Prof. Dr. Jürgen Kühling I RA Florian Sackmann

RECHTE AN DATEN

Regulierungsbedarf aus Sicht des Verbraucherschutzes?

20. November 2018

Rechtsgutachten im Auftrag des

verbraucherzentrale
Bundesverband

Gefördert durch:

Bundesministerium der Justiz und für Verbraucherschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Impressum

Verbraucherzentrale Bundesverband e.V.

Team Digitales und Medien

Markgrafenstraße 66
10969 Berlin

digitales@vzbv.de

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

Abstract

Seit einiger Zeit wird in Deutschland eine Debatte um die Modifikation beziehungsweise Ergänzung des datenschutzrechtlichen Ordnungsrahmens unter dem Schlagwort eines „Dateneigentums“ geführt. Das vorliegende Rechtsgutachten bewertet eine solche mögliche Entwicklung hin zu einem Ausschließlichkeitsrecht an Daten primär aus der Perspektive der Verbraucher. Dabei wird festgestellt, dass die gegenwärtige Rechtsordnung Rechte an Daten nach dem jeweiligen Schutzzweck zuweist. Ein einheitliches Datenrecht kennt die Rechtsordnung nicht. Es würde sich auch nicht in ihre Systematik einfügen. Die Idee einer Dateneigentumsordnung, die in unterschiedlichen Ausprägungen Daten jeweils einem Berechtigten exklusiv die Verfügung darüber zuweisen will, ist daher abzulehnen. Neue Rechte an Daten, die diese einzelnen Akteuren in Form eines Ausschließlichkeitsrechts zuweisen, sind unnötig und – auch wegen der dadurch weiter steigenden Komplexität – kontraproduktiv. Die gegenwärtige Rechtslage ist geeignet, die sich stellenden Probleme zu lösen. Das bedingt jedoch eine konsequente Nutzung der gegebenen Möglichkeiten im exekutiven Vollzug insbesondere durch die Datenschutzaufsichts- und Kartellbehörden. Die Betrachtung der Referenzgebiete Mobilität und Gesundheit verschärft die Einwände gegen einen dateneigentumsrechtlichen Regulierungsansatz. Das Beispiel der Mobilität zeigt die wachsende Bedeutung von Daten auf, ist gleichzeitig aber auch ein Beispiel für einen an sich funktionierenden gegenwärtigen Rechtsrahmen. Bei der Verarbeitung von Gesundheitsdaten zeigt sich umgekehrt, dass ein komplexes und wenig zielführendes Datenschutzrechtsregime besteht, das sich durch die Einführung von Ausschließlichkeitsrechten an Daten weiter verkomplizieren würde.

For some time, there is a discussion in Germany about the modification or rather complementation of the data privacy regime under the slogan of „data ownership“. This legal opinion evaluates the possible further steps towards a data ownership right from a consumer perspective. It is noted that in the current legal system, the rights for data are determined according to the respective protective purpose. A consistent data law does not exist (in Germany) within the legal system and such a legislation could not be embedded into the current system. The idea of a data ownership, which seeks in variant degrees to assign data exclusively to an entitled person, must be rejected. Assigning new rights to data to single actors by the means of exclusive rights are unnecessary and counterproductive, as they also increase the system´s overall complexity. The present legal situation allows for ways to resolve these problems. However, any solution to the current problems requires the resolute use of relevant options by the respective executive organs (especially data protection and competition authorities) in the field. Two reference areas (of data protection law) provide further arguments against a regulatory approach based on data ownership. Mobility as a reference issue highlights the increasing importance of data generally and simultaneously serves as an example for a functioning modern legal framework. On the other hand, the way in which health data is processed highlights the existence of a complex and rather disadvantageous data protection regime, which would become even more complex by introducing new rights to data.

INHALT

I. EINFÜHRUNG

Daten seien die „Rohstoffe des 21. Jahrhunderts“ ist inzwischen eine gängige Formulierung, die auch von Bundeskanzlerin Dr. Angela Merkel verwendet wird.[1] Richtig ist zweifellos, dass Daten inzwischen eine überragende Bedeutung für die wirtschaftliche Wertschöpfung haben. Die Bedeutung von Daten und deren Nutzbarmachung prägen allerdings nicht nur die wirtschaftliche Wertschöpfung, sondern auch das alltägliche Leben der Menschen in Deutschland, Europa und weltweit. Es ist daher selbstverständlich, dass Daten beziehungsweise deren Nutzung auch einer umfangreichen rechtlichen Steuerung unterliegen müssen. Seit den Anfängen automatisierter Datenverarbeitung stellt sich im Spannungsbereich zwischen der Freiheit, Daten zu verarbeiten einerseits, und der Freiheit, nicht von der Verarbeitung eigener Daten betroffen zu sein, andererseits, die Frage nach der Zulässigkeit des Umgangs mit Daten. Das zunächst in Deutschland, genauer gesagt in Hessen,[2] entwickelte Datenschutzrecht adressiert die Fragen dieses Zielkonflikts und findet in dieser Ausprägung zunehmend weltweit Verbreitung.[3] Mit der Anwendbarkeit der Europäischen Datenschutzgrundverordnung (DS-GVO)[4] hat auch ein wichtiger – wenngleich noch nicht endgültiger – Reformprozess mit einem größeren Fokus auf die europäische Harmonisierung seinen vorläufigen Höhepunkt gefunden.[5]

Die Verbreitung des Datenschutzrechts deutscher Prägung ging auch einher mit einer internationalen Harmonisierung, die über die Grenzen Europas weit hinausgeht. So hat jüngst sogar China wesentliche Elemente und Prinzipien des europäischen Datenschutzrechts in seine Rechtsordnung integriert[6] und auch in den USA schreitet mit einem an

---

[1] http://www.faz.net/aktuell/wirtschaft/cebit/vor-der-cebit-merkel-daten-sind-die-rohstoffe-des-21-jahrhunderts-14120493.html, 06.08.2018.

[2] Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 110.

[3] So orientierten sich beispielsweise China und Kalifornien jüngst an den Grundstrukturen der DS-GVO für eigene Reformvorhaben, vgl. *Müller-Peltzer*, Ping 2018, 65; http://www.faz.net/aktuell/wirtschaft/unternehmen/kalifornien-orientiert-sich-an-europas-DS-GVO-15665526.html, 06.08.2018.

[4] Verordnung (EU) 2016/679 des Europäischen Parlaments 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).

[5] Kühling/Sackmann, NVwZ 2018, 681.

[6] Hoffmann, Datenschutz in China, abrufbar unter: http://www.ecovis-beijing.com/ge/blog-g/artikel/datenschutz-china, 06.08.2018

den Prinzipien der DS-GVO orientierten neuen Datenschutzgesetz im Bundesstaat Kalifornien die Entwicklung in diese Richtung.[7]

Seit einiger Zeit wird in Deutschland nun eine Debatte um beziehungsweise Ergänzung dieses datenschutzrechtlichen Ordnungsrahmens unter dem Schlagwort eines „Dateneigentums“ geführt. Ausgangspunkt der gegenwärtigen Diskussion war der Umgang mit den Daten aus vernetzten Fahrzeugen.[8] Insbesondere die deutsche Automobilindustrie sucht nach Wegen, wie sie in einer zunehmend datengetriebenen Mobilität weiterhin wesentliche Teile der Wertschöpfung in eigenen Händen halten kann und nicht etwa zu reinen Zulieferern von Digitalkonzernen degradiert werden. Vor dem Hintergrund der starken deutschen Automobilindustrie bei einer – verglichen mit den USA – wenig entwickelten Datenwirtschaft besteht daran in Deutschland auch ein industriepolitisches Interesse. So verwundert es nicht, dass es inzwischen Überlegungen dahingehend gibt, die Frage der Zuordnung von Daten auch und gerade im Mobilitätsumfeld regulatorisch neu zu ordnen. Das vorliegende Rechtsgutachten soll eine solche mögliche Entwicklung hin zu einem Ausschließlichkeitsrecht an Daten primär aus der Perspektive der Verbraucher bewerten. Die Ergebnisse sollen dazu dienen, die Folgen einer entsprechenden Rechtssetzung einordnen und besonders aus dem Blickwinkel der Verbraucher bewerten zu können.

Dazu sollen zunächst allgemeine Erwägungen zu Ausschließlichkeitsrechten an Daten angestellt (dazu II. 1.) und daran anknüpfend spezifische Auswirkungen und mögliche Probleme aus Verbrauchersicht identifiziert werden (dazu II. 2.). Aufbauend auf diesen Erkenntnissen soll vor dem Hintergrund der Herkunft der Debatte als sektorspezifisches Referenzgebiet der Mobilitätssektor genauer betrachtet (dazu III. 1.) und ferner das Gesundheitswesen als besonders verbrauchersensibles Referenzgebiet flankierend analysiert werden (dazu III. 2.). Abschließend sollen die gefundenen Ergebnisse einer umfassenden Bewertung zugeführt und daraus der Umfang und die nähere Ausgestaltung eines Handlungsbedarfs für die weitere Entwicklung des deutschen und europäischen Rechtssystems identifiziert werden (dazu IV.).

[7] http://www.faz.net/aktuell/wirtschaft/unternehmen/kalifornien-orientiert-sich-an-europas-DS-GVO-15665526.html, 06.08.2018.

[8] Schulzki-Haddouti, Wem nützt ein neues Eigentum an Daten?, abrufbar unter https://www.golem.de/news/datenschutz-wem-nuetzt-ein-neues-eigentum-an-daten-1805-134162.html, 06.08.2018; zu dieser Thematik hat das BMVI auch eine umfassende Studie erstellen lassen, abrufbar unter https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile, 06.08.2018.

II. DATENEIGENTUMSRECHTE AUS VERBRAUCHERSICHT

1. GRUNDSÄTZLICHE ERWÄGUNGEN ZU DATENEIGENTUMSRECHTEN

1.1 Begrifflichkeiten

Die gegenwärtige Diskussion dreht sich um die rechtlichen Rahmenbedingungen der Datenverarbeitung. In diesem Sinne geht es um digitale Informationen, die elektronisch in einem maschinenlesbaren Format auf einem Datenträger gespeichert sind.[9] Man versteht im zivilrechtlichen Sinne darunter nicht die Information selbst, sondern eine die durch Daten vorgegebene Syntax, also die Anordnung.[10] Das Datenschutzrecht hingegen geht eher von einem semantischen Verständnis aus, sodass das Datenschutzrecht auch die mit den Daten transportierten Informationen selbst unter Schutz stellt.[11]

Ein Datenträger ist ein elektronisches Gerät, das der kurz- oder längerfristigen Aufbewahrung der Daten in einem strukturierten Format dient. Derzeit erfolgt die Speicherung größerer Datenmengen im Regelfall auf magnetscheibenbasierten Festplatten (HDD) und in geringerem Umfang auch in elektronischen Speichermedien (SSD/Flash-Speicher). Die Datenträger selbst sind als körperliche Gegenstände gem. den §§ 903 i.V.m. 90 BGB eigentumsfähig. Daten per se sind hingegen keine körperlichen Gegenstände. Ein Eigentum an Daten im klassischen zivilrechtlichen Sinn ist daher nicht möglich. Der in der gegenwärtigen Debatte vielfach gebrauchte Begriff des „Dateneigentums“ ist daher missverständlich. Er umschreibt auch nicht etwa das Eigentum am Datenträger. Vielmehr handelt es sich um einen Sammelbegriff für unterschiedliche Konzepte einer rechtlichen Zuordnung von Daten zu einem Verfügungsberechtigten.[12]

Aus diesem Grund darf der Begriff des Dateneigentums nicht dazu verleiten, die diskutierten Rechte an Daten auch in rechtlicher Hinsicht mit dem Eigentum an Sachen gleichzusetzen. Das Wesensmerkmal digitaler Daten, das diese von anderen Wirtschaftsgütern unterscheidet, ist die Möglichkeit, sie ohne größeren Aufwand und ohne Substanzverlust zu multiplizieren. Das klassische Problem der Güterknappheit, das mit der Zuordnung von Sacheigentum an eine bestimmte Person adressiert wird, stellt sich bei Daten nicht in vergleichbarer Weise. Daher hinkt insoweit auch der Vergleich als „Rohstoff des

[9] Vgl. dazu auch die Definition bei https://www.duden.de/rechtschreibung/Daten, 06.08.2018.

