BGH, Urt. v. 21.7.2005 – I ZR 290/02 –, GRUR 2005, 857 f.; Schricker/Loewenheim/*Vogel*, Urheberrecht, § 87a Rn. 8.

bedeutende Primärdatum für eine spätere Analyse nutzbar gemacht werden kann[663], dürfte die Ausklammerung von „Rohdaten“ aus dem Datenbankbegriff jedenfalls im hier untersuchten Kontext keine Bedeutung haben.

Die unabhängigen Elemente müssen weiter einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sein. Einzeln zugänglich ist ein Element, wenn es isoliert aus der Datenbank abgerufen werden kann.[664] Dieses Erfordernis ist regelmäßig erfüllt, schon weil die an der Datengenerierung Beteiligten zwecks Datenanalyse auf die einzelnen Daten zugreifen wollen und ihnen typischerweise die entsprechende Software zur Verfügung steht.[665]

Schließlich steht der Anwendung der §§ 87a ff. UrhG auf Maschinendaten nicht entgegen, dass diese systematisch oder methodisch angeordnet sein müssen. Dieses Merkmal verlangt eine Methode oder ein System beliebiger Art, mit der bzw. mit dem sich jedes der Elemente der Sammlung wieder auffinden lässt.[666] Entscheidend ist somit die Verbindung des Datenbestandes mit einem Abfragemittel, das zielgerichtet Recherchen nach Einzelelementen in dem Datenbestand ermöglicht.[667] Dem Kriterium kommt neben dem Merkmal der Einzelzugänglichkeit keine eigenständige Bedeutung zu, weil sich nur durch eine systematische oder methodische Anordnung Einzelzugänglichkeit erreichen lässt.[668] Es erschöpft sich in der Vorgabe, dass die Daten logischen oder sachlichen Zusammenhängen folgend oder planmäßig strukturiert angeordnet sein müssen und ist dementsprechend unter denselben Voraussetzungen erfüllt wie das Merkmal der Einzelzugänglichkeit.[669]

---

[663] Studie des BMVI, „Eigentumsordnung“ für Mobilitätsdaten, S. 52; *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (419).

[664] Vgl. EuGH, Urt. v. 9.11.2004 – C-444/02 –, GRUR 2005, 254 f. Rn. 30, 32 – Fixtures-Fußballspielpläne II; Wandtke/Bullinger/*Thum/Hermes*, UrhR, § 87a Rn. 14.

[665] Problematisch ist das Merkmal der Einzelzugänglichkeit bei erlerntem Verhalten selbstlernender Maschinen und bei neuronalen Netzen. In diesen Anwendungsfällen der künstlichen Intelligenz werden Daten generiert, die dem Nutzer verborgene Informationen enthalten. Die Dateneigenschaft verneinen Schricker/Loewenheim/*Vogel*, Urheberrecht, § 87a Rn. 13; *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (420). Diese Problematik ist hingegen nicht Gegenstand dieser Untersuchung.

[666] EuGH, Urt. v. 9.11.2004 – C-444/02 –, GRUR 2005, 254 f.; *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (419).

[667] Wandtke/Bullinger/*Thum/Hermes*, UrhR, § 87a Rn. 19.

[668] *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (419). In diese Richtung auch Wandtke/Bullinger/*Thum/Hermes*, UrhR, § 87a Rn. 14, die wiederum dem Tatbestandsmerkmal der Einzelzugänglichkeit einen eigenen Bedeutungsgehalt absprechen und in dem Merkmal nur eine Klarstellung erblicken, dass sowohl elektronische als auch herkömmliche analoge Datenbanken dem Datenbankschutz unterfallen.

[669] Wandtke/Bullinger/*Thum/Hermes*, UrhR, § 87a Rn. 25 f.; Schricker/Loewenheim/*Vogel*, Urheberrecht, § 87a Rn. 19 ff.

b. Wesentliche Investition

Ob das Leistungsschutzrecht im Einzelfall besteht, hängt somit allein davon ab, ob eine nach Art und Umfang wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung der einzelnen Daten getätigt worden ist. Schutzgegenstand ist die wesentliche Investition des Datenbankherstellers.[670] Mit Blick auf den Schutzzweck der Richtlinie ist nach der Rechtsprechung des Europäischen Gerichtshofs der Begriff der mit der Beschaffung des Inhalts einer Datenbank verbundenen Investition im Sinne des Art. 7 Abs. 1 der Datenbankrichtlinie dahin zu verstehen, dass diese (nur) die Mittel bezeichnet, die der Ermittlung von vorhandenen Elementen und deren Zusammenstellung in dieser Datenbank gewidmet werden.[671] Das (Schutz-)Recht schützt daher Investitionen in die Beschaffung, Sammlung, Überprüfung, Aufbereitung und Darbietung der Daten, nicht aber Investitionen in die Erzeugung der Daten selbst. Die enge Auslegung des sachlichen Anwendungsbereichs der Datenbankrichtlinie durch den Europäischen Gerichtshofs ist dem Ziel geschuldet, einen möglichst freien Datenzugang und Datenverkehr sicherzustellen und Datenmonopole zu verhindern. Zudem dient sie dem Zweck, Investitionen zur Herstellung von Datenbanken und nicht zur Generierung von Daten zu erhöhen.[672]

Diese Rechtsprechung führt in der Praxis zu gewisser Ratlosigkeit und gibt die bislang rechtlich nicht eindeutig gelöste Frage auf, wie Investitionen in die Datengenerierung von berücksichtigungsfähigen Investitionen in die Datenbeschaffung abzugrenzen sind. Die Beantwortung dieser Frage wird als entscheidende Aufgabe für einen rechtssicher ausgestalteten Datenbankschutz im Hinblick auf maschinengenierte Daten angesehen.[673]

Die Relevanz des Problems sei an dem folgenden Beispiel vor Augen geführt: Ähnlich wie in dem in der Einleitung erwähnten Streitfall zwischen Lufthansa, Airbus und Boeing bieten zahlreiche Automobilhersteller eine Online-Diagnose von Fahrzeugen als zusätzliche Dienstleistung an. Mittels Sensoren werden

---

[670] Dreier/Schulze/*Dreier*, Urheberrechtsgesetz, § 87a Rn. 11; *Rehbinder/Peukert,* Urheberrecht, Rn. 841.

[671] EuGH, Urt. v. 9.11.2004 – C-203/02 –, GRUR 2005, 244 Tz. 42 - BHB-Pferdewetten.

[672] Vgl. insbesondere Erwägungsgründe 10 bis 12 der Datenbankrichtlinie.

[673] EU-Kommission, Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 146 fin., S. 27, abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-and-executive-summary-evaluation-directive-969ec-legal-protection (letzter Abruf: 21.2.2019), *Leistner,* Datenbankschutz - Abgrenzung zwischen Datensammlung und Datengenerierung, CR 2018, 17 (18) und JZ 2005, 408 ff.; *Ehmann,* Big Data auf unsicherer Grundlage - was ist "wesentlich" beim Investitionsschutz für Datenbanken?, K&R 2014, 394 (397 ff.); *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (421); *Wiebe,* Der Schutz von Datenbanken - ungeliebtes Stiefkind des Immaterialgüterrechts, CR 2014, 1 (4).

Messwerte über die Luftmenge, Kraftstoffmenge, Drehzahlen etc. unmittelbar am Automobil erfasst und zum Teil durch elektronische Steuergeräte direkt im Fahrzeug verarbeitet.[674] Die erhobenen Sensordaten oder die im Fahrzeug errechneten Diagnoseergebnisse werden via Mobilfunk an den Hersteller übertragen, der diese wiederum an eine Werkstatt weiterleitet. Gesammelt werden sie also entweder unmittelbar am Aufnahmeort (Automobil) oder nach Übertragung am Zielort (Hersteller bzw. Werkstatt). Stellen die gesammelten Daten eine Datenbank im Sinne von § 87a UrhG dar, wovon nach den obigen Ausführungen regelmäßig auszugehen sein wird, kann sich der Datenbankhersteller[675] unter den weiteren Voraussetzungen der §§ 87a ff. UrhG gegen die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Datenbank insgesamt oder eines nach Art oder Umfang wesentlichen Teils der Datenbank wenden und gegen den Rechtsverletzer Ansprüche nach §§ 97 ff. UrhG geltend machen (insbesondere auf Unterlassung, Beseitigung, Schadensersatz).

Die Rechtsprechung des Europäischen Gerichtshofs zugrunde gelegt, bleibt allerdings zweifelhaft, welche Investitionen berücksichtigungsfähig sind. Der Aufwand zur Datengenerierung - also der Betrieb des Fahrzeugs - wäre nicht vom Anwendungsbereich des Leistungsschutzrechts erfasst, weil es sich insoweit nicht um Investitionen in die Beschaffung vorhandener Daten handelt. Anders dürfte es sich indes bei dem Aufwand zur Erfassung von Daten verhalten, die in der Natur vorhanden sind und durch Messung erhoben und damit im Sinne der Rechtsprechung des Europäischen Gerichtshofs „beschafft werden".[676] Problematisch ist die Abgrenzung dann, wenn der Datenbankhersteller an der Datengenerierung mitwirkt, wenn also beispielsweise der Maschinenbetreiber die generierten Daten ohne oder nur mit geringem Zusatzaufwand selbst in einer Datenbank strukturiert. Der Europäische Gerichtshof unterzieht diese Konstellationen einer wertenden Betrachtung und fragt, ob die Investition primär dem Aufbau einer Datenbank dient oder anderen Zwecken.[677] Fallen die Daten als Nebenprodukt einer anderen selbständigen Tätigkeit ab, erfasse der Schutzzweck des Leistungsschutzrechts nicht die Ausgaben in deren Erzeugung (sogenannte „spin-off-Theorie"). Im Zusammenhang mit der automatischen Datengenerierung wird es jedoch immer schwieriger, zwischen Datenherstellung und Datenbeschaffung zu unterscheiden. Dies zeigt sich etwa bei der sensorgestützten Datenerhebung. So erzeugt der Fahrer einer mit Messsensoren ausgestatten Landmaschine Daten über seine Fahrtstrecke und sammelt diese gleichzeitig neben anderen Daten (geologischen Daten, Wetterdaten etc.). Damit kann der mit

---

[674] Das Beispiel stammt aus der Studie des BMVI, „Eigentumsordnung für Mobilitätsdaten", 2017, S. 21 f., abrufbar unter www.bmvi.de.
[675] Zur Zuordnung s. nachfolgend unter C. III. 2. c.
[676] *Schmidt/Zech,* Datenbankherstellerschutz für Rohdaten?, CR 2017, 417 (421).
[677] EuGH, Urt. v. 9.11.2004 - C-203/02 -, GRUR 2005, 244 - BHB Pferdewetten; Studie des BMVI, „Eigentumsordnung für Mobilitätsdaten", S. 52.

der Fahrt entstehende Aufwand der Datenerzeugung (Fahrtstrecke) zugerechnet werden, gleichzeitig aber auch der Datenbeschaffung. Denn die Tätigkeit des Landmaschinenfahrers erschöpft sich nicht in der Erzeugung der Daten über die Fahrtstrecke, sondern erstreckt sich auf die Sammlung „vorhandener" Daten über die Bodenbeschaffenheit. Da die gemessenen Daten in der Natur vorhanden sind und nur gemessen werden, dürfte es sich vorzugswürdig um einen Vorgang der Datenbeschaffung handeln, dessen Aufwand bei der Beurteilung der Wesentlichkeit der Investition einfließt.[678] Sie können aber auch der Datenerzeugung zugerechnet werden, weil der Einsatz der Landmaschine nicht primär der Datenerhebung dient und die gewonnenen Daten nur als Nebenprodukt abfallen. Ähnliche Abgrenzungsfragen stellen sich bei der Erfassung menschlichen Verhaltens. Auch in dem oben beschriebenen Beispiel fallen die Sensordaten gleichsam als Nebenprodukte des Fahrens ab.[679] Das Gleiche gilt für Produktionsdaten, die in Wertschöpfungsnetzwerken erhoben werden. Diese können dem Bereich der Datensammlung zuzuordnen sein, weil die Echtzeitdaten aus der Produktion (Stückzahl, Geschwindigkeit, Verzögerungen etc.) bereits vorhanden sind.[680] Sie können aber als Nebenprodukt des Produktionsprozesses auch der Datengenerierung zugeordnet werden, deren Investitionen nicht durch §§ 87a ff. UrhG geschützt sind.