[10] Denga, NJW 2018, 1371.

[11] Vgl. zu den Begrifflichkeiten auch Steinrötter, MMR 2017, 731, 732 m.w.N.

[12] Vgl. Schulz, Dateneigentum in der deutschen Rechtsordnung, PinG 2018, 72.

21. Jahrhunderts“, da es sich jedenfalls um einen mehr oder wenig beliebig vervielfachbaren „Rohstoff“ handelt – anders als die klassischen Rohstoffe wie das oftmals benannte Öl.[13] Auch ist die mit dem Besitz an körperlichen Gegenständen (etwa dem Besitz eines Pkw) verbundene Publizitätswirkung bei Daten losgelöst von ihren jeweiligen Datenträgern nicht in gleicher Weise darstellbar. Mit anderen Worten kann man Daten nicht vergleichbar einfach ansehen, wem sie zuzuordnen sind. Während der Besitz des Pkw eine entsprechende Publizitätswirkung auslöst, ist das für die im Rahmen der Fortbewegung des Pkw in dem Fahrzeug erhobenen Daten nicht vergleichbar der Fall. Insofern ist das Eigentum als Rechtsinstitut grundsätzlich nicht geeignet, konfligierende Interessen am Wirtschaftsgut Daten sachgerecht aufzulösen. Der Begriff eines Eigentums an Daten ist besonders missverständlich. Treffender als der Begriff des Dateneigentums ist daher derjenige eines Datenausschließlichkeitsrechts. Damit wird die Funktion derartiger Rechte besser umschrieben, denn es geht im Kern darum, auch an Daten ein Ausschluss- und Nutzungsrecht zugunsten einzelner Personen zuzulassen und damit die Funktionen des Sacheigentums auf digitale Daten zu übertragen, ohne dass die Rechtsinstitute rechtsdogmatisch gleichzusetzen wären. Insofern liegt den unter dem Stichwort „Dateneigentum“ diskutierten Konzepten ein Verständnis zugrunde, dass vorhandene Informationen nur von einer Person genutzt werden sollten und diese Person über die Nutzung der Informationen durch Dritte verfügen kann, also insbesondere diese auch untersagen kann.

1.2 Ausschließlichkeitsrechte an Daten als hemmendes Verbotsgesetz

Eine allgemeine Freiheit zur Nutzung von Daten besteht gegenwärtig schon auf Grundlage der allgemeinen Handlungsfreiheit in den Grenzen des geltenden Rechts. Inhalt eines „neuen“ Rechts an Daten, das am Eigentum orientiert ist, könnte demnach nur eine Ausschlussfunktion sein, die Einzelnen das exklusive Nutzungsrecht an bestimmten Daten zuweist. Ein eigentumsähnliches Recht an Daten wäre im Kern also nicht ein Recht zur Datenverarbeitung für Einzelne, sondern ein Verbot der Datenverarbeitung für Dritte.

Schon die Grundidee eines Ausschluss- und Nutzungsrechts an Informationen ist vor diesem Hintergrund abzulehnen. Gelöst würde dadurch allenfalls ein scheinbarer Konflikt, der mangels Güterknappheit bei Daten jedoch schon im Ausgangspunkt nicht existiert. Das Problem, das vielmehr durch das Rechtssystem adressiert werden sollte, ist wettbewerblicher Natur. Durch den exklusiven faktischen Zugriff auf Daten, der beispielsweise auf dem Eigentum am Datenträger oder – praktisch relevanter – auf der Hoheit

[13] So auch das Max Planck Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“ – 10 Fragen und Antworten, S. 1, abrufbar unter https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf, 06.08.2018.

über die Gestaltung von Schnittstellen zur Interoperabilität datenverarbeitender Systeme besteht, kann heute schon faktisch eine Hoheit über Daten bestehen.

Ein Regelungsbedarf besteht also allenfalls bezogen auf die Frage, wie Datenmärkte sinnvoll am Gemeinwohl orientiert reguliert zugeführt werden, damit auch volkswirtschaftlich betrachtet größtmögliche wirtschaftliche Wertschöpfung aus der Datennutzung erfolgt. Der Schlüssel zu einem zweckmäßigen Regulierungsregime sind dabei nicht *Verbote der Datenverarbeitung* wie bei eigentumsorientierten Rechten an Daten, sondern *Zugangsrechte zu Daten.* Diese können gegebenenfalls bestehende Probleme der monopolisierten Hoheit an Daten und daraus folgende verzerrte Verteilungsergebnisse in Bezug auf die Wertschöpfung effektiv bekämpfen.

Denn die Diskussion um ein „neues Recht an Daten“ darf nicht den Blick darauf verdecken, dass auch nach aktueller Rechtslage der Zugriff auf Daten sich nicht gleichsam in einem rechtsfreien Raum bewegt. Vielfach gibt es rechtliche Implikationen des Zugriffs auf Daten und deren Verarbeitung.

Die Rechtsordnung ist allerdings nicht sachbezogen, sondern zweckbezogen strukturiert. Das bedeutet, dass die Rechtsbeziehungen zwischen Rechtssubjekten im Mittelpunkt stehen und nicht um einzelne Kategorien von Rechtsobjekten herum ausgestaltet werden und jedes denkbare Verhalten in Bezug auf diese in einem Regelungskontext zusammengefasst ist. Insofern entspricht es der Struktur der Rechtsordnung, dass es einheitliche Regelungen für die Rechtsobjekte „Daten“ ebenso wenig gibt wie beispielsweise für die Rechtsobjekte „Sachen“. Vielmehr werden durch Rechtsnormen menschliche Verhaltensweisen adressiert, die im Grundsatz erlaubt (Art. 2 Abs. 1 GG) und ausnahmsweise untersagt werden. Ein überzeugendes Regulierungsregime im Hinblick auf Daten kann daher kaum in einem horizontal wirkenden Datengesetz gesucht werden, denn Daten haben eine gesellschaftliche und ökonomische Breitenwirkung wie kaum ein anderes Gut. Es entstünde so fast unweigerlich eine Parallelstruktur zu bestehenden Normsystemen mit erheblichen Friktionsflächen zu anderen Regelungsgebieten. Die Folge wäre eine höhere Regelungskomplexität und damit einhergehend eine geringere Rechtssicherheit. Denn auch die gegenwärtigen rechtlichen Vorgaben für die Datenverarbeitung erfolgen sektoral und schutzzweckorientiert. Sie passen sich dabei in den verhaltensbezogenen Regelungsansatz der Rechtsordnung ein. Lösungen, die sich in dieses gewachsene Regelungsregime einfügen, versprechen den größeren Nutzen durch hohe Rechtssicherheit und große Akzeptanz. Die Zweckmäßigkeit eines horizontalen Regelungsbedarfs ist deshalb nicht nur nicht erkennbar, eine sehr weitreichende Neustrukturierung wäre sogar kontraproduktiv, denn sie würde die Komplexität im Regelungsgefüge weiter steigern.

KEINE NOTWENDIGKEIT FÜR EIN DATENEIGENTUMSRECHT

Im Vergleich zu Sachen sind Daten kein knappes Gut. Sie müssen und dürfen somit nicht wie Sachen behandelt werden, von denen sie sich wesensmäßig unterscheiden. Ein Dateneigentum ist deshalb zu einfach gedacht. Ein Regelungsinteresse besteht allenfalls punktuell dahingehend, dass der Zugang zu Daten, hinsichtlich derer bereits faktisch Einzelne die Hoheit ausüben, im Interesse größtmöglicher Gesamtwertschöpfung und/oder Gemeinwohlbelangen, sichergestellt wird. Eine weitreichende Ergänzung der rechtlichen Rahmenbedingungen würde sich hingegen nicht in das aktuelle Regelungssystem im Datenrecht einfügen und würde nur unnötig die Komplexität und Rechtsunsicherheit weiter erhöhen.

1.3 Bedeutung des Personenbezugs

Daten unterliegen bereits nach gegenwärtiger Rechtslage weitgehenden rechtlichen Rahmenbedingungen. An erster Stelle zu nennen ist dabei das Datenschutzrecht und damit zentral die erst seit dem 25. Mai 2018 anwendbare DS-GVO. Deren sachlicher Anwendungsbereich (Art. 2 DS-GVO) bezieht sich ganz wesentlich auf den Begriff der personenbezogenen Daten. Dabei handelt es sich nach der Legaldefinition des Art. 4 Nr. 1 DS-GVO um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Innerhalb ihres Anwendungsbereichs geht die DS-GVO jeglichem nationalen Recht vor (sogenannter Anwendungsvorrang des Unionsrechts). Sofern auf nationaler Ebene ein besonderes Recht an Daten geschaffen werden sollte, so müsste es also mit den Vorgaben der DS-GVO kompatibel ausgestaltet werden. Die DS-GVO enthält zwar zahlreiche fakultative beziehungsweise obligatorische Öffnungsklauseln,[14] also Regelungsspielräume und Regelungsaufträge, allerdings würde ein umfassendes neues Recht an Daten zwangsläufig mit den Grundlagen der DS-GVO konfligieren, soweit diese anwendbar ist. Um das zu verhindern, müsste ein Recht an Daten, das auf nationaler Ebene etabliert werden würde, die datenschutzrechtlichen Anforderungen vollständig unberührt lassen, oder aber nur für nicht-personenbezogene Daten anwendbar sein.

Dabei würde die erste zentrale Herausforderung darin bestehen, trennscharf zwischen personenbezogenen und nicht-personenbezogenen Daten zu unterscheiden. Die schon unter dem Regime der RL 95/46/EG und dem BDSG sehr umstrittene[15] Frage, ob der

[14] Vgl. dazu im Überblick Kühling/Martini, EuZW 2016, 448 und ausführlich Kühling/Martini et. al., Die Datenschutzgrundverordnung und das nationale Recht, abrufbar unter: https://fah.nrw.de/sites/default/files/asset/document/kuehling_martini_et_al_die_DS-GVO_und_das_nationale_recht_2016.pdf, 06.08.2018.

[15] Vgl. nur etwa zum BDSG a.F. Gola/Klug/Körffer in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3, Rn. 10 m.w.N.

Personenbezug absolut oder relativ zu verstehen ist, wurde auch in der DS-GVO nicht klar beantwortet. Dabei geht es um die Frage, ob bei der Identifizierbarkeit von Personen nur die Mittel und das Wissen des Verantwortlichen (relativer Ansatz) oder auch das Wissen und die Mittel beliebiger Dritter einzubeziehen sind (absoluter Ansatz).[16] Diese Frage ist zentral für eine Abgrenzung zweier nebeneinanderstehender Regelungsregime. Solange auf europäischer Ebene aber noch derartige Unklarheiten in der Abgrenzung bestehen, würde ein weiteres paralleles Regelungsregime für nicht-personenbezogene Daten für erhebliche Rechtsunsicherheit sorgen.

Noch zur Richtlinie 95/46/EG hat der EuGH zu dieser Frage ein erstes Urteil gefällt und dabei einen vermittelnden Ansatz verfolgt, allerdings spezifisch bezogen auf die Frage der Identifizierbarkeit bei dynamischen IP-Adressen.[17] Dabei wird im Grundsatz von einem relativen Personenbezug ausgegangen. Das ist auch überzeugend, da es bei strenger Anwendung eines absoluten Ansatzes letztlich kaum mehr nicht-personenbezogene Daten geben würde. Wissen und Mittel Dritter rechnet der EuGH allerdings dann zu, wenn der Verantwortliche über rechtliche Mittel verfügt, um von dem Dritten Auskunft zu erlangen. Offen ist, inwieweit man sich – nicht nur spezifisch bei dynamischen IP-Adressen – auf das Vorhandensein von rechtlichen Mitteln beschränken darf. Das Datenschutzrecht muss die Verbraucher als betroffene Personen umfassend vor der Verletzung ihrer Privatsphäre schützen. Der Anwendungsbereich des Datenschutzrechts muss daher tendenziell weit gefasst werden.

Das entscheidende Kriterium für die Abgrenzung von personenbezogenen und nicht-personenbezogenen Daten ist daher in teleologischer Hinsicht das vorhandene Risiko für die Beeinträchtigung der Privatsphäre der potenziell betroffenen Person. Dieser risikobasierte Ansatz äußert sich insbesondere in Erwägungsgrund 26 der DS-GVO: „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 direkt oder indirekt zu identifizieren.“ Personenbezogene Daten liegen also stets dann vor, wenn das nicht völlig zu vernachlässigende Risiko besteht, dass ein Verantwortlicher oder ein Dritter die Daten der betroffenen Person zuordnen kann. Dieser im Ausganspunkt relative, aber um die risikobasierte Zurechnung des Wissens Dritter ergänzte Ansatz bietet einen interessengerechten Ausgleich zwischen betroffenen Personen und datenverarbeitenden Stellen.

---

[16] Klar/Kühling in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO, Rn. 26.

[17] EuGH, Urteil vom 19.10.2016, Rs. C-582/14 – *Breyer.*

Ein ernstzunehmendes Risiko für die Privatsphäre der betroffenen Personen ist dabei im Regelfall nur dann anzunehmen, wenn der Verantwortliche im Zeitpunkt der Datenverarbeitung weiß, welcher Dritte über Zusatzwissen verfügt, das für die Identifizierung natürlicher Personen erforderlich ist. Dies hängt aber von den Umständen des Einzelfalls ab. Maßstab muss sein, dass die Interessen der betroffenen Personen nicht ernsthaft gefährdet sind. Diese subjektive Komponente trägt dem Willen des Verordnungsgebers Rechnung, der gemäß Erwägungsgrund 26 eine risikobasierte Prognoseentscheidung vor Augen hatte. Gleichzeitig wird dadurch die Rechtssicherheit entscheidend erhöht. Das ist für die gesellschaftlich wünschenswerte Nutzung der Datenverarbeitung essenziell, denn es besteht andernfalls die Gefahr, dass eine Datenverarbeitung im Zweifel unterlassen wird mit allen negativen Konsequenzen für Verbraucher wie eine möglicherweise verminderte Produktqualität, geringere Angebotsvielfalt oder höhere Preise. Der Verantwortliche kann mit dem hier vertretenen Ansatz bei der Gestaltung seiner Dienste zuverlässig abschätzen, ob die von ihm verarbeiteten Daten personenbezogen sind oder nicht. Umgekehrt besteht für die Verbraucher als betroffene Personen nur dann ein ernsthaftes Risiko, identifiziert zu werden, wenn der Verantwortliche weiß, dass und bei wem die notwendigen Informationen zur Identifizierung vorliegen und auf diese realistischerweise auch Zugriff hat.

PERSONENBEZOGENE UND NICHT-PERSONENBEZOGENE DATEN

Die Trennung von personenbezogenen und nicht-personenbezogenen Daten definiert den Anwendungsbereich des Datenschutzrechts. Eine sachgerechte und rechtssichere Lösung kann auf der Basis eines relativen Ansatzes mit risikobasiert objektiven Elementen gefunden werden. Die Abgrenzung ist gleichwohl mit Unsicherheiten behaftet. Ein Dateneigentumsrecht auf nationaler Ebene, das insoweit sich wohl nur auf nicht-personenbezogene Daten beziehen könnte, ist schon aufgrund der verbleibenden Abgrenzungsschwierigkeiten ein fragliches Unterfangen.

1.4 Verfügungen über Daten de lege lata

Als gegenwärtiges Regelungsregime der Verarbeitung von Daten, das auf den Privatsphärenschutz ausgerichtet ist, greift demnach das Datenschutzrecht. Es regelt das Spannungsfeld zwischen dem verfassungsrechtlichen Schutz des Persönlichkeitsrechts und dem ebenfalls grundrechtlich geschützten Recht zur Nutzung von Daten und steuert damit menschliches Verhalten im Umgang mit personenbezogenen Daten sehr weitgehend vor.

Auch nicht-personenbezogene Daten sind jedoch nicht frei von Restriktionen. Vielmehr setzt die Rechtsordnung an mehreren Stellen einen Berechtigten am Umgang mit bestimmten Daten voraus. Insbesondere ist der in den vergangenen Jahren stark ausgebaute strafrechtliche Schutz von Datenbeständen in §§ 303a, 202a, 202b, 202c, 202d StGB zu nennen. So untersagt § 202a StGB etwa unter bestimmten Umständen, sich unbefugt Zugang zu Daten zu verschaffen, wenn diese nicht für den Verarbeiter bestimmt sind. Hier wird also ein Berechtigter an den Daten vorausgesetzt, der die entsprechende Verfügungsbefugnis über die Daten hat.[18] Ebenfalls unter dem Stichwort „Dateneigentum“ wird in der Zivilrechtswissenschaft vertreten, dass Daten ein sonstiges Recht im Sinne des § 823 Abs. 1 BGB darstellen.[19] Ferner können Daten einem lauterkeitsrechtlichen Schutz als Betriebs- und Geschäftsgeheimnisse unterliegen oder aber urheberrechtlich geschützt sein.[20]

All diese Regelungen bezwecken jedoch den Schutz der Integrität gespeicherter Datenbestände. Sie unterscheiden sich insoweit konzeptionell und in der Schutzrichtung von der Bestrebung zur Schaffung von Ausschließlichkeitsrechten an Daten in Form der Zuweisung von Daten.

Bei den gegenwärtig schon bestehenden Rechten an Daten, die sich primär auf eine faktische Position stützen, die gleichwohl eine rechtliche Absicherung erfährt, stellt sich die Frage, wie der jeweils Berechtigte über diese verfügen kann. Als Berechtigten wird man im Regelfall denjenigen ansehen können, auf dessen Veranlassung die Daten gespeichert werden beziehungsweise der diese Verarbeitung nicht-personenbezogener Daten steuert. Ein anderer Ansatz könnte darin liegen, dass man auf die tatsächliche Beherrschung der datenspeichernden Systeme abstellt, also auf eine dem zivilrechtlichen Besitz (§§ 854 ff. BGB) angenäherte Betrachtungsweise. Im Ergebnis gibt es rein tatsächlich gegenwärtig nur wenig Unsicherheiten, wer im Hinblick auf bestimmte Daten nach dem jeweiligen Rechtsgebiet als Berechtigter anzusehen ist. Eine Kernidee von Ausschließlichkeitsrechten an Daten ist daher die Harmonisierung von Berechtigungszuweisungen, die sich gegenwärtig je nach Regelungsregime (Datenschutzrecht, Zivilrecht, etc.) unterscheiden. Eine solche Differenzierung ist aber auch sinnvoll, denn die Regelungen unterscheiden sich in der Schutzrichtung, die teils auch bereits grundrechtlich vorstrukturiert ist. Eine Einebnung der Zuordnungsregime ist daher wenig zielführend.

---

[18] Kargl in: Kindhäuser/Neumann/Paeffgen, Strafgesetzbuch, 5. Auflage 2017, § 202a, Rn. 7.

[19] Vgl. nur Wagner in: MüKo-BGB, 7. Aufl. 2017, § 823, Rn. 295.

[20] Vgl. dazu Schulz, PinG 2018, 72, 74.

Aus dem rechtlichen Schutz der Daten vor unberechtigtem Zugriff erwächst dem Berechtigten auch ein Recht auf Verfügungen über die Daten. Privatautonom kann dieser entscheiden, ob und gegebenenfalls wem er diese Daten zugänglich macht. Dabei kann auch privatautonom vereinbart werden, zu welchen Bedingungen dies erfolgen soll, in welchem Umfang und gegebenenfalls zu welchen Konditionen. Selbstredend steht es dem Berechtigten frei, für die Zugänglichmachung auch ein Entgelt zu fordern. Ein klassisches Beispiel dafür sind private Wetterdienste, die durch selbst generierte oder zugekaufte Analysedaten von Sensoren Wettervorhersagen generieren. Bei den Wetterdaten als Ergebnis des Verarbeitungsprozesses handelt es sich eindeutig nicht um personenbezogene Daten, sodass datenschutzrechtliche Belange keine Rolle spielen. Die Rohwetterdaten oder aber auch die daraus abgeleiteten Vorhersagen lassen sich selbstredend vermarkten. Das Beispiel zeigt, dass Daten bereits gegenwärtig ein handelbares Gut darstellen. Der Berechtigte kann frei entscheiden, ob beziehungsweise wer Zugang zu seinen Datenbeständen erhalten soll.

DATEN SIND BEREITS EIN HANDELBARES GUT
Der Berechtigte an einem Datenbestand kann über diesen Verfügungen treffen und für die Zugänglichmachung von Dritten ein Entgelt fordern.