Die Rechtsprechung des Europäischen Gerichtshofs wurde in den EU-Mitgliedstaaten unterschiedlich rezipiert.[681] Der Bundesgerichtshof hebt bei der Abgrenzung der berücksichtigungsfähigen Investitionen allein darauf ab, ob die gesammelten Daten vorhanden waren oder erst erzeugt werden mussten. Ob das primäre Ziel der Investition im Aufbau einer Datenbank bestand, spielt bei der Entscheidungsfindung ersichtlich keine Rolle. Exemplarisch zeigt sich dies in dem vom Bundesgerichtshof entschiedenen Fall über die Schutzfähigkeit von Aufwendungen bei Erhebung mautpflichtiger Fahrten.[682] Die Kosten für die Errichtung der stationären Mautterminals und für die Anschaffung der mobilen Fahrzeuggeräte sah der Bundesgerichtshof als von § 87a UrhG mittelbar geschützte Investitionen in die Beschaffung der Daten an, obwohl nicht primär der Aufbau einer Datenbank bezweckt war, sondern die Erhebung einer Maut. Denn die erfassten Daten der mautpflichtigen Fahrten (Kfz-Kennzeichen, Datum der Fahrt, Länge der gefahrenen Strecke) seien auch ohne Erfassung vorhanden. Et-

---

[678] Wandtke/Bullinger/*Thum/Hermes*, UrhR, § 87a Rn. 49 ff.; *Wiebe,* Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, CR 2017, 338 (341).
[679] Studie des BMVI, „Eigentumsordnung für Mobilitätsdaten", S. 53.
[680] Beispiel stammt von *Wiebe,* Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, CR 2017, 338 (341).
[681] Hierzu im Einzelnen der Bericht der EU-Kommission, Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 146 fin., S. 27 f.
[682] BGH, Urt. v. 25.3.2010 - I ZR 47/08 -, CR 2011, 43 - Toll Collect; ähnlich BGH, Urt. v. 21.7.2005 – I ZR 290/02 –, GRUR 2005, 857 - HIT BILANZ.

was anderes gelte nur für die errechnete Maut, weil es sich insoweit um ein Datum handele, das erst erzeugt werde.

Ist die Hürde der Schutzfähigkeit der Investition genommen, ist in einem zweiten Schritt zu prüfen, ob die Summe der berücksichtigungsfähigen Investitionen nach Art und Umfang insgesamt die Schwelle der Wesentlichkeit erreicht. Diesem Erfordernis wird in der Regel Genüge getan sein, weil - wenngleich die Schutzuntergrenze noch ungeklärt ist - an die Schwelle in der Rechtsprechung der EU-Mitgliedstaaten keine hohen Anforderungen gestellt werden.[683] So ließ der Bundesgerichtshof Investitionen in Höhe von 4000 Euro als wesentlich genügen.[684]

c. Zuweisung an Datenbankhersteller

Schließlich genießt der Datenbankhersteller im Sinne von § 87a Abs. 2 UrhG Leistungsschutz, der die Investition vorgenommen hat. Das ist derjenigen, der die Initiative zur Erstellung der Datenbank ergriffen hat und die Investition in die Datenbank trägt.[685] Im Beispiel des mit Sensoren ausgestatten Kraftfahrzeugs, in dem die erhobenen Daten lokal erfasst und in geordneter Form lokal abgelegt und gespeichert werden, kann eine Datenbank im Fahrzeug entstehen. Als Datenbankhersteller kommen dann Eigentümer und Halter des Fahrzeugs in Betracht, die durch Kaufpreiszahlung bzw. Unterhaltung der im Fahrzeug vorhandenen Technik die Investitionsleistung erbringen. Werden die Daten hingegen durch Online-Diagnose unmittelbar in Echtzeit an den Hersteller oder einen Werkstattbetrieb übermittelt und dort in geordneter Form abgelegt und gespeichert, entsteht die Datenbank außerhalb des Kraftfahrzeugs beim Hersteller bzw. beim Werkstattbetreiber. Geschützt wären also diejenigen, die Investitionen zur Sammlung, Sichtung und systematischen Anordnung der Daten tätigen.[686] Werden die Daten in einer zentralen Datenbank abgelegt, genießt nicht der Eigentümer des datengenerierenden Gerätes, sondern allein der Betreiber dieser Datenbank unter den Voraussetzungen von § 87a Abs. 1 UrhG Leistungsschutz.

---

[683] Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 146 Final, S. 27, abrufbar unter: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-and-executive-summary-evaluation-directive-969ec-legal-protection (letzter Abruf: 21.2.2019).

[684] BGH, Urt. v. 1.12.2010 – I ZR 196/08 –, GRUR 2011, 724 Zweite Zahnarztmeinung II.

[685] BGH, Urt. v. 1.12.2010 – I ZR 196/08 –, GRUR 2011, 724 - Zweite Zahnarztmeinung II; Wandtke/Bullinger/*Thum/Hermes*, UrhG, § 87a Rn. 131.

[686] Wohl zu Unrecht hält Sassenberg/Faber/*Sattler*, Rechtshandbuch Industrie 4.0 und Internet of Things, S. 35 die im Rahmen der sog. predictive maintenance vom Hersteller genutzten Daten für nicht durch § 87a UrhG geschützt.

d. Zusammenfassung

Die Vorschriften der §§ 87a ff. UrhG (sowie die ihnen zugrundeliegende Datenbank-richtlinie) schützen die Datenbank als systematische Anordnung und nicht die in der Datenbank enthaltenen Einzeldaten. Als Grundlage für ein „Schutzrecht des Datenerzeugers“ scheiden sie deshalb von vornherein aus.

Es konnte jedoch gezeigt werden, dass das Schutzrecht sui-generis grundsätzlich Investitionen im Zusammenhang mit maschinengenerierten Daten erfassen kann, wobei sich allerdings auch Abgrenzungsfragen stellen: Leistungsschutz für die Datengenerierung ist ausgeschlossen, weil nur Investitionen in die Beschaffung, Überprüfung oder Darstellung geschützt sind. Ob zu den geschützten Investitionen auch die Kosten der Datenbeschaffung fallen, wenn diese Daten als Nebenprodukt anfallen und die getätigten Investitionen nicht primär der Datenbeschaffung dienen, ist bislang nicht abschließend geklärt.

IV. Lauterkeitsrechtlicher Leistungsschutz

Ähnlich wie für § 826 BGB ist in der Vergangenheit immer wieder die Forderung erhoben worden, Ausschließlichkeitsrechte an neuen Gütern auf der Grundlage unmittelbaren Leistungsschutzes, der aus § 3 UWG hergeleitet werden soll, zu gewähren.[687] Eine solche Annahme wird durch eine weit zurückreichende Rechtsprechung genährt, die „eigenartige“ Waren und Dienstleistungen um ihrer selbst willen vor unerlaubten Nachahmungen und Übernahmen schützte.[688] Der wettbewerbsrechtlichen Generalklausel wird geradezu eine „Schrittmacherfunktion“ für die Güterzuordnung zugeschrieben.[689]

Ob § 3 UWG güterzuordnender Gehalt zukommt, ist heftig umstritten, betrifft aber einzig die Frage, ob die Generalklausel als Basis für eine *richterrechtliche* Entwicklung von Leistungsschutzrechten dienen kann. Zwingend vorgeschrieben - hierin besteht Einigkeit - ist die Gewährung unmittelbaren Leistungsschutzes nach dieser Vorschrift nicht. Aus diesem Grund lässt sich aus ihr *de lege lata* auch kein Ausschließlichkeitsrecht an maschinengenerierten Daten ableiten. Ob die Rechtsprechung zur Entwicklung eines solchen Rechts befugt wäre, ist zweifelhaft[690], kann aber offenbleiben.

Von der Güterzuordnung zu unterscheiden ist die Gewährung wettbewerbsrechtlichen Leistungsschutzes für getätigte Investitionen im Zusammenhang mit ma-

---

[687] *Schröer,* Der unmittelbare Leistungsschutz, S. 39 ff.
[688] Siehe hierzu oben unter C. I. 1. b.
[689] *Peukert*, Güterzuordnung als Rechtsprinzip, S. 316 ff.; *Sieber*, Informationsrecht und Recht der Informationstechnik, NJW 1989, 2569 (2575).
[690] Siehe hierzu bereits oben unter C. I. 1. b.

schinengenerierten Daten, etwa Datengenerierung oder Datenspeicherung. Anders als die Ausschließlichkeitsrechte, die unkörperliche Gegenstände einem Rechtssubjekt zuweisen und alle anderen vom Zugriff ausschließen, erklärt das Wettbewerbsrecht unlautere geschäftliche Handlungen für unzulässig und gewährt Abwehr- und Ersatzansprüche nach §§ 8 ff. UWG. Das Wettbewerbsrecht kodifiziert somit besonderes Verhaltensunrecht und hat keinen güterzuweisenden Gehalt.[691]

Dies gilt auch für den in § 4 UWG niedergelegten Schutz, der auf Wettbewerbshandlungen beschränkt ist, ohne das Leistungsergebnis als solches zu schützen.[692] Geschützt wird „nur" vor der unlauteren Vermarktung der Leistungsergebnisse durch Mitbewerber. Damit ist das „Wie" der Nachahmung betroffen, mithin das Verhalten im Zusammenhang mit der Herstellung und Vermarktung der Nachahmung.[693] Dies gilt auch für Daten, die Geschäfts- und Betriebsgeheimnisse beinhalten, also in Anlehnung an Art. 39 Abs. 2 TRIPS geheime Informationen mit kommerziellem Wert, die Gegenstand angemessener Geheimhaltungsmaßnahmen sind.[694] Denn auch insoweit wird kein Verbotsrecht für die Nutzung einer Information als solcher gewährt, sondern allein ein Schutz gegen unlauteren Zugang.[695]

1. Wettbewerbsrechtlicher Leistungsschutz nach § 4 Nr. 3 UWG

Der in § 4 Nr. 3 UWG normierte wettbewerbsrechtliche Leistungsschutz umfasst drei Tatbestände der unlauteren Produktnachahmung. Ihr gemeinsamer Normzweck ist der Schutz des Leistungsergebnisses eines Mitbewerbers vor einer Übernahme mit unlauteren Mitteln oder Methoden.[696] Nach dieser Vorschrift handelt unlauter, wer Waren oder Dienstleistungen anbietet, die eine Nachahmung der Waren oder Dienstleistungen anderer Wettbewerber sind, wenn er eine vermeidbare Täuschung der Abnehmer über die betriebliche Herkunft herbeiführt (lit. a), die Wertschätzung der nachgeahmten Ware oder Dienstleistung

---

[691] So die herrschende Auffassung, vgl. statt aller Ohly/Sosnitza/*Ohly*, UWG, Einf. D., Rn. 78: *Rehbinder/Peukert,* Urheberrecht, Rn. 114.

[692] BGH, Urt. v. 28.10.2010 – I ZR 60/09 –, GRUR 2011, 436 Rn. 17 - Hartplatzhelden.de.

[693] Zu den Voraussetzungen des lauterkeitsrechtlichen Nachahmungsschutzes siehe Köhler/Bornkamp/*Köhler*, UWG, § 4 Rn. 3.7.

[694] *Specht/Kerber*, Datenrechte – Eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland - USA, S. 21 f. Zum Begriff auch Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. EU 2016 v. 15.6.2016, Nr. L 157/1.

[695] *Specht/Kerber*, Datenrechte – Eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland - USA, S. 21 f.

[696] *Schröer,* Der unmittelbare Leistungsschutz, S. 11 ff.; *Hilty/Henning-Bodewig,* Leistungsschutzrecht für Sportveranstalter?, S. 45.

unangemessen ausnutzt oder beeinträchtigt (lit. b) oder die für die Nachahmung erforderlichen Kenntnisse oder Unterlagen unredlich erlangt hat (lit. c).