Mit der Weitergabe an Dritte endet vielfach jedoch der Schutz von Datenbeständen und beschränkt sich dann auf einen relativen Schutz gegenüber dem Vertragspartner. Dieser hat die vertragliche (Neben-)Pflicht, die Daten nur im vereinbarten Umfang zu nutzen und weiterzugeben. Verletzt der Vertragspartner diese Pflicht, bestehen gegebenenfalls (Schadensersatz-)Ansprüche gegen den Vertragspartner. In den meisten Konstellationen wird der ursprünglich Berechtigte an den Daten aber gegen Dritte, die widerrechtlich Zugang zu den Daten erhalten haben, keine rechtliche Handhabe haben. Etwas anderes kann sich sektorspezifisch aus besonderen Rechten wie dem Urheberrecht oder dem Schutz von Betriebs- und Geschäftsgeheimnissen oder auch dem Datenschutzrecht bei personenbezogenen Daten ergeben. Handelt der Dritte allerdings vorsätzlich und waren die Daten technisch gesichert, kommen Ansprüche nach § 823 Abs. 2 BGB i.V.m. § 202a StGB in Betracht, jedoch abhängig von der Definition des Berechtigten im strafrechtlichen Sinn. Es zeigt sich hier der Charakter der Rechte an Daten als nicht ausschließlich. Allein die faktische Herrschaft über Daten kommt dem aber in den meisten Fällen sehr nahe. Jedenfalls schließen die dazu noch bestehenden Defizite keineswegs Verfügungen über Daten aus oder sind ein wesentliches Hindernis dafür. Ohnehin wäre die

Schutzwirkung eines etwaigen rechtlichen Konstrukts, das sich mehr einem echten Ausschließlichkeitsrecht annähert, in seiner Wirkung begrenzt. Es könnte räumlich nämlich nur im Rahmen der Hoheitsgewalt der Bundesrepublik Deutschland durchgesetzt werden. Sobald die Daten in der Hand von Akteuren außerhalb Deutschlands liegen, ist es ohnehin nicht mehr an der deutschen Rechtsordnung, den weiteren Umgang damit zu regeln und dies ließe sich auch praktisch nicht durchsetzen. Auch nach einer entsprechenden Erweiterung der Ansprüche des ursprünglich Berechtigten an den Daten orientiert an echten Ausschließlichkeitsrechten wäre es nach wie vor erforderlich, anderweitige technische oder rechtliche Sicherungen der Daten vor Weitergabe in Drittstaaten vorzusehen. Insofern passt die Regulierung über relative, also vertragliche Rechtsverhältnisse besser zur Realität als ein absolutes Recht, das – im Gegensatz zu Daten – an der Landesgrenze Halt macht. Ein pauschales Ausschließlichkeitsrecht an Daten würde so vor allem den Blick auf die wirklichen Probleme bei Verfügungen über Daten verstellen.

Diese liegen viel eher bei personenbezogenen Daten. Hier gibt es als zusätzliche Schranke das Datenschutzrecht. Zentral für das Verständnis ist es auch hier wieder, dass nicht strikt von einem zweigeteilten Rechtsregime ausgegangen werden kann (personenbezogene und nicht-personenbezogene Daten), sondern vielmehr in Beziehungen von Rechtssubjekten und der Wechselwirkung unterschiedlicher Schutzzwecke gedacht werden muss. Im Datenschutzrecht selbst gibt es mit der sogar primärrechtlich geschützten (Art. 8 Abs. 2 S. 1 GrCh) Möglichkeit der Einwilligung ein zentrales Instrument für Verfügungen über Daten. Dabei ist es keineswegs so, dass personenbezogene Daten allein einer datenschutzrechtlichen Regulierung unterliegen würden. Die rechtlichen Implikationen in Bezug auf Daten stehen also nicht streng nebeneinander, sondern überlagern sich teils und stehen in Wechselwirkung zueinander.

1.5 Probleme der Anonymisierung von Daten

Die umfangreichen Restriktionen des Datenschutzrechts können für eine ökonomisch sinnvolle Verwertung von Daten hinderlich sein. Soweit das der Fall ist, wird dies durch die Grundrechtsrelevanz des Datenschutzrechts jedoch grundsätzlich gerechtfertigt. Aus personenbezogenen Daten können jedoch nicht-personenbezogene Daten abgeleitet werden, indem man diese anonymisiert. Dabei wird teils problematisiert, dass eine Anonymisierung ohne vorherige Erfassung der Daten gar nicht möglich sei. Insbesondere

Specht[21] hält einen besonderen Zulässigkeitstatbestand für eine kurzfristige Speicherung zum Zwecke der Anonymisierung in Anlehnung an § 44a UrhG für zielführend. Dies erscheint angesichts der erst kürzlich abgeschlossenen umfassenden Datenschutzrechtsreform rechtspolitisch wohl ohnehin nicht zeitnah umsetzbar. Eine Lösung kann und muss daher im gegenwärtigen Recht gesucht werden. Dabei ist bei Aufweichungen der konzeptionellen Unterscheidung zwischen personenbezogenen und anonymisierten, also nicht-mehr-personenbezogenen Daten, Vorsicht angebracht. Solange Daten die Identifizierung eines Verbrauchers als betroffene Person zulassen, besteht latent immer zumindest ein Missbrauchsrisiko. Diesem begegnet das Datenschutzrecht mit geeigneten Mitteln. Daten sollen daher erst dann aus diesem Regulierungsregime entlassen werden, wenn ein Risiko für die Privatsphäre der betroffenen Person nicht mehr besteht, also erst nach entsprechender Anonymisierung.

Dem steht allerdings nicht entgegen, dass Ansätze wie in der bundesverfassungsgerichtlichen Rechtsprechung[22] zur automatisierten Kennzeichenerfassung, die bei einer sehr kurzfristigen Verarbeitung schon keinen Eingriff in das Recht auf informationelle Selbstbestimmung sieht, generalisierend und auch auf europäischer Ebene im Einzelfall zu gerechten Ergebnissen verhelfen können. Dem steht auch nicht der eindeutige Wortlaut des Art. 4 Nr. 2 DS-GVO entgegen.[23] Denn die DS-GVO verfolgt einen streng risikobasierten Ansatz. Soweit Daten nur kurzzeitig technisch erfasst werden und unmittelbar im Anschluss wieder rein maschinell gelöscht oder anonymisiert werden, und nicht ohne Weiteres eine menschliche Zugriffsmöglichkeit auf die Daten besteht, dürften die verarbeiteten Daten für den Verantwortlichen nicht identifizierbar im Sinne des Art. 4 Nr. 1 DS-GVO sein. Denn nach Erwägungsgrund 26 der DS-GVO sollen bei der Frage der Identifizierbarkeit „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren“. Werden personenbezogene Daten nur in einem vollautomatisierten Verfahren erfasst und verarbeitet und allenfalls sehr kurzfristig vorgehalten, ohne dass eine menschliche Interaktion vorgesehen oder ohne technische Modifikation möglich ist, nutzt der Verantwortliche keine technischen Mittel, um eine Person zu identifizieren. Dies erfordert jedoch, dass ein Missbrauch nach technischen Maßstäben weitgehend ausgeschlossen ist, bedingt also ein hohes Maß an technischer Datensicherheit im Verfahren, für das der potenziell Verantwortliche – der ja dann mangels personenbezogener Daten nach der Diktion der DS-GVO eigentlich kein

[21] Specht, GRUR Int. 2017, 1040, 1047.

[22] BVerfG, BVerfG, Urteil des Ersten Senats vom 11. März 2008, 1 BvR 2074/05, Rn. 68.

[23] A.A. Specht, GRUR Int. 2017, 1040, 1047.

Verantwortlicher ist, Art. 4 Nr. 7 DS-GVO – gem. Art. 25 DS-GVO Sorge zu tragen hat. Art. 25 DS-GVO muss aus teleologischen Erwägungen auch für derartige Fälle Anwendung finden. Dies alles ist allerdings einer weiteren Klärung durch die Datenschutzaufsichtsbehörden und letztverbindlich durch den EuGH vorbehalten.

Zugleich bleibt die Anonymisierung jedoch gerade für die Sekundärverwertung von Daten ein wichtiges Instrument. Der Verantwortliche kann vor der Weitergabe an Dritte die Daten anonymisieren und diese als nicht(-mehr)-personenbezogene Daten weitergeben, ohne dass er an die Erfordernisse des Datenschutzrechts gebunden wäre.

Bei dem vorzugswürdigen relativen Verständnis des Personenbezugs ergibt sich im Zusammenspiel mehrerer Akteure auch die Gestaltungsmöglichkeit eines Datentreuhandverhältnisses.[24] Nach dem hier zugrunde gelegten Begriffsverständnis ist ein Datentreuhänder eine Instanz, die abhängig von der Wertung des Personenbezugs als eher relativ oder absolut die für ihn pseudonymen Daten gegenüber Dritten als für diese anonyme Daten weiterreichen kann. Durch eine solche Pseudonymisierungsinstanz, der der Verbraucher vertraut – insbesondere, weil diese kein eigenes Interesse an der wirtschaftlichen Verwertung seiner Daten hat – kann der Personenbezug von Daten verwaltet werden. Diese kann die Daten bei sich pseudonymisieren und sodann zur Verwertung nach Freigabe des Verbrauchers an den gewünschten Datenempfänger weiterreichen. Da der Empfänger nicht über den Bezug zu einer natürlichen Person verfügt, sind nach dem streng relativen Ansatz die Daten für diesen nicht personenbezogen. Nach dem hier erläuterten vermittelnden Ansatz mit ergänzender Risikobetrachtung sind derartige Daten wohl trotzdem personenbezogen. Gleichwohl ist hier ein fehlendes Interesse des Verbrauchers am Unterlassen einer Verarbeitung dieser Daten indiziert, denn das Risiko für seine Privatsphäre ist gering. Derartige Daten dürfen also bei Vorliegen eines hinreichenden sachlich rechtfertigenden Grundes nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO verarbeitet werden. Dennoch gelten die Anforderungen an die Datensicherheit und Einschränkungen beim Drittlandtransfer weiter, sodass dem Restrisiko für den Verbraucher entsprechend Rechnung getragen wird. Derartige Konstruktionen können es dem Verbraucher ermöglichen, über seine Daten zu verfügen, ohne diese unmittelbar an den Empfänger weiterreichen zu müssen. Für die wirtschaftliche Verwertung kann der Empfänger dem Verbraucher ein Entgelt bezahlen, das über den Datentreuhänder ausbezahlt werden kann, denn nur er verfügt in dieser Konstellation über die notwendigen Kontaktdaten des Verbrauchers. Handelt es sich beim Datentreuhänder um verbrauchernahe Akteure,

[24] Kritisch dazu Brockmeyer, ZD 2018, 258.

so bleiben die Verbraucher im Kollektiv Herr über ihre Daten, ohne auf eine wirtschaftliche Verwertung verzichten zu müssen.

Der Begriff des Datentreuhandverhältnisses wird im Gegensatz zu dem hier zugrundeliegenden Verständnis derzeit auch für andere Konstruktionen verwendet, so etwa im Mobilitätsbereich für die Speicherung von KFZ-Daten[25], in Zusammenhang mit Biodatenbanken[26], oder auch bei der Telekom, die in Deutschland über ihre Infrastruktur Microsoft-Cloud-Produkte betreibt und anbietet[27]. Ein Datentreuhänder, der die Daten der Kunden verwaltet, kann seine Funktion dabei nur dann erfüllen, wenn er wirklich neutral und unabhängig ist sowie keinerlei eigene Interessen verfolgt.