Die digitale Vervielfältigung fremder Daten erfüllt grundsätzlich den Nachahmungstatbestand der unmittelbaren Leistungsübernahme, sofern die Daten als Waren angeboten werden. Denn eine identische (unmittelbare) Nachahmung liegt vor, wenn die fremde Leistung unverändert übernommen wird.[697] Auch ist der Begriff der Waren und Dienstleistungen im Sinne von § 4 Nr. 3 UWG weit auszulegen und beinhaltet Leistungs- und Arbeitsergebnisse aller Art.[698] Maschinengenerierten Daten dürfte jedoch die für den Leistungsschutz nach § 4 Nr. 3 UWG notwendige wettbewerbliche Eigenart fehlen. Für die Annahme der wettbewerblichen Eigenart ist maßgebend, ob das Produkt durch seine konkrete Ausgestaltung oder bestimmte Merkmale geeignet ist, die interessierten Verkehrskreise auf seine betriebliche Herkunft oder seine Besonderheiten hinzuweisen.[699] Sie ist zu verneinen, wenn der angesprochene Verkehr die prägenden Gestaltungsmerkmale des Erzeugnisses nicht (mehr) einem bestimmten Hersteller oder einer bestimmten Ware zuordnet. Damit bezieht sich der lauterkeitsrechtliche Leistungsschutz immer nur auf die konkrete Gestaltung eines Erzeugnisses.[700] Die Annahme einer Nachahmung im Sinne von § 4 Nr. 3 UWG setzt mithin voraus, dass gerade die übernommenen *Gestaltungsmittel* diejenigen sind, die die wettbewerbliche Eigenart des nachgeahmten Produkts begründen.[701] Derartige Gestaltungsmittel fehlen Rohdaten; sie finden sich allenfalls in Datenstrukturen, etwa in der Zusammenstellung von Daten für bestimmte Zwecke. Die Rechtsprechung hat diese Voraussetzung bei Datenbanken als erfüllt angesehen, wenn der Verkehr besondere Gütevorstellungen aufgrund der Vollständigkeit und Zuverlässigkeit des Inhalts der Datenbank entwickelt hat.[702]

---

[697] BGH, Urt. v. 30.10.1968 – I ZR 52/66 –, BGHZ 51, 41 (45 f.) – Reprint; BGH, Urt. v. 6.5.1999 – I ZR 199/96 –, GRUR 1999, 923 (927) – Tele-Info-CD; *Becker*, Lauterkeitsrechtlicher Leistungsschutz für Daten, GRUR 2017, 346 (350).

[698] BGH, Urt. v. 22.3.2012 – I ZR 21/11 –, GRUR 2012, 1155 Rn. 19 - Sandmalkasten; BGH, Urt. v. 23.9.2015 – I ZR 105/14 –, GRUR 2015, 1214 - Goldbären.

[699] BGH, Urt. v. 15.4.2010 – I ZR 145/08 –, GRUR 2010, 1125 Rn. 21- Femur-Teil; BGH, Urt. v. 22.3.2012 – I ZR 21/11 –, GRUR 2012, 1155 Rn. 19 - Sandmalkasten.

[700] BGH, Urt. v. 4.5.2016 – I ZR 58/14 –, WRP 2017, 51 Rn. 71 – Segmentstruktur; Köhler/Bornkamm/Feddersen/*Köhler*, UWG § 4 Rn. 3.23.

701 BGH, Urt. v. 6.5.1999 – I ZR 199/96 –, BGHZ 141, 329 (340) - Tele-Info-CD; BGH, Urt. v. 11.1.2007 – I ZR 198/04 –, WRP 2007, 1076 - Handtaschen; BGH, Urt. v. 15.4.2010 – I ZR 145/08 –, GRUR 2010, 1125 Rn. 25 - Femur-Teil.

[702] BGH, Urt. v. 6.5.1999 – I ZR 199/96 –, BGHZ 141, 329 (341) - Tele-Info-CD; BGH, Urt. v. 4.5.2016 – I ZR 58/14 –, WRP 2017, 51 – Segmentstruktur.

2. Unmittelbarer Leistungsschutz nach § 3 UWG

Ob § 3 Abs. 1 UWG die Grundlage für einen sog. unmittelbaren Leistungsschutz bieten kann, wenn die Voraussetzungen des § 4 Nr. 3 UWG oder § 4 Nr. 4 UWG nicht erfüllt sind, ist noch nicht abschließend geklärt.[703] Der BGH hat dies bisher offengelassen, aber für den jeweiligen konkreten Fall verneint.[704] Das Schrifttum ist gespalten.[705]

Bei der Anwendung der Generalklausel des § 3 UWG als Schutz eigenartiger Leistungen oder Daten als solcher ist größte Zurückhaltung geboten. Nur ausnahmsweise ist die Nutzung nicht spezialgesetzlich zugewiesener Güter als unlautere geschäftliche Handlung gemäß § 3 UWG zu verbieten, wenn die angegriffene Handlung nach den Gesamtumständen die ernstliche Gefahr begründet, dass der Bestand des Wettbewerbs hinsichtlich der in Rede stehenden Warenart in nicht unerheblichem Maße durch die Beseitigung der Freiheit von Angebot und Nachfrage gefährdet ist.[706] Ein Marktversagen kann möglich sein, wenn der bestehende Rechtsschutz nicht ausreicht, um einen Anreiz zu einer bestimmten Investition zu schaffen und dadurch die Gefahr besteht, dass eine im Allgemeininteresse liegende Leistung unterbleibt.[707] Ein Marktversagen soll insbesondere dann angenommen werden, wenn die Herstellung des Originalprodukts wesentliche Investitionen erfordert; das Produkt mit minimalem Aufwand vervielfältig werden kann; der Originalhersteller weder rechtlich noch faktisch in der Lage ist, die Vervielfältigung zu verhindern und dadurch die ernsthafte Gefahr besteht, dass weder der ursprüngliche Anbieter noch ein anderer Mitbewerber in diesen Markt investiert.[708]. Unter diesen Voraussetzungen und unter Berücksichtigung der letztgenannten Konsequenz ist es vertretbar, das Verhalten des Kopisten als unlautere Geschäftshandlung gemäß § 3 UWG zu verbieten und Leis-

---

[703] BGH, GRUR 2011, 436 - Hartplatzhelden; *Schröer,* Der unmittelbare Leistungsschutz, S. 11 ff.; *Hilty/Henning-Bodewig,* Leistungsschutzrecht für Sportveranstalter?, S. 45.

[704] BGH, Urt. v. 28.10.2010 – I ZR 60/09 –, GRUR 2011, 436 Rn. 19 ff. – Hartplatzhelden.de mit Anm. Ohly; BGH, Urt. v. 19.11.2015 – I ZR 149/14 –, WRP 2016, 850 Rn. 21 ff. – Pippi-Langstrumpf-Kostüm II; BGH, Urt. v. 4.5.2016 – I ZR 58/14 –, WRP 2017, 51 Rn. 97 – Segmentstruktur.

[705] Für eine Anwendung des § 3 Abs. 1 UWG in Ausnahmefällen: *Becker,* Lauterkeitsrechtlicher Leistungsschutz für Daten, GRUR 2017, 346 (352 ff); *Büscher*, Aus der Rechtsprechung des EuGH und des BGH zum Lauterkeitsrecht seit 2015, GRUR 2017, 105 (106); *Ohly*, Hartplatzhelden.de oder: Wohin mit dem unmittelbaren Leistungsschutz?, GRUR 2010, 487 (492 f.). Grds. gegen eine Anwendung Köhler/Bornkamm/*Köhler*, UWG § 4 Rn. 3.5 - 3.5c m.w.N..

[706] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 812 f.; Köhler/Bornkamm/*Köhler*, UWG, § 3 Rn. 150**;** zur Funktion der Generalklausel des § 3 UWG siehe Götting/Nordemann/*Wirtz*, UWG, § 3 Rn. 37 ff.

[707] *Hilty/Henning-Bodewig*, Leistungsschutzrecht für Sportveranstalter?, S. 76; *Peukert,* Güterzuordnung als Rechtsprinzip, S. 813.

[708] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 813.

tungsschutz zu gewähren. Es handelt sich dabei um eine eng begrenzte Gewährleistung von Grundvoraussetzungen für Wettbewerb. Von diesen Merkmalen trifft auf den Vorgang der Datengenerierung lediglich das zweitgenannte zu. Daten sind ohne größeren Aufwand vervielfältigbar. Ob die Generierung und Bearbeitung von maschinell generierten Daten wesentliche Investitionen voraussetzt, mag schon bezweifelt werden. Ungeachtet der bestehenden faktischen Möglichkeiten, den Zugriff auf generierte Daten zu verhindern, lässt sich die Gefahr eines Marktversagens in der Gestalt, dass ein potentieller Wettbewerb verhindert wird, jedenfalls derzeit nicht feststellen.

3. Ergebnis

Nach geltender Rechtslage lässt sich ein Ausschließlichkeitsrecht an maschinengenerierten Daten nicht begründen. Leistungsschutz wird im Wesentlichen durch das Wettbewerbsrecht gewährt, das das Bestehen einer Wettbewerbshandlung voraussetzt und in seiner Anwendung von den Umständen des Einzelfalls geprägt ist.

D. Überlegungen de lege ferenda

Will man ein neues Leistungsschutzrecht an maschinengenerierten Daten schaffen, ist zunächst der gesetzgeberische Handlungsspielraum auszuloten. Er wird durch das Recht der Europäischen Union und das Verfassungsrecht begrenzt. Im Folgenden soll geklärt werden, ob der deutsche Gesetzgeber die Kompetenz zur Schaffung neuer Ausschließlichkeitsrechte an maschinell generierten Daten besitzt (unten I.) sowie ob die Schaffung neuer Leistungsschutzrechte an diesen Daten verfassungsrechtlich geboten ist und gerechtfertigt werden kann (unten II.). Naturgemäß ist eine valide Einschätzung eines gesetzgeberischen Handlungsbedarfs für einen stark von ökonomischen Gesichtspunkten durchdrungenen Rechtsbereich in einem juristischen Gutachten, das die Erkenntnisse aus der Ökonomie, der Soziologie oder der Politikwissenschaften allenfalls kursorisch einbeziehen kann, nur eingeschränkt möglich. Insbesondere erweisen sich Aus- und Vorhersagen zu einem etwaigen Marktversagen auf dem Datenmarkt aus der Perspektive einer Landesjustizverwaltung mit ihrem eigenen Erfahrungshorizont als problematisch. Hier gilt es, unter Hinzuziehung des Sachverstands anderer Ressorts zur Wahrung von Länderinteressen den zuvörderst auf europäischer Ebene einsetzenden Rechtssetzungsprozess zu begleiten.

I. Kompetenz des deutschen Gesetzgebers zur Schaffung neuer Leistungsschutzrechte an maschinell generierten Daten

1. Keine Sperrwirkung durch Regelungen des Europäischen Primärrechts

Die Europäische Union hat eine eigene Kompetenz im Hinblick auf das geistige Eigentum. Diese Kompetenz könnte von Bedeutung werden, wenn ein neues Leistungsschutzrecht an maschinell generierten Daten in Anlehnung an die verwandten Schutzrechte im Sinne des Urheberrechts ausgestaltet werden würde und damit im weitverstandenen Sinne ein geistiges Eigentumsrecht darstellen könnte. Während es für das Gebiet des geistigen Eigentums vor Inkrafttreten des Vertrages von Lissabon nur eine allgemeine Unionskompetenz zur Harmonisierung verschiedener nationaler Rechte gab (Art. 95 EGV alt = Art. 114 AEUV), wurde mit dem Vertrag von Lissabon in Art. 118 AEUV eine eigene Rechtssetzungskompetenz der Europäischen Union zum Erlass von europäischen Rechtstiteln zum Schutz des geistigen Eigentums und zur Errichtung zentralisierter Zulassungs-, Koordinierungs- und Kontrollregelungen auf Unionsebene erlassen. Der Begriff des „geistigen Eigentums" in Art. 118 AEUV ist weit zu verstehen und umfasst neben den klassischen gewerblichen Schutzrechten (Patent, Marke, Designschutz/Geschmacksmuster, Gebrauchsmuster) das Urheberrecht und die Leistungsschutzrechte, die *sui generis*-Schutzrechte für Datenbanken, Halbleiterschutz, Sortenschutzrechte sowie nach Auffassung der Kommission auch geographische Herkunftsbezeichnungen und Handelsnamen.[709] Aufgrund der Zielsetzung der Binnenmarktverwirklichung gehört die durch Art. 118 AEUV übertragene Zuständigkeit zu einem Bereich der geteilten Zuständigkeiten im Sinne von Art. 4 Abs. 2 lit. a AEUV.[710] Sowohl die Union als auch die Mitgliedstaaten können im Bereich des geistigen Eigentums Regelungen erlassen. Soweit die Union auf diesem Gebiet tätig wird, entfaltet diese Regelung eine Sperrwirkung.[711] Die Union kann wahlweise europäische Rechtstitel schaffen, welche nationale Schutzrechte verdrängen sollen oder nicht verdrängen sollen.[712] Wenn

---

[709] Schwarze/Becker/Hatje/Schoo/H*olzmüller*, EU-Kommentar, Art. 118 AEUV Rn. 10; Calliess/Ruffert/ *Wichard*, EUV/AEUV, Art. 118 Rn. 2.; Grabitz/Hilf/Nettesheim/*Stieper* Das Recht der Europäischen Union, Art. 118 Rn. 28.