Wenig praktikabel zur Kommerzialisierung von Daten erscheint dabei eine umfassende Lösung, wie sie etwa von Autoren vom *Fraunhofer MOEZ* verfolgt wird.[28] Die Verfasser einer Stellungnahme schlagen vor, dass eine zentrale Stelle – nach dem Vorbild der GEMA oder der VG Wort – die die Abwicklung der wirtschaftlichen Verwertung von Daten übernimmt.[29] Neben den Praktikabilitätserwägungen wirft die mit einem solchen Ansatz verbundene Konzentration großer Datenmengen bei einem Akteur grundrechtliche Fragen auf, da damit ein hohes Missbrauchspotenzial verbunden ist.

Derart umfassende und damit langwierige wie auch bürokratische Ansätze werden der Schnelllebigkeit der digitalen Welt kaum gerecht. Datentreuhandverhältnisse scheinen bei allen Möglichkeiten wohl nur in Nischenbereichen Erfolg versprechend, können dort allerdings einen wichtigen Beitrag zur Souveränität des Verbrauchers über die Verwendung „seiner Daten“ bei gleichzeitiger wirtschaftlicher Nutzbarmachung der Daten leisten.

---

[25] Brockmeyer, ZD 2018, 258, 259; https://www.versicherungsmagazin.de/rubriken/branche/daten-aus-dem-auto-versicherer-kaempfen-auf-allen-ebenen-2057839.html, 03.08.2018.

[26] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Datentreuhänderschaft in der Biobank-Forschung, 2009, S. 38 ff., abrufbar unter https://www.datenschutzzentrum.de/uploads/projekte/bdc/1-20090630-datent-reuhaender-biobankenforschung-endbericht.pdf, 03.08.2018.

[27] https://cloud.telekom.de/de/blog/office-365/7-fragen-und-antworten-zur-microsoft-cloud-deutschland, 03.08.2018.

[28] Fraunhofer/HSBD, Die Initiative zu einer deutschen Datentreuhand (DEDATE) als ultima ratio der persönlichen digitalen Datenwirtschaft (PDD), abrufbar unter https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Working_Paper/DEDATE-gesamt.pdf, S. 16, 06.08.2018.

[29] Fraunhofer/HSBD, Die Initiative zu einer deutschen Datentreuhand (DEDATE) als ultima ratio der persönlichen digitalen Datenwirtschaft (PDD), abrufbar unter https://www.imw.fraunhofer.de/content/dam/moez/de/documents/Working_Paper/DEDATE-gesamt.pdf, S. 16, 06.08.2018.

2. BESONDERE PROBLEME VON DATENEIGENTUMSRECHTEN AUS VERBRAUCHERSICHT

Wie sich aus den vorangehenden Ausführungen ergibt, ist das Konzept eines Ausschließlichkeitsrechts an Daten grundsätzlich sehr kritisch zu betrachten. Im Folgenden soll analysiert werden, inwiefern sich aus bereits bestehenden rechtlichen oder tatsächlichen Beschränkungen des Zugangs zu Daten Probleme ergeben und ob sich diese gegebenenfalls durch neu eingeführte Rechte an Daten weiter verstärken würden. Dabei wird der Perspektive der Verbraucher besondere Beachtung geschenkt.

2.1 Probleme durch faktische Ausschließlichkeitsrechte an Daten

Wie oben dargestellt, erfolgt bereits nach gegenwärtiger Rechtslage die Verarbeitung von und der Zugriff auf Daten keinesfalls in einem rechtsfreien Raum. Das Datenschutzrecht, aber auch andere Rechtsregime, ordnen und steuern den Zugang zu und den Umgang mit Daten.

Auch in tatsächlicher Hinsicht hat nicht jedermann Zugang zu allen verfügbaren Daten. So können sich Datenträger physikalisch in der Hand von Personen befinden oder aber der Zugriff über Netzwerke durch entsprechende technische Maßnahmen verhindert werden. Derartige technische Sicherungsmaßnahmen genießen sogar den strafrechtlichen Schutz des § 202a StGB. Insofern hat derjenige, der Datenverarbeitungsanlagen betreibt, den ersten Zugriff auf die dadurch generierten Daten. Diese rechtlich geschützte tatsächliche Herrschaft über neu erzeugte Daten ist im Kern bereits das, was vielfach als Dateneigentumsrecht diskutiert wird. Erzeugte Daten sind zunächst an einen Datenträger gebunden, der sich in der Herrschaftssphäre des Datenerzeugers befindet. Dieser kann sodann entscheiden, ob und gegebenenfalls wem er eine Kopie der Daten überlässt. Insofern ist die Vermarktung von Daten derzeit auf privatautonomer beziehungsweise vertraglicher Basis geregelt.[30]

Durch die Position desjenigen, der den Erstzugriff auf die Daten hat und frei entscheiden kann, wem er diese zugänglich macht, können sich große Datenmengen in der Hand einzelner Akteure bündeln und können so zu einer hohen Daten- und in der Folge auch Marktmacht führen. Dieses Phänomen ist besonders bei Plattformmärkten zu beobachten.[31] Aufgrund der skalierenden Netzwerkeffekte haben hier große Anbieter stets Vorteile vor kleineren Anbietern. So wird beispielsweise in einem sozialen Netzwerk bei der Auswahl des Anbieters durch den Verbraucher stets dasjenige den Vorzug erhalten

[30] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau einer Europäischen Datenwirtschaft vom 10.1.2017, COM(2017) 9 final, S. 11.

[31] Vgl. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.pdf?__blob=publicationFile&v=3, S. 5, 06.08.2018.

(müssen), in dem auch die Mehrzahl der persönlichen Kontakte des Nutzers vertreten sind. Die an sich bestehende Wahlfreiheit für Verbraucher kann so beeinträchtigt werden. Auch innovative Angebote können ihm dadurch vielfach vorenthalten bleiben, wenn die Markteintrittsschranke für neue Akteure aufgrund der Datenkonzentration bei den etablierten Anbietern sehr hoch ist. Diese Gefahr besteht zwar bei Plattformdiensten in besonderem Maße, aber letztlich bei jedem datenbasierten Dienst.[32]

Gerade bei Systemen, die ein Verbraucher einsetzt, muss darüber hinaus noch berücksichtigt werden, dass Modifikationen an Hard- und Software durch den Verbraucher häufig nicht vorgenommen werden können oder dies anderweitig erschwert werden (etwa durch das Androhen des Ausschlusses von Gewährleistungsrechten), auch wenn dieser als Eigentümer oder Besitzer eines Systems oder Gerätes wie beispielsweise eines Smartphones oder Fahrzeugs gem. § 903 S. 1 BGB an sich nach Belieben verfahren können müsste. Rein tatsächlich wird aber kaum ein Standardsystem angepasst, sodass Daten regelmäßig nicht anders genutzt werden können als vom Hersteller des Produktes vorgesehen. Allenfalls vom Hersteller ermöglichte Konfigurationsmöglichkeiten kann der Verbraucher nutzen. Bei zunehmender technischer Komplexität der Geräte wird allerdings auch das schwieriger. Auch Hersteller von beim Verbraucher eingesetzten Geräten haben daher eine starke faktische Position bei der Bestimmung über den Umgang mit Daten.

Das Problem der gegenwärtigen Rechtslage ist also keineswegs der mangelnde Schutz desjenigen, auf den die Datenerzeugung zurückgeht. Dieser ist bereits nach gegenwärtiger Rechtslage und seiner rechtlich abgesicherten tatsächlichen Position gut geschützt. Vielmehr ist die Privatautonomie in Bezug auf die Nutzung von Daten steuerungsbedürftig. Denn zur Freiheit, Daten weitergeben zu können, gehört spiegelbildlich auch die Freiheit, genau dies nicht zu tun. Letztlich besteht durchaus die Gefahr, dass Datenbestände in der Hand des ursprünglichen Datenerzeugers konzentriert werden. In der Folge können Wertschöpfungsmöglichkeiten in Bezug auf diese Daten ungenutzt bleiben. Eine sinnvolle Regulierung des Datenverkehrs darf daher nicht die Abschottung von Daten zugunsten des ursprünglichen Erzeugers verfolgen, sondern muss vielmehr den Zugang zu Datenbeständen Dritter für eine möglichst optimale gesamtwirtschaftliche Wertschöpfung sicherstellen. Geeignetes Instrument dafür sind nicht Ausschließlichkeitsrechte an Daten, sondern Rechte auf Zugang zu Daten. Partiell können sich entsprechende Rechte

[32] Vgl. dazu detailliert Monopolkommission, 68. Sondergutachten, abrufbar unter https://www.monopolkommission.de/images/PDF/SG/SG68/S68_volltext.pdf, 06.08.2018.

auf Zugang zu Daten bereits aus dem Kartellrecht ergeben, wenn der Inhaber eines Datenbestandes ein marktbeherrschendes Unternehmen ist.[33]

Ergänzend hat der einzelne Verbraucher das Recht auf Datenportabilität nach Art. 20 DS-GVO, dem so primär eine wettbewerbspolitische und verbraucherschützende Bedeutung zukommt.[34] Das Recht auf Datenübertragbarkeit hat im Kern zwei Zielrichtungen, eine wettbewerbsrechtliche und eine allgemein-verbraucherschutzrechtliche.[35] Zum einen soll sie den Lock-In-Effekt adressieren und den Wettbewerb auf digitalen Märkten stärken. Um dieses Ziel zu erreichen, müssen allerdings Standards geschaffen werden, welche die Interoperabilität der einzelnen Plattformen und Dienste verbessern. Aus diesem Grund hat Art. 20 DS-GVO eine zweite Zielrichtung, nämlich einen qualifizierten Herausgabeanspruch der betroffenen Person bezüglich ihrer Daten zu schaffen. Indem der Nutzer eines Dienstes die von ihm bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format erhalten kann, erlangt er auch gleichzeitig neue Möglichkeiten, die Daten selbst für seine eigenen Zwecke zu verarbeiten beziehungsweise verarbeiten zu lassen. Aufbauend auf diesem Recht sind neue Angebote und Geschäftsmodelle denkbar, bei denen Verbraucher die erhaltenen Daten von Dritten analysieren lassen können, um sich beispielsweise mithilfe von Vergleichsportalen individualisierte Angebote erstellen zu lassen. Dementsprechend beinhalten „personenbezogene Daten, die die betroffene Person bereitgestellt hat“, nicht nur Daten, die Verbraucher aktiv in ein System eingeben – beispielsweise indem sie ein Formular ausfüllen – sondern auch personenbezogene Daten, die die Verbraucher durch die Nutzung von Angeboten und Diensten im Hintergrund generieren.[36] Einen Zugang zu Daten von Wettbewerbern erfasst Art. 20 DS-GVO hingegen nicht.[37]

Monopolistische Strukturen aufgrund großer Datenmacht Einzelner oder weniger Akteure könnten sich künftig verstärken. Für Verbraucher kann das eine geringere Angebotsauswahl und gegebenenfalls weniger innovative Angebote zur Folge haben. Auch höhere Preise sind eine denkbare Konsequenz. Ein allgemeiner legislativer Handlungs-

[33] Vgl. https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Schriftenreihe_Digitales/Schriftenreihe_Digitales_1.pdf?__blob=publicationFile&v=3, S. 10, 06.08.2018.