[710] Vgl. etwa EuGH (Große Kammer), Urt. v. 16.4.2013 – C-274/11, C-295/11 (Spanien und Italien/Rat der Europäischen Union), NJW 2013, 2009; Streinz/*Bings*, EUV/AEUV, Art. 118 AEUV Rn. 15.

[711] Schwarze/Becker/Hatje/Schoo/*Holzmüller*, EU-Kommentar, Art. 118 AEUV Rn. 14; Grabitz/Hilf/Nettesheim/*Stieper*, Das Recht der Europäischen Union, Art. 118 Rn. 28.

[712] Schwarze/Becker/Hatje/Schoo/*Holzmüller*, EU-Kommentar, Art. 118 AEUV Rn. 16-18; Groeben/Schwarze/*Pipkorn/Bardenhewer-Rating/Taschner*, EUV/EGV, Art. 95 Rn. 40. Vgl. auch schon EuGH, Urt. v. 13.7.1995 – Rs. C-350/92 („ergänzendes Schutzzertifikat"), GRUR Int 1995, 906 Rn. 23: „Der Gerichtshof hat im übrigen im Gutachten 1/94 vom 15.11.1994 (Slg. 1994, I-5267, Rn. 59 = GRUR Int. 1995, 248) bekräftigt, dass die Gemeinschaft auf der Ebene der internen Rechtsetzung im Bereich des geistigen Eigentums über eine Zuständigkeit zur Harmonisierung der nationalen Rechtsvorschriften gemäß den Art. 100 und 100a verfügt und auf der Grundlage von Art. 235 neue Titel schaffen kann ..."; Rn. 27: „Art. 235 kann zwar zur Schaffung neuer Titel verwendet werden, die dann die nationalen Titel überlagern

die Union allerdings einen europäischen Rechtstitel schafft, der nationale Schutzrechte verdrängen soll, ist dieser Rechtsakt noch immer mit Blick auf den Subsidiaritätsgrundsatz aus Art. 5 Abs. 3 EUV zu überprüfen.[713]

Weiterhin muss die Zulässigkeit einer etwaigen deutschen Regelung am Maßstab der unionsrechtlichen Grundfreiheiten überprüft werden. Als Konsequenz aus den Verpflichtungen, die ihnen aus den Bestimmungen des AEUV über die Grundfreiheiten sowie aus dem einschlägigen Sekundärrecht erwachsen, müssen sich die Mitgliedstaaten bei allen Maßnahmen, die sich auf den Datenverkehr auswirken, vom „Grundsatz des freien Datenverkehrs in der Europäischen Union“ leiten lassen, wie er in zahlreichen Legislativakten der Union seinen Niederschlag gefunden hat. Beschränkungen des freien Datenverkehrs durch nationale Ausschließlichkeitsrechte dürften nach dem Grundgedanken des Art. 36 AEUV gerechtfertigt sein. Demnach sind Beschränkungen zulässig, die zum Schutz des gewerblichen und kommerziellen Eigentums gerechtfertigt sind. Soweit durch den Leistungsschutz die Verhinderung unlauteren Wettbewerbs bezweckt ist, lässt sich die Einführung eines neuen Leistungsschutzrechts jedenfalls durch ein zwingendes Erfordernis im Sinne der Cassis-Rechtsprechung[714] - die Lauterkeit des Handelsverkehrs - stützen.

2. Keine Sperrwirkung durch EU-Sekundärrecht

Sofern und soweit der Unionsgesetzgeber von einer (konkurrierenden) Kompetenz positiv Gebrauch macht, tritt eine Sperrwirkung des Unionsrechts zulasten der Regelungsbefugnisse der Mitgliedstaaten ein. Art. 2 Abs. 2 Satz 2 AEUV bestimmt: „Die Mitgliedstaaten nehmen ihre Zuständigkeit wahr, sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat“. Hierbei ist allerdings zu differenzieren. Die Mitgliedstaaten können über eine europarechtliche Mindestnorm hinausgehende Regelungen treffen.[715] Eine Unterschreitung dieses

---

(siehe oben, Rn. 23)“. Eine Mindermeinung betont, dass Art. 118 AEUV zwar zur Schaffung neuer europäischer Rechtstitel ermächtige, nicht aber so weit gehe, dass diese europäischen Titel auch nationale Schutzrechte verdränge, vgl. Lenz/Borchardt/*Fischer*, EU-Verträge, Art. 118 AEUV Rn. 2. Dieser Mindermeinung ist nicht zu folgen. Art. 118 AEUV findet sich systematisch im Abschnitt über Harmonisierung, die auch damit einhergehen kann, dass nationale Regelungen hinter europäischen Vorschriften zurücktreten. Wenn die Union allerdings einen europäischen Rechtstitel schafft, der nationale Schutzrechte verdrängen soll, ist dieser Rechtsakt noch immer auf seine Erforderlichkeit (Subsidiarität) zu überprüfen. Art. 118 AEUV findet sich systematisch im Abschnitt über Harmonisierung, die auch damit einhergehen kann, dass nationale Regelungen hinter europäischen Vorschriften zurücktreten.

[713] Schwarze/Becker/Hatje/Schoo/*Holzmüller*, EU-Kommentar, Art. 118 AEUV Rn. 15; Grabitz/Hilf/Nettesheim/*Stieper*, Das Recht der Europäischen Union, Art. 118 Rn. 20.

[714] Calliess/Ruffert/*Kingreen*, EUV/AEUV, Art. 36 AUEV, Rn. 45 ff.; Grabitz/Hilf/Nettesheim/*Leible/Streinz*, Das Recht der Europäischen Union, Art. 34, Rn. 69 ff.

[715] Calliess/Ruffert/*Calliess*, EUV/AEUV, Art. 2 AEUV Rn. 13.

Mindeststandards wäre hingegen unzulässig. Die Mitgliedstaaten verlieren ihre Zuständigkeit über einen bestimmten Regelungsbereich nur hinsichtlich derjenigen Elemente, die durch den entsprechenden Rechtsakt der Union positiv geregelt werden. Das EU-ZustProt bestimmt hierzu ausdrücklich: „Ist die Union in einem bestimmten Bereich im Sinne des Artikels 2 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union betreffend die geteilte Zuständigkeit tätig geworden, so erstreckt sich die Ausübung der Zuständigkeit nur auf die durch den entsprechenden Rechtsakt der Union geregelten Elemente und nicht auf den gesamten Bereich“. [716] Ein „Schweigen“ der Union führt also grundsätzlich nicht zur Entfaltung einer Sperrwirkung. Eine solche Sperrwirkung kann sich nur ergeben, wenn die Europäische Union ausdrücklich von einer geteilten Kompetenz abschließend Gebrauch machen möchte.

Es lassen sich drei Formen einer Sperrwirkung durch eine europarechtliche Norm unterscheiden[717]: Für die Sperrung eines ganzen Regelungsbereichs (field pre-emption) ist notwendig, dass ein Sekundärrechtsakt seinen Anwendungsbereich erschöpfend geregelt hat, so dass die eigene Rechtssetzung durch die Mitgliedstaaten ausgeschlossen ist. Bei der Sperrung von nationalstaatlichen Hindernissen (obstacle pre-emption) darf das mitgliedstaatliche Recht nicht das ordnungsgemäße Funktionieren oder die Zielvorgaben eines Unionsrechtsaktes behindern. Bei der Sperrung einer einzelnen Norm (rule pre-emption) dürfen die Mitgliedsstaaten keine nationalen Normen erlassen, die einer konkreten Unionsnorm widersprechen, weil die Befolgung beider Normen unmöglich ist.

Die Europäische Union hat bislang zahlreiche Regelungen auf dem Gebiet des geistigen Eigentums getroffen und das Urheberrecht durch sektorspezifische Richtlinien harmonisiert.[718] Allerdings hat die Union von ihrer Regelungskom-

---

[716] Einziger Artikel des Protokolls über die Ausübung der geteilten Zuständigkeiten, ABl. 2008 Nr. 115, S. 307.

[717] Vgl. *Bauerschmidt*, Die Sperrwirkung im Europarecht, EuR 2014, 277(291 ff.).

[718] Zur Frage der Sinnhaftigkeit eines einheitlichen europäischen Urheberrechts vgl. *Fischer*, Perspektiven für ein europäisches Urheberrecht, Baden-Baden 2014. Harmonisiert wurden auch die nationalen Schutzrechte für die Topographie von Halbleitererzeugnissen (RL 87/54/EWG) und für Datenbanken (RL 96/9/EG). Folgende unionsweite Schutzrechte hat die Europäische Union geschaffen: ein unionsweites Markenrecht (VO (EG) 40/94), ein einheitliches europäisches Geschmacksmuster (VO (EG) 6/2002) sowie als „Schutzrecht sui generis“ einen unionsweiten Sortenschutz für Pflanzenzüchtungen (VO (EG) Nr. 2100/94) und einen unionsweiten Schutz der geographischen Herkunftsbezeichnung für Agrarerzeugnisse und Lebensmittel (VO (EG) Nr. 2081/92). Weiterhin gibt es europäische Regelungen zum EU-Patent, die allerdings im Wege der Verstärken Zusammenarbeit (ohne Spanien und Italien) zustande kommen (werden). Die (erforderliche) Ratifikation durch Deutschland pausiert derzeit aufgrund eines Verfahrens vor dem Bundesverfassungsgericht (Az. 2 BvR 739/17). Auf Art. 118 Abs. 1 und Abs. 2 AEUV hat sich die EU insbesondere bei den beiden Verordnungen zur „Umsetzung der Verstärkten Zusammenarbeit im Bereich der Schaffung eines einheitlichen Patentschutzes“ (Verordnung (EU) Nr. 1257/2012) und zur „Umsetzung der verstärk-

petenz auf dem Gebiet des geistigen Eigentums oder der Leistungsschutzrechte nicht in der Weise Gebrauch gemacht, dass die unionsrechtlichen Schutzrechte abschließend wären. Es ist sogar denkbar, dass selbst neben unionsrechtlichen Schutzrechten parallel nationale Schutzrechte bestehen (bleiben).[719]

Indes hat die Union innerhalb des geistigen Eigentums einige Bereiche abschließend geregelt. Hervorzuheben ist das Datenbankherstellerrecht aufgrund der Datenbankrichtlinie 96/9/EG. Hier können die Mitgliedstaaten keine widersprechenden Regelungen zur Datenbankrichtlinie erlassen. Allerdings besteht selbst hier ein gewisser nationaler Spielraum, denn die Mitgliedstaaten könnten Regelungen treffen, die über die europäischen Mindestnormen hinausgehen. Der nationale Gesetzgeber ist auch nicht aufgrund der restriktiven Auslegung der Richtlinie durch den EuGH, der Investitionen der Datengenerierung ausdrücklich aus dem Schutzbereich der Richtlinie herausnimmt[720], gehindert, diese Investitionen durch ein nationales Leistungsschutzrecht zu schützen. Denn es gibt keinen Grundsatz, dass ein ausdrücklich von einem Schutzrecht ausgenommener Gegenstand nicht durch ein anderes Gesetz unter Schutz gestellt werden dürfte.[721]

Die Europäische Union hat durch ihr bloßes Nicht-Tätigwerden auf dem Gebiet der sonstigen Leistungsschutzrechte (Schutzrechte sui generis) aber auch nicht die negative Regelung getroffen, dass es keine weiteren Schutzrechte geben dürfe. Eine solch weitgehende (negative) Regelung wäre mit dem Subsidiaritätsprinzip (Art. 5 Abs. 3 EUV) unvereinbar. Sie würde die Kompetenz der Europäischen Union auf dem Gebiet der Leistungsschutzrechte faktisch zu einer ausschließlichen Kompetenz überhöhen, die ihr Art. 118, Art. 4 Abs. 2 lit. a AEUV gerade nicht verleiht.

Auch mit Blick auf ein Leistungsschutzrecht an Daten hat sich die Europäische Union bislang nicht gesetzgeberisch betätigt. Die Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung betrifft zwar den Schutz vor unredlicher Datennutzung, etabliert indes

---

ten Zusammenarbeit im Bereich der Schaffung eines einheitlichen Patentschutzes im Hinblick auf die anzuwendenden Übersetzungsregelungen“ (Verordnung (EU) Nr. 1260/2012) gestützt. Auf Art. 118 Abs. 1 AEUV hat sich die Union weiterhin bei der Verordnung (EU) 2017/1001 über die Unionsmarke sowie bei der Verordnung (EU) 2015/2424 zur Änderung der Gemeinschaftsmarkenverordnung gestützt.