[34] Herbst, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 20 DS-GVO, Rn. 4; so auch das Max Planck Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“ – 10 Fragen und Antworten, S. 2, abrufbar unter https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf, 06.08.2018.

[35] Vgl. dazu auch Herbst in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 20 DS-GVO, Rn. 4.

[36] Vgl. dazu auch Herbst in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 20 DS-GVO, Rn. 11.

[37] Louven, NZKart 2018, 217, 219.

bedarf ist dennoch nicht zu erkennen. Nicht auszuschließen ist es jedoch, dass sektorspezifisch und abhängig von der weiteren Entwicklung ein partielles Nachsteuern durch Normierung von Zugangsrechten zu Daten marktbeherrschender Unternehmen notwendig werden könnte.[38] Gegen ein präventives gesetzgeberisches Tätigwerden spricht gegenwärtig die dadurch weiter steigende Komplexität im Regelungssystem. Ein allgemeiner Zugangsanspruch zu Daten von Wettbewerbern würde aufgrund der enormen Breitenwirkung in Folge der horizontalen Bedeutung von Daten zu weit gehen und wäre auch nicht zielführend, da er in einer dynamischen Perspektive Anreize zum Aufbau von Datenbeständen beseitigt. Der Aufbau großer Datenmengen als Kapital muss wirtschaftlich belohnt werden, um Anreize für eine größtmögliche gesamtwirtschaftliche Wertschöpfung zu erreichen. Rechtliche Grenzen sollten erst dort eingezogen werden, wo monopolistische Strukturen weitere Innovationen verhindern oder die starke Stellung im Markt von dem Dateninhaber missbraucht wird. Dafür aber sieht das Kartellrecht geeignete Instrumentarien vor, die bisher noch eher zurückhaltend angewandt wurden. Dabei besteht auch die Möglichkeit der Verknüpfung des kartellrechtlichen Instrumentariums mit der Sicherung datenschutzrechtlicher Standards, wie das jüngste Missbrauchsverfahren des Bundeskartellamts gegen Facebook zeigt.[39] Dabei geht es vor allem um den Missbrauch einer marktbeherrschenden Stellung beziehungsweise den Zugang zu wesentlichen Einrichtungen. Es besteht daher ein Bedürfnis für einen konsequenteren Vollzug der geltenden Regularien, nicht aber für eine neue Gesetzgebung.

DIE INSTRUMENTARIEN DES KARTELLRECHTS REICHEN AUS

Eine über die bestehenden Möglichkeiten des Kartellrechts hinausgehende Regulierung ist gegenwärtig nicht erforderlich. Zielführend ist eine konsequente Nutzung der im bestehenden Rechtsrahmen bereits vorgesehenen Möglichkeiten des Kartellrechts bei marktbeherrschenden Unternehmen, die ihre marktbeherrschende Stellung ihrer Datenmacht verdanken.

2.2 Zusätzliche Probleme durch rechtliche Schranken der Datenverarbeitung

Weitergehende Datenrechte in absoluter Form, wie derzeit diskutiert, würden im Extremfall dem Berechtigten eine dauerhafte Position nicht nur an einem Datenbestand, sondern an der mit den Daten transportierten Information geben und damit zum „Super-IP-

[38] So auch das Max Planck Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“ – 10 Fragen und Antworten, S. 4, abrufbar unter https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf, 06.08.2018; so auch

[39] Vgl. dazu Monopolkommission, Hauptgutachten XII, 2018, Rn. 687 ff., abrufbar unter http://monopolkommission.de/images/HG22/HGXXII_Gesamt.pdf, 06.08.2018.

Right“[40] anwachsen. Ein solches ist abzulehnen. Weder gibt es bei Daten einen Rechtsscheinträger wie den Besitz beim Eigentum, noch kann es sinnvoll ein öffentliches Register wie bei Grundstücken oder Patenten geben. Es ist auch nicht ersichtlich, weshalb gewonnene Informationen dauerhaft einem Datenerzeuger zugeordnet werden sollen. Ein solches Verständnis würde die Informationsgesellschaft nachhaltig lähmen und neue Monopole schaffen. So besteht ein erhebliches Missbrauchspotenzial gerade in Bezug auf Abmahnungen für nicht rechtsberatene Marktakteure. Das aber sind regelmäßig Verbraucher oder aber innovative Startups.

Diese Problematik stellt sich unabhängig von der konkreten Ausgestaltung etwaiger Rechte an Daten für jede Komplexitätssteigerung im Rechtssystem. Große und finanzstarke Unternehmen werden in der Regel in der Lage sein, auch komplexe Regelwerke durch Einholung spezialisierten Rechtsrats in ihren Strukturen abzubilden. Kleine und mittlere Unternehmen und Vereine, vor allem aber Verbraucher, stellt bereits die gegenwärtige komplexe Rechtslage vor erhebliche Probleme. In der Folge könnte die Nutzung einer Datenverarbeitung für eigene Zwecke im Zweifel entweder unterlassen oder aber ohne genaue Rechtskenntnis genutzt werden. Die hierdurch entstehenden Probleme wie die Gefahr von Bußgeldern, Schadensersatzforderungen und wettbewerbsrechtlichen Abmahnungen, müssten dann als Begleiterscheinungen hingenommen werden und könnten die Akzeptanz des Rechtsrahmens in der Breite senken.

Jedes Ausschließlichkeitsrecht an Daten würde mit datenschutzrechtlichen Vorschriften konfligieren, sodass eine Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten vorzunehmen wäre. Dass eine trennscharfe Unterscheidung aber oftmals schwierig ist, wurde oben (unter 1.3.) bereits aufgezeigt. Auch die Weiterentwicklung der Abgrenzungskriterien durch die Rechtsprechung und den Europäischen Datenschutzausschuss kann die grundsätzliche Wertungsentscheidung, die mit der Zuordnung zu einer der beiden Kategorien verbunden ist, nicht verbindlich und katalogartig hinreichend eindeutig strukturieren. Unschärfen im Randbereich sind bei der – durchaus sachgerechten – risikobasierten Anlage der DS-GVO vielmehr unvermeidbar.

Hinzu kommt, dass das datenschutzrechtliche Rechtsregime nach wie vor stark fragmentiert ist. Von einer europaweit vollharmonisierten Rechtslage kann derzeit noch keine Rede sein. Dies ergibt sich aus der Vielzahl an Öffnungsklauseln in der DS-GVO, von denen dann in den einzelnen Mitgliedstaaten auch noch sehr heterogen Gebrauch gemacht wurde. In Deutschland tritt vor allem im öffentlichen Bereich eine weitere Fragmentierung auf Bundes- und Landesebene hinzu. Daneben ist im Datenschutzrecht stets

[40] Vgl. Denga, NJW 2018, 1371.

eine Vielzahl vorrangig geltender bereichsspezifischer Normen zu beachten. Diese dreifache Ausdifferenzierung des Datenschutzrechts in bereichsspezifisches und allgemeines, europäisches und nationales Recht sowie Bundes- und Landesrecht allein sorgt für ein nur noch schwer zu überblickendes Normensystem.[41]

Setzt man neben dieses komplexe System nun noch ein weiteres Regulierungsregime, dessen Abgrenzung am Merkmal des Personenbezugs nicht trennscharf möglich ist, steigert das die Komplexität zum einen noch einmal deutlich. Zum anderen wird auch die Wirkreichweite von datenspezifischen Rechtsnormen deutlich ausgeweitet, da auch nicht-personenbezogene Daten umfassenden, gleichwohl aber nicht vollständig konsistenten, rechtlichen Restriktionen unterliegen würden.

Ein neues Regulierungsregime müsste auch aufgrund des zu erwartenden technischen Fortschritts durch weitere Innovationen technologieoffen formuliert werden und regelungstechnisch mit unbestimmten Rechtsbegriffen arbeiten. Die dadurch geschaffene Rechtsunsicherheit kann auch kaum durch die klassischen Instrumente wie eine höchstrichterliche Rechtsprechung substantiell reduziert werden. Das Verhältnis von Schnelllebigkeit digitaler Innovationszyklen einerseits und die lange Dauer von Gerichtsverfahren über mehrere Instanzen andererseits bedingt, dass eine gesicherte Rechtsprechung im Regelfall erst vorliegt, wenn sich das hinter dem Streit stehende Problem bereits wieder erledigt hat. Vergleichbares konnte man bei den Patentstreitigkeiten beim Aufkommen des mobilen Betriebssystems Android beobachten. So einigten sich erst kürzlich die Konkurrenten Apple und Samsung nach jahrelangen Rechtsstreitigkeiten in unterschiedlichen Jurisdiktionen rund um den Globus.[42] Inzwischen hat sich das Betriebssystem Android längst etabliert und der Initiator Google Inc. arbeitet bereits an einem Nachfolgeprodukt.[43] Auch im Datenschutzrecht ist zu beobachten, dass Jahrzehnte nach der Etablierung dieses Rechtsgebiets auf europäischer Ebene wesentliche Fragen ungeklärt sind.[44] Es stünde zu befürchten, dass sich dieses Faktum auch in Bezug auf Ausschließlichkeitsrechte an Daten vor allem große Akteure zu Nutze machen könnten. Wer kapitalstark genug ist, auch jahrelange Rechtsstreitigkeiten auszutragen, wird es bei unklarer Rechtslage eher wagen können, die eigene Entwicklung trotz langwieriger Gerichtsverfahren fortzusetzen und statt dem frühen Kompromiss die langfristige Konfrontation zu suchen. Die Innovationskraft trotz auftretender Rechtsstreitigkeiten bliebe so tendenziell

---

[41] Dazu detailliert Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 198 ff.

[42] https://www.tagesschau.de/wirtschaft/apple-samsung-103.html, 06.08.2018.

[43] https://www.heise.de/newsticker/meldung/Fuchsia-ist-kein-Linux-Google-veroeffentlicht-Dokumentation-zu-neuem-OS-4021845.html, 06.08.2018.

[44] Vgl. dazu auch Kühling/Klar, NJW 2013, 3611.

eher großen Unternehmen vorbehalten. Dabei haben sich gerade bei datengetriebenen Geschäftsmodellen kleinere Start-Ups als besonders innovativ erwiesen. Der dadurch erzielte gesamtwirtschaftliche Nutzen, der einher geht mit einer größtmöglichen Angebotsvielfalt für Verbraucher, könnte gefährdet werden.