[719] Vgl. *Hilty/Henning-Bodewig*, Leistungsschutzrecht für Sportveranstalter?, S. 12.

[720] *EuGH*, Urt. v. 9.11.2004, verb. Rs. C-338/02, C-444/02 und C-45/02 - Fixture Marketing; hierzu ausführlich siehe oben unter C. III. 2. b.

[721] *Hilty/Henning-Bodewig*, Leistungsschutzrecht für Sportveranstalter?, S. 21.

gerade kein solches Leistungsschutzrecht an Daten. Im Übrigen hält die Richtlinie in ihrem Art. 1 Abs. 1 S. 2 ausdrücklich fest, dass „die Mitgliedstaaten unter Beachtung der Bestimmungen des AEUV einen weitergehenden als den durch diese Richtlinie vorgeschriebenen Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb, rechtswidriger Nutzung und rechtswidriger Offenlegung vorsehen“ können. Ein solcher weitergehender Schutz wäre etwa die Schaffung eines entsprechenden Schutzrechtes.

Allerdings hat die EU-Kommission im Januar 2017 ein entsprechendes Arbeitspapier in Richtung eines „Datenherstellerrechtes“ / „Datenerzeugerrecht“ / Schutzrechtes an Daten vorgelegt.[722] Die Rede ist von einem “data producer's right for non-personal or anonymised data”. Das Arbeitspapier verweist auch auf die entsprechende Diskussion in Deutschland zu einem Rechtsrahmen für die Datenwirtschaft.[723] Der Vorschlag hat allerdings in erster Linie die Interessenlage im Verhältnis von Maschinenherstellern und den Maschinennutzern (und möglichen Maschineneigentümer) im Blick.[724] Würde die Europäische Union ein solches unionsweites Datenerzeuger- und/oder Datenherstellerrecht einführen, bestünde für nationale Regelungen nur noch dann Spielraum, wenn der entsprechende EU-Rechtsakt den Mitgliedstaaten die Freiheit zur Gesetzgebung zugesteht bzw. wenn die nationalen Regelungen noch über die EU-Regelung hinausgingen.

Damit kann als Zwischenergebnis festgehalten werden, dass der deutsche Gesetzgeber nach derzeitiger Rechtslage an der Schaffung eines Leistungsschutz-

---

[722] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD (2017) 2 final v. 10.1.2017, S. 33; dazu *Wiebe*, Von Datenrechten zu Datenzugang - Ein rechtlicher Rahmen für die europäische Datenwirtschaft, CR 2017, 87.

[723] *Zech*, "Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im Digitalen Binnenmarkt, GRUR 2015, 1151; *Zech*, Information as a tradable commodity, in: De Franceschi (Ed.), European Contract Law and the Digital Single Market, 2016, 51-79; *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: Büscher/Glöckner/Nordemann/Osterrieth/Rengier (Eds.), Marktkommunikation zwischen Geistigem Eigentum und Verbraucherschutz. Festschrift für Karl-Heinz Fezer zum 70. Geburtstag, S. 815; *Dorner*, Big Data und "Dateneigentum", CR 2014, 617; *Spindler*, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805; *Härting*, "Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, 646; *K.-H. Fezer*, Dateneigentum, MMR 2016, S. 3; *Wiebe*, Protection of industrial data – a new property right for the digital economy? GRUR Int. 2016, 877; *Kerber*, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int 2016, 989; *Faust*, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update? Gutachten zum Deutschen Juristentag 2016, NJW Beilage 2/2016, S. 29.

[724] Vgl. ausführlich hierzu *Schweitzer/Peitz*, Discussion Paper No. 17-043 „Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?“, S. 73 ff., abrufbar unter: http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf (letzter Abruf: 21.2.2019).

rechts nicht gehindert wäre. Der europäische Gesetzgeber entfaltet jedoch derzeit Tätigkeiten, an deren Ende der Spielraum für die Mitgliedstaaten, neue nationale Leistungsschutzrechte und Schutzrechte zu schaffen, deutlich eingeschränkt sein könnte. Darüber hinaus ist im Blick zu behalten, dass nationale Leistungsschutzrechte so ausgestaltet sein müssen, dass sie keine Verstöße gegen die Grundfreiheiten begründen.

II. Rechtfertigung für die Schaffung eines neuen Leistungsschutzrechts

Nach dem Verteilungsprinzip des Grundgesetzes wird die Freiheitssphäre des Einzelnen als gegeben und prinzipiell unbegrenzt vorausgesetzt, während jede staatliche Verkürzung dieser Freiheit rechtfertigungsbedürftig ist.[725] Dieses Verteilungsprinzip findet im Grundrecht der „allgemeinen Handlungsfreiheit“ in Art. 2 Abs. 1 Grundgesetz seinen Ausdruck, wonach ein Eingriff in die allgemeine Handlungsfreiheit nur auf der Grundlage eines formell und materiell verfassungsmäßigen Gesetzes gerechtfertigt werden kann, wobei der Eingriff seinerseits verhältnismäßig sein muss.[726] Die Schaffung von Leistungsschutzrechten hätte automatisch zur Folge, dass maschinengenerierte Daten bestimmten Personen zugeordnet und damit dem Zugriff anderer entzogen werden würden. Die hiermit verbundene Einschränkung in bestehende Freiheiten bedarf nach dem eben Gesagten einer Rechtfertigung. Als Vorfrage zu klären ist, ob die Schaffung eines Ausschließlichkeitsrechts an Maschinendaten aus verfassungsrechtlichen Gründen geboten ist, weil diese Daten andernfalls unverhältnismäßig dem Zugriff Dritter ausgesetzt sein würden und der Staat seine Schutzpflichten im Sinne des Untermaßverbotes verletzten würden (unten 1.). Im Anschluss erfolgt eine Bewertung, ob die Schaffung eines Ausschließlichkeitsrechts an maschinengenerierten Daten gerechtfertigt werden kann (unten 2.).

1. Verfassungsrechtliche Eigentumsgarantie

Die Schaffung eines neuen Ausschließlichkeitsrechts an maschinengenerierten Daten lässt sich verfassungsrechtlich aus der Eigentumsgarantie des Grundgesetzes (Art. 14) ableiten. Das Grundgesetz kennt einen weiten Eigentumsbegriff, der über das Sacheigentum hinaus sämtliche Vermögenspositionen erfasst, die die Rechtssubjekte in die Lage versetzen, aus eigener Kraft ihre wirtschaftliche

---

[725] *Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305 (2307); vgl. auch Maunz/Dürig/*Herdegen*, Grundgesetz Kommentar, Art. 1 Abs. 3 Rn. 29.

[726] Maunz/Dürig/*Di Fabio,* Grundgesetz Kommentar, Art. 2 Abs. 1 Rn. 39*;* Erfurter Kommentar zum Arbeitsrecht/*Schmidt*, Art. 2 Rn.13.

Existenz zu behaupten.[727] Hierunter können auch vermögensrechtliche Positionen in Bezug auf maschinell generierte Daten fallen. Der Gesetzgeber ist nicht gehindert, die Zuordnung bislang nicht zugewiesener Güter rechtsschöpferisch zu begründen, um bestimmte Verhaltensweisen ordnungspolitisch anzuregen oder zu ermöglichen.[728]

Ein *Gebot* zur Schaffung eines Leistungsschutzrechts ergibt sich aus Art. 14 Grundgesetz jedoch nicht. Ein solches Gebot folgt insbesondere nicht aus der Institutsgarantie. Diese verbietet dem eigentumsregelnden Gesetzgeber, „solche Sachbereiche der Privatrechtsordnung zu entziehen, die zum elementaren Bestand grundrechtlich geschützter Betätigung im vermögensrechtlichen Bereich" gehören.[729] Die Institutsgarantie sichert demnach einen Grundbestand an Normen, ohne die das Rechtsinstitut seinen Namen nicht verdiente und die den Gesetzgeber als strikt zu beachtendes Untermaßverbot verpflichtet, einen Mindeststandard an freiheitssichernden Vermögensrechten zur Verfügung zu stellen.[730]

Es liegt auf der Hand, dass angesichts der detailliert geregelten und weitreichenden Güterrechtsordnung ohne die Schaffung eines neuen Schutzrechts an Daten eine wesentliche Schmälerung des eigentumsrechtlich geschützten Freiheitsbereichs nicht zu befürchten ist. Dies gilt auch für eine isolierte Betrachtung des Güterschutzes von Daten. Daten sind schon nach derzeitiger Rechtslage dem Zugriff Dritter nicht schutzlos ausgesetzt. Wie bereits an anderer Stelle ausgeführt, finden sich in §§ 202a ff. und 303a StGB Straftatbestände, die Daten unabhängig von einem Speichermedium und von ihrem Inhalt gegen Ausspähung und unbefugte Veränderung schützen. Bei den genannten Straftatbeständen handelt es sich um Schutzgesetze im Sinne von § 823 Abs. 2 BGB, so dass auch zivilrechtliche Ansprüche auf Unterlassung und Schadensersatz im Falle von Verletzungshandlungen bestehen. Ein gesetzgeberischer Handlungsbedarf zum Schutz des „elementaren Bestands grundrechtlich geschützter Betätigung" besteht vor diesem Hintergrund nicht. Die Schaffung eines neuen Leistungsschutzrechts an Daten ist jedenfalls verfassungsrechtlich nicht geboten.

---

[727] v. Mangoldt/Klein/Starck/*Depenheuer/Froese*, Grundgesetz, Art. 14 Rn. 51 ff.; *Schröer,* Der unmittelbare Leistungsschutz, S. 356; Maunz/Dürig/*Papier/Shirvani,* Grundgesetz Kommentar, Art. 14 Rn. 160.

[728] v. Mangoldt/Klein/Starck/*Depenheuer/Froese*, Grundgesetz, Art. 14 Rn. 61; Maunz/Dürig/*Papier/Shirvani,* Grundgesetz Kommentar, Art. 14 Rn. 314.

[729] BVerfG, Urt. v. 18.12.1968 – 1 BvR 638/64 –, BVerfGE 24, 367 (389); BVerfG, Beschl. v. 15.7.1981 – 1 BvL 77/78 –, BVerfGE 58, 300 (339).

[730] v. Mangoldt/Klein/Starck/*Depenheuer/Froese*, Grundgesetz, Art. 14 Rn. 226 f.; Maunz/Dürig/*Papier/Shirvani,* Grundgesetz Kommentar, Art. 14 Rn. 118 ff.

2. Naturrechtliche Gerechtigkeitsüberlegungen und Persönlichkeitsschutz

Angelehnt an die philosophische Arbeitstheorie von *John Locke*, nach der geistige Schöpfungen von Natur aus ihrem Schöpfer zustehen, hat das Reichsgericht in seiner anfänglichen Rechtsprechung erste Leitlinien zum Leistungsschutz formuliert. Kennzeichnend ist die Formel des „mit Kosten und Mühen errungenen Arbeitsergebnisses", dessen Originalhersteller nicht „um die Früchte seiner Arbeit gebracht werden darf".[731] Nach diesem naturrechtlichen Ansatz wird die Freiheit des Menschen als Freiheit an der eigenen Person begriffen, in welchem sich das Recht widerspiegelt, über sich selbst und die eigenen Fähigkeiten frei verfügen zu können.[732] Dieser Ansatz ist in der Vergangenheit auch als Argument herangezogen worden, zur Lösung der sich aus dem technischen Fortschritt ergebenden Probleme die Ausweitung des Urheberrechts zu einem umfassenden Schutzrecht zu legitimieren.[733] Indes besteht heute weitestgehend Einigkeit, dass nicht jede Leistung von einem herrschaftsrechtlichen Schutz erfasst werden kann. Eine solche Annahme stünde nicht im Einklang mit dem oben beschriebenen Verteilungsprinzip des Grundgesetzes, das die allgemeine Handlungsfreiheit in Artikel 2 Abs. 1 gewährleistet und sie gegen unverhältnismäßige Eingriffe des Staates abschirmt und deshalb bei der Zuweisung einzelner Güter konkreter Rechtfertigung bedarf. Es ist auch zweifelhaft, ob dieser Ansatz für Maschinendaten fruchtbar gemacht werden kann, die (ungeachtet eines möglichen personalen Bezugs) nicht das Ergebnis einer schöpferischen Arbeit darstellen.

3. Utilitaristische Rechtfertigungsansätze

Damit sich ein Eingriff in die allgemeine Handlungsfreiheit rechtfertigen lässt, muss das zu schaffende Leistungsschutzrecht zunächst die Erreichung eines dem Allgemeininteresse dienenden Ziels bezwecken.[734] Die sogenannte „Incentive-Theorie" geht davon aus, dass (auch zeitlich befristete) Ausschließlichkeitsrechte einen Anreiz zur geistigen Betätigung und zur Investition in diese schaffen, welche auch nach Ablauf der zeitlichen Befristung positive Wirkungen auf die Schaffung neuer Güter und den Wettbewerb haben. Der Anreizgedanke wurde vor allem für das Patentrecht entwickelt, er kommt aber auch bei nichtgewerblichen Schutzrechten zum Tragen. Dies gilt etwa im deutschen Urheberrecht, in dem die vermögensrechtliche Komponente neben die persönlichkeits-

---

[731] RG, Urt. v. 7.4.1910 – VI 344/09 –, RGZ 73, 294. Eine ausführliche Nachzeichnung der Rechtsprechung liefert *Schröer,* Der unmittelbare Leistungsschutz, S. 11 ff.
[732] *Schröer,* Der unmittelbare Leistungsschutz, S. 353.
[733] Schricker/Loewenheim/*Loewenheim*, Urheberrecht, Einl. Rn. 8 ff.; *Schröer,* Der unmittelbare Leistungsschutz, S. 353 ff.
[734] *Zech,* Information als Schutzgegenstand, S. 152 ff.

rechtliche tritt.[735] Auf der anderen Seite sind mit der Schaffung neuer Leistungsschutzrechte ökonomische Nachteile verbunden. Es besteht die Gefahr einer Überinvestition in immaterielle Güter, wobei Ressourcen für produktive Aktivtäten gebunden werden. Außerdem kann es zu einer ungünstigen Verbreitung bestehender Werke, Erfindungen etc. kommen, weil die Kosten der unveränderten Nutzung und der kreativen Weiterentwicklung bestehenden Wissens erhöht werden.[736] Da Markteingriffe aus volkswirtschaftlicher Perspektive nur notwendig sind, wenn die innovationsfördernde Wirkung des Eingriffs durch die Marktmechanismen nicht erreicht wird, setzt die Schaffung eines neuen Leistungsschutzrechts voraus, dass ohne dessen Schaffung ein Marktversagen droht.[737] Ein Marktversagen ist möglich, wenn im Allgemeininteresse liegende Leistungen unterbleiben, etwa weil Trittbrettfahrer nicht bis zur Amortisation der Investitionskosten an der kostenfreien Übernahme der Leistungsergebnisse ferngehalten werden.[738] Ein Marktversagen ist zudem insoweit möglich, als ein Übermaß an Schutz den Wettbewerb verzerren und neue Innovationen verhindern kann. Diese negativen Effekte verschärfen sich, wenn der Rechtsinhaber aufgrund des Ausschließlichkeitsrechts über erhebliche Marktmacht verfügt.

Bei der Beurteilung eines gesetzgeberischen Handlungsbedarfs müssen die ökonomischen Nachteile (beziehungsweise die Vorteile der Gemeinfreiheit) mit den Vorteilen der Gewährleistung eines Ausschließlichkeitsrechts abgewogen werden. Um ein möglichst optimales Gleichgewicht zu schaffen, werden Ausschließlichkeitsrechte gewährt, aber zugleich wieder begrenzt – etwa durch eine enge Definition des Schutzgegenstandes, eine zeitlich begrenzte Dauer oder Schrankenbestimmungen. Der Gesetzgeber entscheidet in diesem Zusammenhang auch, welche rechtliche Konstruktion zu einer optimalen Ressourcenallokation beiträgt. Eine Entschädigungslösung nach dem Vorbild von §§ 950, 951 BGB kann effizienter erscheinen als Leistungsschutz durch ein zeitlich begrenztes Ausschließlichkeitsrecht.

Gemessen daran ist im Folgenden zu untersuchen, ob die Schaffung eines neuen Leistungsschutzrechts im Allgemeininteresse liegt, weil ohne dieses keine ausreichenden Innovations- und Investitionsanreize hinsichtlich der Erzeugung dieser Daten bestehen (unten a und b.), weil ein Leistungsschutzrecht zur Beseitigung von Hindernissen beim Datenzugang (unten c.) und zur Absenkung von Transaktionskosten (unten d.) beitragen oder bislang fehlende Offenbarungsanreize setzen würde (unten e.).

---

[735] *Zech,* Information als Schutzgegenstand, S. 155.
[736] *Peukert,* Güterzuordnung als Rechtsprinzip, S. 112 f.
[737] *Hilty/Henning-Bodewig,* Leistungsschutzrecht für Sportveranstalter?, S. 75; *Garstka/Coy* in: GS Steinmüller, Wovon - für wen - wozu - Systemdenken wider die Diktatur der Daten, S. 195 (210 f.).
[738] *Hilty/Henning-Bodewig,* Leistungsschutzrecht für Sportveranstalter?, S. 76.

a. Anreiz von Innovationen

Die Schaffung von Immaterialgüterrechten schützt die Anreize zur Innovation.[739] Die Europäische Kommission geht in ihrer Mitteilung „Aufbau einer Datenwirtschaft" unwidersprochen davon aus, dass Daten zu einer unerlässlichen Quelle für das Wirtschaftswachstum, für Innovationen, für die Schaffung von Arbeitsplätzen und den gesellschaftlichen Fortschritt geworden sind.[740] Dieser Anreizgedanke lässt sich auf maschinell generierte Daten nur eingeschränkt übertragen. Unbestreitbar sind Maschinendaten ein wichtiger „Rohstoff", der Unternehmen mit Zugang zu diesem Rohstoff zu verbesserten Produktions- und Vertriebsabläufen und zur Produktentwicklung und -innovation verhelfen kann. Die Datengenerierung für sich genommen stellt jedoch keine Innovation dar. Die Daten fallen zumeist als Nebenprodukt der eigentlichen Zweckverrichtung der jeweiligen Maschine an. Diese ebenso wie die von Sensoren erhobenen Messdaten entfalten ihre „innovative Kraft" erst nach ihrer Analyse, die Zusammenhänge in den Daten aufdeckt und für den Anwendungszweck nutzbar machen kann.

Der Innovationsanreizgedanke könnte allenfalls mittelbar dann zum Tragen kommen, wenn Innovationsdefizite bei der Datenanalyse aufgedeckt würden oder zu befürchten wären, die auf einen Mangel an maschinengenerierten Daten zurückzuführen wären. Indes begegnet auch diese Begründung Bedenken: Die zur Datenanalyse eingesetzten Techniken sind bereits jetzt regelmäßig Gegenstand von Immaterialgüterrechten, insbesondere eines Patents oder eines Urheberrechts an Software. Dass die damit beförderten Innovationen wegen Datenmangels ausbleiben, erscheint vor dem Hintergrund eines immer stärker wachsenden Datenmarktes eher zweifelhaft. Die EU-Kommission geht davon aus, dass sich der Anteil der Datenwirtschaft am Bruttoinlandsprodukt der Europäischen Union von 1,99 % im Jahr 2016 auf 4 % im Jahr 2020 ebenso verdoppeln wie die Anzahl der Datenunternehmen.[741] Diese Zahlen legen nicht nahe, dass ohne die Schaffung eines Ausschließlichkeitsrechts an maschinengenerierten Daten künftig Innovationen spürbar unterblieben.

---

[739] *Schweitzer/Peitz,* Datenmärkte in der Digitalen Wirtschaft, S. 59; *Hilty/Henning-Bodewig,* Leitungsschutzrecht für Sportveranstalter?, S. 74.

[740] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau einer Europäischen Datenwirtschaft", COM(2017) 9 fin., S. 1.

[741] Von 254.850 im Jahr 2016 auf geschätzt 360.000 im Jahr 2020, Nachweise in EU-Kommission, Mitteilung „Aufbau eines gemeinsamen Datenraums", COM(2018) 232 final.

b. Anreiz von Investitionen

Eine weitere Rechtfertigung für die Schaffung eines Leistungsschutzrechts könnte der Gedanke des Investitionsschutzes liefern. Geschützt werden unabhängig vom Vorliegen einer innovativen Leistung die auf die Herstellung eines immateriellen Gutes gerichteten Investitionen. Anwendungsfälle finden sich in § 14 Abs. 2 Nr. 3 MarkenG (Schutz der bekannten Marke), in § 4 Nr. 3 lit. b UWG (Schutz gegen Rufausbeutung) und im Urheberrechtsgesetz (§§ 81, 85 f., 87, 94 f UrhG). Vor diesem Hintergrund wird auch diskutiert, ob und inwieweit das ebenfalls dem Investitionsschutz dienende *sui generis*-Leistungsschutzrecht des Datenbankherstellers nach § 87a ff. UrhG als Vorlage für ein neues Leistungsschutzrecht an Daten herangezogen werden sollte.[742]

Geschützt werden indes nicht die individuellen wirtschaftlichen Belange der jeweiligen Investoren ihrer selbst willen. In einem System freien Wettbewerbs kann es nicht Aufgabe des Gesetzgebers sein, Unternehmern ihr Investitionsrisiko abzunehmen.[743] Dementsprechend wird in den Erwägungsgründen der Datenbankrichtlinie die Bedeutung der Investitionen in Datenbanken für die Entwicklung des Informationsmarktes und für das Allgemeininteresse ausdrücklich hervorgehoben.[744] Es ist daher auch an dieser Stelle zu prüfen, ob die mit dem Investitionsschutz verbundene Güterzuweisung zur Erreichung eines im Allgemeininteresse liegenden Zwecks erforderlich ist und ohne die Güterzuweisung ein Marktversagen droht.[745]

Ein Defizit an Investitionen in die Datengenerierung ist nicht feststellbar. Es fehlen auch Hinweise auf eine Unterversorgung mit Daten. Im Gegenteil ist - wie dargelegt - sogar von einem weiteren Anstieg des Datenvolumens auszugehen.[746] Das augenscheinliche Fehlen eines Anreizdefizits mag daran liegen, dass Maschinendaten in großer Menge als allenfalls wenig kostenintensives „Nebenprodukt“ bestehender Produktionsprozesse abfallen. Zum anderen stehen Datenerzeugern technische und vertragliche Instrumente zur Verfügung, um sich die faktische Zugriffshoheit auf „ihre“ Daten zu erhalten und hierdurch ein Trittbrettfahrerverhalten durch Dritte auszuschließen.[747] Dass ein Ausschließlichkeitsrecht zu vermehrten Investitionen in die Datengenerierung beitragen würde, ist eine vage Hoffnung. Die Evaluierung der Datenbankrichtlinie zeigt, dass die Schaffung neuer Leistungsschutzrechte die hieran geknüpften Erwartungen enttäuschen kann. Das *sui generis*-Leistungsschutzrecht hat jedenfalls nicht zu ei-

---

[742] *Specht*, Ausschließlichkeitsrechte an Daten - Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288 (293).
[743] *Hilty/Henning-Bodewig,* Leistungsschutzrecht für Sportveranstalter?, S. 74 f.
[744] Vgl. nur Erwägungsgründe 7, 8, 9 und 12.
[745] Siehe oben unter C. IV. 2.
[746] Siehe oben unter D. II. 3. a.
[747] *Schweitzer/Peitz,* Datenmärkte in der digitalisierten Wirtschaft, S. 68.

ner volkswirtschaftlichen gewünschten Steigerung der Investitionen in Datenbanken geführt.[748]

c. Anreiz für Datenverkehr: Datenzugang und Datenübertragung

Die Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten könnte dadurch zu rechtfertigen sein, dass sie den Datenzugang erleichtert, damit die Zugänglichkeit der Daten für Dritte erhöht und so die Innovations- und Wettbewerbsfähigkeit von Unternehmen steigert. Nach Auffassung der EU-Kommission ist der Zugang zu und die Übertragung von maschinengenerierten Rohdaten für das Entstehen einer Datenwirtschaft von zentraler Bedeutung.[749] Da derjenige, der die Daten erhoben hat, im Zweifel nicht über ein umfassendes Wissen über alle möglichen nutzbringenden Einsatzmöglichkeiten verfügt, kann es die Wohlfahrt erhöhen, wenn auch Dritte auf die Daten zugreifen können.[750] Zusätzlicher Nutzen kann aus der Zusammenführung oder Verknüpfung verschiedener Datensätze im Lichte spezifischer Anwendungsideen folgen.

Es ist nicht von der Hand zu weisen, dass Dateninhaber von der Datenweitergabe abgehalten werden könnten, weil sie befürchten, dass diese Daten unbefugten Dritten in die Hände fallen. Dieses Risiko lässt sich durch vertragliche Regelungen und den bestehenden Deliktsschutz[751] nur minimieren, jedoch nicht vollends ausschließen. Vertragliche Regelungen greifen nur relativ und bieten keinen Schutz gegen Dritte.