2.3 Ökonomisierung von personenbezogenen Daten - gerechte Verteilung der Wertschöpfung durch stärkere Akzentuierung der datenschutzrechtlichen Einwilligung

Die Diskussion über Dateneigentumsrechte suggeriert, dass derzeit eine wirtschaftliche Verwertung von Daten nicht möglich sei. Dieses Bild wird weder der gegenwärtigen tatsächlichen noch der rechtlichen Situation gerecht. Die fünf nach ihrem Börsenwert wertvollsten Konzerne der Welt[45] bauen ihre Geschäftsmodelle auf die Nutzung von Daten auf oder tragen mit datengetriebenen Diensten stark zu ihrer jeweiligen Wertschöpfung bei. Zudem ist die wirtschaftliche Nutzung von Daten rechtlich keineswegs unreguliert (siehe dazu bereits oben). Die Ökonomisierung von Daten ist bereits weit verbreitet und schreitet weiter voran. Dabei sind personenbezogene wie auch nicht-personenbezogene Daten betroffen. Verbraucher sind zwar teilweise Nutznießer der Verarbeitung ihrer Daten. Allerdings sind auch Konstellationen erkennbar, in denen zumindest unklar ist, ob die Verbraucher angemessen an der Wertschöpfung mit ihren Daten beteiligt werden. Dies kann insbesondere dann der Fall sein, wenn eine Auswahlmöglichkeit am Markt nicht besteht und aufgrund faktischer Zwänge nur ein Anbieter in Betracht kommt und dieser seine Leistungen von einer Einwilligung in die Nutzung der Daten des Verbrauchers abhängig macht. Daraus lässt sich gleichwohl kein gesetzgeberischer Handlungsbedarf ableiten, denn auch diese Problematik ist vor allem wettbewerblicher Natur beziehungsweise wird auch datenschutzrechtlich erfasst. Dass insbesondere auch kartellrechtliche Aspekte eine zentrale Rolle spielen können, zeigt das derzeit anhängige Facebook-Verfahren beim Bundeskartellamt.[46]

Die Lösung könnte hier in der stärkeren Akzentuierung der datenschutzrechtlichen Einwilligung durch eine konsequente Umsetzung des geltenden Rechts liegen. Mit ihrer Hilfe könnten Verbraucher nach dem Modell „Daten gegen Service“, das bereits heute weit verbreitet ist, oder aber „Daten als alternatives Zahlungsmittel“ ihre Daten wirtschaftlich verwerten.[47] Denn eine Verfügung über personenbezogene Daten kann insbesondere

---

[45] http://www.faz.net/aktuell/wirtschaft/diginomics/das-sind-die-wertvollsten-unternehmen-der-welt-15364862.html, 06.08.2018.

[46] Vgl. dazu Monopolkommission, Hauptgutachten XII, 2018, Rn. 659, abrufbar unter http://monopolkommission.de/images/HG22/HGXXII_Gesamt.pdf, 06.08.2018.

[47] Krohm/Müller-Peltzer, ZD 2017, 551, 553.

durch eine datenschutzrechtliche Einwilligung erfolgen. So kann die betroffene Person mit einer Einwilligung einen Datenverarbeiter von datenschutzrechtlichen Restriktionen freistellen und eine Verarbeitung der Daten erlauben. Sie kann diese Einwilligung ähnlich wie bei einer rechtsgeschäftlichen Willenserklärung davon abhängig machen, ob sie sich davon eigene wirtschaftliche Vorteile verspricht. Da das Datenschutzrecht in erster Linie dem Grundrechtsschutz dient, auf den die betroffene Person auch verzichten kann beziehungsweise die Ausübung ihres Rechts auf informationelle Selbstbestimmung durch eine gewollte Kommerzialisierung erfolgen kann, könnte eine sinnvoll ausgestaltete Einwilligung unter der DS-GVO in dogmatischer Hinsicht das prädestinierte Instrument sein, die wirtschaftliche Verwertung von personenbezogenen Daten zu steuern.

Die Rechtsnatur[48] der Einwilligung war schon unter dem BDSG a.F. umstritten. Zum Teil wurde sie als rechtsgeschäftliche Erklärung[49], zum Teil als Realhandlung[50] und dann wiederum als geschäftsähnliche Handlung[51] begriffen. Fest steht, dass es sich bei der Einwilligung um eine antizipierte Erlaubnis handelt (mit Ähnlichkeit zu § 183 BGB). Die Einwilligung ist somit immer und stets vor der Verarbeitung personenbezogener Daten einzuholen und kann nicht nachträglich als Genehmigung eine Heilung bewirken (mit Ähnlichkeit zu § 184 BGB).[52] Mit der konkreten Regelung der Einwilligung Minderjähriger in Art. 8 Abs. 1 DS-GVO hat dieser Streit stark an Bedeutung eingebüßt. Für die Frage des Umgangs mit Willensmängeln wie Irrtümern oder Täuschung ist er aber gleichwohl noch relevant. Viel spricht dafür, dass unter dem Regime der DS-GVO die Einwilligung eine Handlung sui generis ist, auf welche die nationalen Vorschriften über Willenserklärungen nicht – auch nicht entsprechend – Anwendung finden können. Unionsrechtsautonom müssen jedoch Grundsätze entwickelt werden, die den Umgang mit Fällen der Täuschung und des Irrtums regeln.

Ungeachtet dessen ist die Einwilligung das zentrale, sogar grundrechtlich fundierte,[53] Instrument zur Verfügung über datenschutzrechtlich geschützte Daten. Als einziger Zuläs-

---

[48] Dieser Absatz ist stark orientiert an Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 493.

[49] Zum BDSG a.F. Simitis, in: Simitis (Hrsg.), Kommentar zum BDSG, 8. Aufl. 2014, § 4a, Rn. 20; so jetzt auch zur DS-GVO Schaffland/Holthaus, in: Schaffland/Wiltfang (Hrsg.), DS-GVO/BDSG, EL 10/17 Stand: Dezember 2017, Art. 7, Rn. 11 f.

[50] Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4a, Rn. 10.

[51] Holznagel/Sonntag, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.8, Rn. 21.

[52] Zum BDSG a.F. Gola/Schomerus, BDSG, 12. Aufl. 2015, § 4a, Rn. 15; Schaffland/Holthaus, in: Schaffland/Wiltfang (Hrsg.), DS-GVO/BDSG, EL 10/17 Stand: Dezember 2017, Art. 7, Rn. 12; Tinnefeld/Buchner/u.a., Einführung in das Datenschutzrecht, 6. Aufl. 2018, S. 396 f.

[53] Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 497.

sigkeitstatbestand nach Art. 6 DS-GVO kann die Einwilligung jedwede Datenverarbeitung legitimieren. Diese für das Datenschutzrecht grundlegende Konstrukt ist bereits in Art. 8 GrCh angelegt und hat sich seit Jahrzehnten bewährt.

Damit die Einwilligung tatsächlich als Ausdruck der freien Entscheidung des Verbrauchers über die Verwendung seiner Daten verstanden werden kann, darf sie weder bloßer formalistischer Akt sein, noch erdrückenden wirtschaftlichen Zwängen unterliegen. Für die Wirksamkeit einer Einwilligung gibt es deshalb strenge Voraussetzungen:[54]

Freiwilligkeit der Einwilligung (Art. 4 Nr. 11 DS-GVO; Art. 7 Abs. 4 DS-GVO)

Die explizite Forderung der Freiwilligkeit der Einwilligung für ihre Wirksamkeit spiegelt die Erkenntnis aus der Rechtswirklichkeit wider, dass sich oftmals ungleiche Partner gegenüberstehen. Die Einwilligung droht ihre Legitimationswirkung für den Eingriff in sein informationelles Selbstbestimmungsrecht zu verlieren, wenn aufgrund der faktischen Verhältnisse gleichsam keine Wahl besteht und eingewilligt werden muss, um die begehrte Leistung zu erhalten.[55] Insgesamt sind für die Bewertung der Freiwilligkeit die Kriterien des Ungleichgewichts, der Erforderlichkeit, der vertragscharakteristischen Leistung, der zumutbaren Alternative und eines angemessenen Interessenausgleichs relevant.[56]

So kann eine Einwilligung unfreiwillig sein, wenn zwischen betroffener Person und Datenverarbeiter ein klares Ungleichgewicht besteht (vgl. Erwägungsgrund 43 der DS-GVO). Dies kann bei Hinzutreten weiterer Umstände auch zwischen Unternehmer und Verbraucher der Fall sein.[57] Es sind demnach auch Verbraucher, die in der Gefahr stehen, eine unfreiwillige Einwilligungserklärung abzugeben.

Mit Art. 7 Abs. 4 schreibt die DS-GVO die schon unter dem Regime von Richtlinie und nationalen Umsetzungsgesetzen[58] geltenden Grundsätze des sog. Koppelungsverbots fort und stellt auch sonst an die Freiwilligkeit der Einwilligung vergleichbare Anforderungen.[59] Für Verbraucher gelten demnach hier keine neuen Regeln. Das Koppelungsverbot

---

[54] Der folgende Abschnitt ist stark orientiert an Kühling/Klar/Sackmann, Datenschutzrecht, 4. Aufl. 2018, Rn. 499 ff.

[55] Vgl. Beschl. v. 25.3.1992, 1 BvR 1430/88 = BVerfGE 85, 386.

[56] Siehe dazu und zum Folgenden Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 41 ff.

[57] Vgl. Erwägungsgrund 43 der DS-GVO; dazu auch Buchner, DuD 2016, 155, 158.

[58] Vgl. insbesondere § 28 Abs. 3b BDSG a.F. sowie § 95 Abs. 5 TKG.

[59] Vgl. Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 41 und 43; Buchner, DuD 2016, 155 (158); sehr kritisch dazu Härting, Koppelungsverbot – der Einwilligungskiller nach der DS-GVO, CR-online.de Blog v. 11.10.2016, abrufbar unter https://www.cr-online.de/blog/2016/10/11/, 06.08.2018.

wird verletzt, wenn die Erfüllung eines Vertrages von einer Einwilligung abhängig gemacht wird, obwohl die Datenverarbeitung, in welche eingewilligt wird, für die Erfüllung des Vertrages nicht erforderlich ist.[60] Durch die Einwilligung kann zudem die Bereitstellung der personenbezogenen Daten selbst zum Gegenstand der Hauptleistungspflicht mutieren, etwa im Falle eines Tausches „Daten gegen Leistung“, dessen Zulässigkeit allerdings durchaus umstritten ist.[61] Dann muss dieses Leistungs-Gegenleistungs-Verhältnis aber hinreichend transparent sein, insbesondere wenn ein Verbraucher beteiligt ist. Für die Beurteilung der Erforderlichkeit muss zudem das spezifische Charakteristikum des vom Verantwortlichen erbrachten Dienstes bestimmt werden, was gerade für die „Online-Welt“ ein transparentes Modell „Daten gegen Leistung“ eröffnet.[62] Weiterhin spielt es eine Rolle, ob der betroffenen Person für den gewünschten Vertragsschluss eine zumutbare Alternative am Markt zur Verfügung steht.[63] Das kann besonders bei sehr marktstarken oder marktbeherrschenden Akteuren wie großen Suchmaschinen oder sozialen Netzwerken eher nicht der Fall sein. Richtigerweise muss daneben noch bei der Gesamtbetrachtung das Kriterium eines angemessenen Interessenausgleichs berücksichtigt werden.[64]

Eine stark zulasten der betroffenen Person und gegen dessen objektive Interessen gerichtete Einwilligung indiziert subjektiv Zweifel an der Freiwilligkeit.[65] Je unvorteilhafter eine Einwilligung für die betroffene Person objektiv ist, umso mehr wird bei den anderen Kriterien kritisch zu prüfen sein, ob die Einwilligungserklärung wirklich Ausdruck einer freien Entscheidung der betroffenen Person ist. Im Ergebnis kann also nur dann von einer freien Entscheidung der betroffenen Person gesprochen werden, wenn die betroffene Person effektiv die Möglichkeit hat, selbst zu bestimmen, ob und wie ihre Daten verarbeitet werden. Beruht die Einwilligung der betroffenen Person nicht auf ihrer freien Entscheidung, ist ihre Einwilligung unwirksam. Bereits erhobene Daten sind grundsätzlich zu löschen.