Ob sich diese legitimen Ziele durch die Schaffung eines Ausschließlichkeitsrechts erreichen lassen, ist indes ungewiss. Dies legen auch die Verlautbarungen der Interessenvertreter nahe, die von der EU-Kommission auf der Grundlage ihrer Mitteilung zum „Aufbau einer Datenwirtschaft“ unter anderem zu einem möglichen Leistungsschutzrecht an Maschinendaten befragt worden sind. Die EU-Kommission hat vorgeschlagen, dem Datenerzeuger das Recht zu gewähren, nicht personenbezogene Daten zu nutzen oder anderen deren Nutzung zu gestatten. Dieser Ansatz zielte darauf ab, den ausschließlichen Zugang zu von Maschinen erzeugten Daten aufzuheben. Im Gegenzug war angedacht, für die Inhaber von Daten einen auf bestimmte Grundsätze (wie Fairness, Angemessenheit und Nichtdiskriminierung) gestützten Rahmen zu entwickeln, auf dessen Grundlage sie ihre Daten nach Anonymisierung gegen Entgelt zugänglich machen können. Nach Auffassung der befragten Interessenträger erfüllt der bestehende Rechtsrahmen derzeit seinen Zweck. Rechtsvorschriften, selbst solche, die den

---

[748] EU-Kommission, Zusammenfassung der Bewertung der Richtlinie 96/9/EG über den rechtlichen Schutz von Datenbanken, SWD(2018) 147 fin.
[749] COM(2017) 9 fin., S. 9 und COM(2018) 232 fin., S. 10 f.
[750] *Schweitzer/Peitz,* Datenmärkte in der digitalisierten Wirtschaft, S. 18.
[751] Siehe oben unter C. I. 1.

im Vergleich zu einem Ausschließlichkeitsrecht weniger eingriffsintensiven Zugang zur Datennutzung regeln würden, wurden als verfrüht angesehen.[752] Vielmehr sollten die bestmöglichen Voraussetzungen für die Entwicklung der Datenmärkte geschaffen werden, die maßgeblich auf der Vertragsfreiheit beruhen sollten.[753] Befürwortet werden hingegen nicht legislative Maßnahmen wie die Ausarbeitung von Standardvertragsbedingungen.[754]

Dieser Befund deckt sich weitestgehend mit dem Ergebnis der Stellungnahmen der deutschen Rechtspraxis, wonach die bislang vorherrschenden vertraglichen Regelungen im Bereich der Datenwirtschaft befriedigende Lösungen hervorbringen. Der Deutsche Anwaltsverein hat in seiner Stellungnahme zur Frage des Dateneigentums im November 2016 davor gewarnt, durch vorschnelle gesetzliche Regelungen praxisuntaugliche und interessenwidrige Regelungen herbeizuführen.[755] Ähnlich liegt es mit Äußerungen der Interessenverbände auf Seiten der Wirtschaft.[756] Auch die Monopolkommission sieht in ihrem Sondergutachten zu den Herausforderungen digitaler Märkte keine Veranlassung, den bestehenden Rechtsrahmen grundsätzlich in Frage zu stellen, wenngleich sie eine Vergabe von eindeutigen absoluten Rechten befürwortet, wo immer möglich.[757]

Bestätigt werden die Stellungnahmen der Praxis durch die gesetzgeberische Zurückhaltung. Gesetzliche Regelungen, wie die in Art. 6 Abs. 1 der Verordnung (EG) Nr. 715/2007[758] normierte Pflicht des KFZ-Herstellers, unabhängigen Marktteilnehmern - gegen Gebühr (vgl. Art. 7 der Verordnung) - uneingeschränkten und standardisierten Zugang zu Reparatur- und Wartungsinformationen zu gewähren, sind die Ausnahme. Jedoch vermag auch diese sektorspezifische Regelung nicht Vorbild für ein Leistungsschutzrecht an Daten in anderen Bereichen zu sein, weil sie kein Ausschließlichkeitsrecht normiert, sondern nur den Zugang zu faktisch beherrschten Daten verschafft.

---

[752] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau eines gemeinsamen europäischen Datenraums“ COM(2018) 232 final, S. 11.
[753] COM(2018) 232 final, S. 11.
[754] COM(2018) 232 final, S. 11.
[755] *DAV,* Stellungnahme zur Frage des „Eigentums“ an Daten und Informationen, November 2016, S. 9 f.
[756] Nachweise im Bericht der *Arbeitsgruppe „Digitaler Neustart“*, S. 95 f.
[757] Sondergutachten der Monopolkommission „Herausforderung: digitale Märkte“, BT-Drucks. 18/5080.
[758] Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge.

Schließlich würde ein Ausschließlichkeitsrecht auch nicht zwangsläufig zu einer Erleichterung des Datenverkehrs führen. Der Rechtsverkehr mit Daten lässt sich mit dem bestehenden Rechtsrahmen problemlos abwickeln. Der Vermögenswert der sonstigen Gegenstände kann durch Verkauf gemäß § 433, 453 Abs. 1 2. Alt. BGB realisiert werden. Gegen die Annahme eines Marktversagens beim Datenverkehr spricht die wachsende Zahl an Geschäftsmodellen, in denen Unternehmen auf Datenplattformen industrielle Daten gemeinsam nutzen.[759]

Somit kann festgehalten werden: Grundsätzlich ist die Erleichterung des Datenverkehrs ein legitimes, dem Allgemeinwohl dienendes Ziel. Es erscheint allerdings fraglich, ob die Schaffung eines Leistungsschutzrechts an maschinengenerierten Daten diesem Ziel dient oder nicht vielmehr die Gefahr der Überregulierung in sich birgt und bestehende faktische Monopolstellungen rechtlich noch verstärkt. Im Interesse eines freien Datenverkehrs erscheint die Etablierung von Zugangsregelungen vorzugswürdig. Monopolisierungstendenzen kann bereits nach geltender Rechtslage durch das Kartellrecht entgegengewirkt werden. Denn der ausschließliche Zugriff eines Unternehmens auf Daten kann Grundlage von Marktmacht sein. Dass der exklusive Zugriff auf Daten ein relevanter Faktor bei der Ermittlung einer marktbeherrschenden Stellung sein kann, ist in § 18 Abs. 3a Ziff. 4 GWB ausdrücklich anerkannt, wonach bei der Bewertung der Marktstellung eines Unternehmens dessen Zugang zu wettbewerbsrelevanten Daten zu berücksichtigen ist. Unter diesem Aspekt kann die Weigerung, anderen Unternehmen Zugriff auf die Daten einzuräumen, unter engen Voraussetzungen einen Verstoß gegen § 19 Abs. 1 GWB darstellen, ebenso die Diskriminierung zwischen Nachfragern in der Ermöglichung des Datenzugriffs. Die Pflicht, anderen Unternehmen Zugriff auf bestimmte Daten zu ermöglichen, kann ferner als Abhilfe für einen Marktmachtmissbrauch in Betracht kommen.[760] Konkrete Fallgestaltungen, in denen eine Zugriffsgewährung zwar geboten erscheint, die hohen Anforderungen an einen Kartellverstoß jedoch nicht vorliegen, sind derzeit nicht absehbar. Insoweit sollte jedoch die weitere Entwicklung im Auge behalten werden, um zu beobachten, ob gegebenenfalls durch speziellere Zugangsregelungen lenkend eingegriffen werden muss.

d. Verringerung von Transaktionskosten

Die Schaffung eines Leistungsschutzrechts kann auch dadurch gerechtfertigt sein, dass durch klar definierte Rechte an den Daten die Transaktionskosten re-

---

[759] Zu nennen ist beispielsweise das cloudbasiert arbeitende offene Betriebssystem MindSphere; siehe auch die Initiative der EU-Kommission zur Digitalisierung der europäischen Industrie, COM(2016) 180 fin. In der vom Bundesministerium für Verkehr und digitale Infrastruktur in Auftrag gegebenen Studie „Eigentumsordnung für Mobilitätsdaten“ werden weitere Trends bei datenbasierten Geschäftsmodellen vorgestellt, S. 80 ff.

[760] *Schweitzer/Peitz,* Datenmärkte in der digitalisierten Wirtschaft, S. 79.

duziert und die Effizienz des Handels erhöht werden.[761] Das Ausmaß der Transaktionskostenabsenkung wird allerdings davon abhängen, inwieweit es gelingt, die Ausschließlichkeitsrechte an Daten gesetzlich so zuzuordnen, dass diese Zuordnung der typischen Interessenlage entspricht. Andernfalls muss die Zuordnung später durch Parteivereinbarung korrigiert werden, wofür erneut Transaktionskosten anfallen.[762] Es liegt deshalb näher, die Zuordnung der Daten der Vereinbarung der Vertragspartner zu überlassen, die ihre Interessenlagen selbst kennen. Der Schutz des „schwächeren" Vertragspartners kann durch Zugangsregelungen sichergestellt werden.

e. Offenbarungsanreiz

Eine ökonomische Begründung von Immaterialgüterrechten, die als Registerrecht ausgestaltet sind – insbesondere das Patentrecht –, ist schließlich die Schaffung von Offenbarungsanreizen. Der Patentschutz wird als „Gegenleistung" dafür gewährt, dass der Erfinder seine technische Innovation in einem Patentregister veröffentlicht und somit die entsprechende Information der Öffentlichkeit zugänglich macht.[763] Dieser Zweck ist auf Daten allerdings nur eingeschränkt übertragbar, insbesondere wenn der Wert von Daten in ihrer unmittelbaren Echtzeit-Verfügbarkeit liegt und durch ein öffentliches Register nicht hergestellt werden kann.[764] Des Weiteren bedarf es, anders als bei technischen Erfindungen, des Offenbarungsanreizes bei maschinengenerierten Daten dann nicht, wenn diese Daten - wie dies vielfach der Fall sein wird und wie neue Geschäftsmodelle zeigen[765] - ohne Einbuße eines Wettbewerbsvorsprungs von Dritten verwendet werden können. Denn in der Regel ermöglicht erst die Auswertung der generierten Rohdaten innovative Verbesserungen von Waren und Dienstleistungen. Diese können - je nach Anwendungsidee - für unterschiedlichste Unternehmen wirksam werden, die nicht zwingend in einem Wettbewerb stehen. Dies gilt insbesondere für die Bereitstellung relevanter Daten zum Training von sogenannter künstlicher Intelligenz.[766] Da von datengenerierenden Gegenständen vielfach in kurzer Zeit erhebliche Datenbestände erstellt werden, erscheint die Schaffung eines Registerrechts schließlich wenig praktikabel.[767]

---

[761] *Schweitzer/Peitz,* Datenmärkte in der digitalisierten Wirtschaft, S. 71.
[762] *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft, S. 71.
[763] *Schweitzer/Peitz,* Datenmärkte in der digitalisierten Wirtschaft, S. 70; *Zech,* Information als Schutzgegenstand, S. 155 f.
[764] *Schweitzer/Peitz,* Datenmärkte in der digitalisierten Wirtschaft, S. 70 f.
[765] Hierzu siehe Fn. 759.
[766] COM(2018) 232 fin., S. 11.
[767] In diese Richtung bereits *Arbeitsgruppe „Digitaler Neustart"*, Bericht vom 15. Mai 2017, S. 41.

f. Ergebnis

Ausgehend von dem Verteilungsprinzip des Grundgesetzes, wonach jeder Eingriff in die allgemeine Handlungsfreiheit einer Rechtfertigung bedarf, wurde untersucht, ob die Schaffung eines Leistungsschutzrechts an maschinengenerierten Daten verfassungsrechtlich geboten bzw. gerechtfertigt ist. Die Eigentumsgarantie in Art. 14 Grundgesetz gebietet es nicht, dem Erzeuger, dem faktischen Inhaber oder einem sonstigen an der Datengenerierung, -speicherung oder -verarbeitung Beteiligten ein Ausschließlichkeitsrecht zuzuweisen. Es konnte weiter gezeigt werden, dass die für die Begründung von Leistungsschutzrechten herangezogenen Rechtfertigungsgründe für maschinengenerierte Daten nicht fruchtbar gemacht werden können. Vielmehr bestehen auch in einem System der Gemeinfreiheit ausreichende Innovations- und Investitionsanreize. Belastbare Anhaltspunkte für ein Marktversagen finden sich nicht. Der freie Datenverkehr ist auch ohne die Schaffung eines Leistungsschutzrechts gewährleistet. Es steht im Gegenteil zu befürchten, dass Ausschließlichkeitsrechte an Daten bestehende Monopolstellungen noch verstärkten. Behinderungen des Datenzugangs sollte - wenn nicht die bestehenden kartellrechtlichen Regelungen ausreichend sind - mit Zugangsregelungen begegnet werden. Schließlich tragen Ausschließlichkeitsrechte auch nicht zwingend zur Absenkung von Transaktionskosten bei und der zur Begründung von Registerrechten herangezogene Offenbarungsanreiz greift bei maschinengenerierten Daten nicht und erwiese sich auch als unpraktikabel. Damit überwiegen die mit der Einführung eines Leistungsschutzrechts verbundenen Vorteile, die (derzeit) eine vage Hoffnung sind, die Nachteile der Einschränkungen der allgemeinen Handlungsfreiheit der Wettbewerber nicht. Für die Schaffung von Leistungsschutzrechten an maschinengenerierten Daten besteht deshalb derzeit kein Bedarf.

E. Gesamtergebnis

Das Bürgerliche Recht kennt kein Ausschließlichkeitsrecht an maschinengenerierten Daten. Die gesetzlichen Schuldverhältnisse setzen eine bestehende Rechtezuweisung voraus, ohne sie selbst vorzunehmen. Dem Bürgerlichen Recht lässt sich auch kein Rechtsprinzip entnehmen, das gebietet, ein Leistungsschutzrecht an maschinengenerierten Daten anzuerkennen. Weder in direkter noch in analoger Anwendung treffen die Vorschriften der §§ 950, 951 BGB Aussagen über einen etwaigen Rechtsverlust an Daten durch Speicherung und Verarbeitung oder über eine Entschädigungsregelung. Leistungsschutz im Sinne von Investitionsschutz wird durch § 826 BGB gewährt.

Maschinengenerierte Daten unterliegen als solche auch nicht dem Schutz des Urheberrechts und des *sui-generis*-Leistungsschutzrechts des Datenbankherstel-

lers. De lege lata genießen maschinengenerierte Daten auch keinen unmittelbaren Leistungsschutz nach § 3 UWG. Leistungsschutz kann durch § 4 UWG gegen unlautere Wettbewerbshandlungen gewährt werden.

Die Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten durch den deutschen Gesetzgeber ist (noch) möglich. Der europäische Gesetzgeber entfaltet jedoch derzeit Tätigkeiten, an deren Ende der Spielraum für die Mitgliedstaaten, neue nationale Leistungsschutzrechte zu schaffen, deutlich eingeschränkt sein könnte. Verfassungsrechtlich geboten ist die Schaffung eines neuen Leistungsschutzrechts nicht. Nach dem Verteilungsprinzip des Grundgesetzes ist die Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten wegen der gleichzeitigen Beschränkung der allgemeinen Handlungsfreiheit Dritter rechtfertigungsbedürftig und durch den Grundsatz der Verhältnismäßigkeit begrenzt. Bei der Prüfung eines gesetzgeberischen Handlungsbedarfs wurde untersucht, ob die Schaffung eines neuen Leistungsschutzrechts im Allgemeininteresse liegt, weil ohne dieses keine ausreichenden Innovations- und Investitionsanreize hinsichtlich der Erzeugung dieser Daten bestehen, weil ein Leistungsschutzrecht zur Beseitigung von Hindernissen beim Datenzugang und zur Absenkung von Transaktionskosten beitragen oder bislang fehlende Offenbarungsanreize setzen würde. Es finden sich derzeit keine Belege dafür, dass ohne die Schaffung eines Leistungsschutzrechts an maschinengenerierten Daten künftig Innovationen unterblieben. Eine Unterversorgung mit maschinengenerierten Daten ist ebenfalls nicht feststellbar. Im Interesse eines freien Datenverkehrs, aber auch zur Senkung von Transaktionskosten, erscheint die Etablierung von Zugangsregelungen gegenüber der Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten vorzugswürdig. Zugangsregelungen könnten sektorspezifisch dort vorgesehen werden, wo sich kartellrechtliche Regelungen als nicht (mehr) ausreichend erweisen. Mit der Schaffung eines neuen Leistungsschutzrechts an Daten wären Offenbarungsanreize nur bei gleichzeitiger Ausgestaltung dieses Rechts als Registerrecht verbunden. Die Schaffung eines Registerrechts erscheint hingegen als nicht praktikabel. Somit besteht für die Schaffung eines neuen Leistungsschutzrechts an maschinengenerierten Daten (derzeit) kein Bedarf.

Literaturverzeichnis

Anhalt, Erhard/Dieners, Peter	Medizinprodukterecht, 2. Auflage, München 2017
Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder	Bericht vom 15. Mai 2017
Bergmann, Karl Otto/ Pauge, Burkhard/ Steinmeyer, Heinz-Dietrich	Gesamtes Medizinrecht, 3. Auflage, Baden-Baden 2018
Breidenbach, Stephan/ Glatz, Florian (Hrsg.)	Rechtshandbuch Legal Tech, München 2018
Brünnler, Kai	Blockchain kurz & gut, Heidelberg 2018
Callies, Christian/ Ruffert, Matthias	EUV/AEUV - Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 6. Auflage, München 2016
Dreier, Thomas/ Schulze, Gernot	Urheberrechtsgesetz, 6. Auflage, München 2018
Drescher, Daniel	Blockchain Grundlagen - Eine Einführung in die elementaren Konzepte in 25 Schritten, Frechen 2017
Müller-Glöge, Rudi/ Preis,Ulrich/ Schmidt, Ingrid	Erfurter Kommentar zum Arbeitsrecht, 19. Auflage 2019
Erman	BGB, Kommentar, 15. Auflage, Köln 2017
Fezer, Karl-Heinz/ Büscher, Wolfgang/ Eva Inés Obergfell	Lauterkeitsrecht, Kommentar zum Gesetz gegen den unlauteren Wettbewerb, 3. Auflage, München 2016
Fischer, Oliver	Perspektiven für ein europäisches Ur-

heberrecht, Baden-Baden 2014

Haug, Volker M. — Grundwissen Internetrecht, 3. Auflage, Stuttgart 2016

Haus, Klaus-Ludwig/ Krumm, Carsten/ Quarch, Matthias — Gesamtes Verkehrsrecht, 2. Auflage, Baden-Baden 2017

Heckmann, Dirk/ Schmid, Alexander — Studie Blockchain und Smart Contracts, Recht und Technik im Überblick, Vereinigung der Bayerischen Wirtschaft e.V., Passau, Oktober 2017

Herberger/Martinek/Rüßmann/ Weth/Würdinger (Hrsg.) — jurisPK-BGB Band 1

Hoeren, Thomas (Hrsg.) — Big Data und Recht, München 2014

Hosp, Julian — Blockchain 2.0 einfach erklärt - weit mehr als nur Bitcoin, München 2018

Hoxhaj, Jonela — Quo vadis Medizintechnikhaftung? Arzt-, Krankenhaus- und Herstellerhaftung für den Einsatz von Medizinprodukten, Frankfurt 2000

Ilzhöfer, Volker/ Engels, Rainer — Patent-, Marken- und Urheberrecht 8. Auflage, München 2010

Jauernig — BGB, 17. Auflage 2018

Götting, Horst-Peter/ Nordemann, Axel (Hrsg.) — UWG, Handkommentar, 3. Auflage, Berlin 2016

Grabitz, Eberhard/ Hilf, Meinhard/ Nettesheim, Martin — Das Recht der Europäischen Union, 65. Auflage, München 2018

Groeben von der, Hans/ Schwarze, Jürgen/Hatje, Armin — Europäischen Unionsrecht, 7. Auflage 2015

Hentschel, Peter/König, Peter/ Dauer, Peter — Straßenverkehrsrecht, 45. Auflage, München 2019

Köhler, Helmut/ Bornkamm, Joachim/ Feddersen, Jörn — Gesetz gegen den unlauteren Wettbewerb, Kommentar, 37. Auflage, München 2019

Kullmann, Hans Josef/ Pfister, Bernhard/ Stöhr, Karlheinz/ Spindler, Gerald — Produzentenhaftung, Loseblattwerk mit Aktualisierungen 2018

Larenz, Karl/ Canaris, Claus-Wilhelm — Lehrbuch des Schuldrechts, Band II - Halbband 2, 13. Auflage, München 1994

Lenz, Carl-Otto/ Borchardt, Klaus Dieter — EU-Verträge, 6. Auflage 2012

v. Mangoldt, Hermann/ Klein, Friedrich/ Starck, Christian — Grundgesetz Kommentar, Band 1, Artikel 1 bis 19, 7. Auflage, München 2018

Maunz, Theodor/ Dürig, Günter — Grundgesetz Kommentar, 84. EL August 2018

Meinel, Christoph/ Gayvoronskaya, Tatiana/ Schnjakin, Maxim — Blockchain: Hype oder Innovation Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam, 2018

Morik, Katharina/ Krämer, Walter (Hrsg.) — Daten - wem gehören sie, wer speichert sie, wer darf auf die zugreifen? Nordrhein-Westfälische Akademie der Wissenschaften und der Künste, Leiden, Boston u.a. 2018

Möhring/Nicolini — Urheberrecht, Kommentar, 4. Auflage, München 2018

Münchener Kommentar zum Bürgerlichen Gesetzbuch — Band 1, 8. Auflage, München 2018
Band 6, 7. Auflage, München 2017
Band 7, 7. Auflage, München 2017

Münchener Kommentar zur Zivilprozessordnung	Band 2, 5. Auflage, München 2016
Münchener Kommentar zum StGB	Band 6, Nebenstrafrecht I, 3. Auflage, München 2017
Ohly, Ansgar/Sosnitza, Olaf	UWG, 7. Auflage, München 2016
Oppermann/Stender-Vorwachs	Autonomes Fahren – Rechtsfolgen, Rechtsprobleme, technische Grundlagen, München 2017
Palandt, Otto	Bürgerliches Gesetzbuch, Kommentar, 78. Auflage, München 2019
Peukert, Alexander	Güterzuordnung als Rechtsprinzip, (Jus Privatum 138), Tübingen 2008
Rehbinder, Manfred/ Peukert, Alexander	Urheberrecht und verwandte Schutzrechte, 18. Auflage, München 2018
Rehmann, Wolfgang A.	Arzneimittelgesetz, AMG, Kommentar, 3. Auflage, München 2008
Sassenberg, Thomas/ Faber, Tobias	Rechtshandbuch Industrie 4.0 und Internet of Things - Praxisfragen und Perspektiven der digitalen Zukunft, 2. Auflage, München 2019
Schricker, Gerhard/ Loewenheim, Ulrich	Urheberrecht, Kommentar, 5. Auflage, München 2017
Schröer, Benjamin	Der unmittelbare Leistungsschutz, Tübingen 2010
Spickhoff, Andreas	Medizinrecht, 2. Auflage, München 2014
Steiner, Udo	Fahren ohne Fahrer im Fokus der Rechtswissenschaft, DAR 2017, S. 359
Streinz, Rudolf	EUV/AEUV,

	3. Auflage 2018
Schwarze, Jürgen/ Becker, Ulrich/ Hatje, Armin/ Schoo,Johann (Hrsg.)	EU-Kommentar, 3. Auflage 2012
Schweitzer, Heike/ Peitz, Martin	Datenmärkte in der Digitalen Wirtschaft: Funktionsdefizite und Regelungsbedarf, Dicsussion Paper No. 17-043, Zentrum für Europäische Wirtschaftsforschung GmbH
Spancken, Marius/ Hellenkamp, Mario/ Brown, Christopher/ Thiel, Christian	Kryptowährungen und Smart Contracts, Abschlussbericht zum Forschungs- und Entwicklungsprojekt 2015/2016 im Studiengang Master of Science Wirtschaftsinformatik an der FH Münster
Staudinger, Julius von	Kommentar zum BGB, Buch 2: Recht der Schuldverhältnisse , 1. Auflage, München 2017
Wandtke, Artur-Axel/ Bullinger, Winfried	Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014
Westermann, Harm Peter/ Gursky, Karl-Heinz/ Eickmann, Dieter	Sachenrecht, 7. Auflage, Heidelberg 1998
Zech, Herbert	Information als Schutzgegenstand, Tübingen 2012

Herausgeber:
Ministerium der Justiz
des Landes Nordrhein-Westfalen
Martin-Luther-Platz 40
40212 Düsseldorf

Justiz-ONLINE PRINT
aktuell, kompetent & bürgernah

Druck: JVA Willich I
Titel: panthermedia.net/seewhatmitchsee