Für eine gerechte Monetarisierung von Verbraucherdaten ist die Freiwilligkeit der Einwilligung conditio sine qua non. Insbesondere kann das Abhängigmachen einer Dienstleistung von der Preisgabe von Daten dann auf Basis einer entsprechenden Einwilligung

[60] Vgl. Buchner, DuD 2016, 155 (158); Heckmann/Paschke, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 7, Rn. 52.

[61] A.A. wohl die Art.-29-Datenschutzgruppe, WP 259 v. 28.11.2017, S. 9.

[62] Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 49.

[63] Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 52 ff.

[64] Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 54.

[65] In diese Richtung auch Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 54.

zulässig sein, wenn anstelle der Preisgabe der Daten eine alternative Bezahlmethode angeboten wird und der Preis nicht unangemessen hoch ist. Dann nämlich hat der Verbraucher eine klare Wahlmöglichkeit.[66] Den Daten wird so auch tatsächlich ein transparenter Preis zugewiesen, wodurch der wirtschaftliche Gegenwert dem Verbraucher vor Augen geführt wird und er auch in vergleichbaren Situationen auf eine angemessene Gegenleistung für seine Daten fordern und durchzusetzen versuchen wird. Dabei müssen aber die Interessen finanzschwächerer Verbrauchergruppen im Auge behalten werden.

Informiertheit der Einwilligung (Art. 4 Nr. 11 DS-GVO)

Das Unionsrecht fordert in Art. 4 Nr. 11 DS-GVO darüber hinaus, dass die Einwilligung in informierter Weise zu erfolgen hat. Nur ein Verbraucher, der alle entscheidungsrelevanten Informationen kennt, kann Risiken und Vorteile der Einwilligung abschätzen und eine darauf basierende Entscheidung treffen. Den Verantwortlichen trifft somit eine umfassende Informationspflicht, insbesondere hinsichtlich der Arten von verarbeiteten Daten, des Verarbeitungszwecks, der Identität des Verantwortlichen und dessen Erreichbarkeit und an welche Empfänger gegebenenfalls Daten übermittelt werden, die er *vor* Einholung der Einwilligung erfüllen muss (vgl. im Einzelnen Art. 12 und 13 DS-GVO).[67]

Bestimmtheit der Einwilligung (Art. 5 Abs. 1 lit b, 6 Abs. 1 UAbs. 1 lit. a DS-GVO)

In engem Zusammenhang mit der soeben beschriebenen Informationspflicht des Verantwortlichen steht das Erfordernis der Bestimmtheit der Einwilligungserklärung (Art. 5 Abs. 1 lit. b und Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO), das sich unmittelbar aus dem Zweckbindungsgrundsatz ableitet.[68]

Insbesondere bei Allgemeinen Geschäftsbedingungen stellt die Bestimmtheit der Einwilligung ein Kernproblem dar. Das AGB-Recht ist bei der Gestaltung von vorformulierten Einwilligungserklärungen weiterhin parallel zu prüfen und schützt damit insbesondere die Verbraucher in vollem Umfang. Unklarheiten gehen auch hier zulasten des Verantwortlichen. Im Übrigen ist ganz grundsätzlich Skepsis gegenüber dem Vorliegen einer „freien Entscheidung“ angezeigt, wenn letztlich keine individuelle Willensbetätigung ersichtlich

---

[66] In diese Richtung auch Krohm/Müller-Peltzer, ZD 2017, 551, 553.

[67] Vgl. Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 59 f.

[68] Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 61.

ist.[69] Insofern sind hier die Anforderungen an die Hervorhebung besonders streng.[70] Die Verbraucher müssen erkennen können, ob ein Text eine vorformulierte Einwilligungserklärung oder aber einen Hinweis auf gesetzliche Zulässigkeitstatbestände darstellt oder der Verantwortliche damit Informationspflichten erfüllt.

Jederzeitige Widerrufbarkeit der Einwilligung (Art. 7 Abs. 3 DS-GVO)

Art. 7 Abs. 3 DS-GVO normiert die jederzeitige Widerrufbarkeit der Einwilligung nunmehr explizit.[71] Dies ist Ausdruck der Freiwilligkeit der Einwilligung. Der Widerruf ist dem Verantwortlichen gegenüber zu erklären, der auch Adressat der Einwilligungserklärung war.

Der Widerruf entfaltet Wirkung für die Zukunft. Wurden jedoch Daten bereits gespeichert, sind sie nunmehr grundsätzlich zu löschen, es sei denn, es besteht eine anderweitige Rechtsgrundlage für die Verarbeitung (vgl. Art. 17 Abs. 1 lit. b DS-GVO). Sollte auch eine Übermittlung getätigt worden sein, hat der Verantwortliche den Empfänger über den Widerruf der betroffenen Person zu informieren.[72] Das Fehlen einer Belehrung führt nicht automatisch zur Rechtswidrigkeit der Verarbeitung, auch wenn Art. 7 Abs. 3 DS-GVO eine Pflicht statuiert, die betroffene Person von der Widerrufbarkeit in Kenntnis zu setzen.[73]

Werden die gesetzlichen Vorgaben stringent umgesetzt, so löst sich dadurch auch das Problem, dass die Einwilligung in der Praxis vielfach einem bloßen Formalismus gleicht.[74] Gleichzeitig muss durch die sachgerechte Anwendung der übrigen Zulässigkeitstatbestände eine sinnvolle Vorsteuerung erfolgen, sodass die Einwilligung nur zu wirklich zentralen Fragen erforderlich ist. Andernfalls besteht die Gefahr, dass die große Anzahl an Einwilligungsanfragen an den Verbraucher diesen überfordern und in der Folge ohne entsprechende Reflektion erteilt werden.[75]

---

[69] Siehe auch Menzel, DuD 2008, 400 (406).

[70] So zum BDSG a.F. etwa OLG Koblenz, Urt. v. 26.3.2014, 9 U 1116/13 = WRP 2014, 876 (877 f.).

[71] Buchner/Kühling, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO, Rn. 33.

[72] Frenzel, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 7 DS-GVO, Rn. 16.

[73] Vgl. Ernst, ZD 2017, 110 (112); Heckmann/Paschke, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 7, Rn. 32.

[74] Zu diesem Problem umfassend Radlanski, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, Mohr Siebeck.

[75] In diese Richtung, allerdings mit der Begründung zu umfangreicher Informationen auch Specht/Kerber, Datenrechte, S. 62, abrufbar unter: http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf, 06.08.2018.

DIE DATENSCHUTZRECHTLICHE EINWILLIGUNG ALS GEEIGNETES INSTRUMENT ZUR VERFÜGUNG DES VERBRAUCHERS ÜBER DIE EIGENEN DATEN

Eine Einwilligung, die den Vorgaben der DS-GVO entspricht, könnte ein geeignetes Mittel sein, um Verbrauchern eine echte Wahlfreiheit und die Möglichkeit zur Kommerzialisierung der sie betreffenden Daten zu bieten. Besondere Beachtung kommt dabei der Freiwilligkeit der Einwilligung und somit dem Kopplungsverbot zu, um diese nicht als bloßen Formalismus in ihrer Wirkung zu unterlaufen. Die gegenwärtige Rechtslage bildet dafür einen geeigneten Rahmen.

2.4 Fokus auf exekutivem Vollzug – kein gesetzgeberischer Handlungsbedarf

Ein akuter gesetzgeberischer Handlungsbedarf ist daher insgesamt nicht zu erkennen. Es ist dennoch nicht ausgeschlossen, dass im Verlauf der weiteren Entwicklung punktuell ein gesetzgeberisches Nachsteuern sinnvoll erscheinen könnte. Das aber sollte stets an konkrete tatsächlich bestehende Probleme anknüpfen und nur nach entsprechender Beobachtung des Rechts- und Marktgeschehens erfolgen.[76] Dabei ist jede Form eines Ausschließlichkeitsrechts als kontraproduktiv abzulehnen. Im Blick behalten werden muss vielmehr der möglichst ungehinderte Zugang zu Daten.[77] Dazu kann es sich bei entsprechenden Entwicklungen als sinnvoll erweisen, sektorspezifisch besondere Zugangsrechte zu normieren. Derzeit ist aber nicht erkennbar, dass insbesondere die Instrumente des Kartellrechts nicht ausreichen, um schädlichen Marktmachtkonzentrationen entgegenzuwirken beziehungsweise deren Folgen abzumildern.

ZUGANG STATT ABSCHOTTUNG

Ein sinnvolles Datenrecht jenseits des Persönlichkeitsschutzes sollte den Fokus also nicht auf einen erweiterten Schutz der Rechte eines etwaigen „Datenerzeugers“ legen, sondern auf Eröffnung und Sicherung des Zugangs zu Datenbeständen bei mono- oder oligopolistischen Marktgegebenheiten. Auch hier besteht derzeit aber kein spezifischer Regulierungsbedarf. Das Kartellrecht bietet ausreichende Instrumente, um den sich gegenwärtig stellenden Problemen zu begegnen.

---

[76] So auch das Max-Planck-Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“ – 10 Fragen und Antworten, S. 4, abrufbar unter https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf, 06.08.2018.

[77] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau einer Europäischen Datenwirtschaft vom 10.1.2017, COM(2017) 9 final, S. 4 und 9; so auch das Max Planck Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“ – 10 Fragen und Antworten, S. 4, abrufbar unter https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf, 06.08.2018.

III. EXEMPLARISCHE SEKTORSPEZIFISCHE ANALYSE

Die jeder neuen Regelsetzung zugrundeliegende These, dass die bestehende Rechtslage unbillige Ergebnisse schaffe, hieße konkret bezogen auf die Verteilung der datengenerierten Wertschöpfung, dass die gegenwärtigen rechtlichen Instrumente zu unbilligen oder unklaren Ergebnissen kämen. Um durch Gesetzesanpassungen Verbesserungen zu erzielen, müsste sich demnach durch die potenziellen Änderungen entweder in materieller Hinsicht die Verteilung gerechter/effizienter gestalten und beziehungsweise oder das Regelungsgefüge zu klareren Ergebnissen gelangen und damit unter Rechtssicherheitsgesichtspunkten vorzugswürdig sein. Dies soll exemplarisch an zwei geeigneten sektorspezifischen Referenzgebieten untersucht werden. Die Analyse beschränkt sich auf die Zweckmäßigkeit einer Regelungsanpassung per se, also auf das „ob“ eines gesetzgeberischen Handlungsbedarfs, da der Befund schon insoweit jeweils negativ ist und sich daher die Frage nach dem „wie“ gar nicht mehr stellt.

1. SEKTORSPEZIFISCHES REFERENZGEBIET I: MOBILITÄT

Dass die digital unterstützte Mobilität ein wichtiges Zukunftsthema darstellt, ist bereits seit einiger Zeit offenkundig. Denn die Mobilität von Personen erfasst letztlich jeden Einzelnen in vielen alltäglichen Situationen und hat daher wie kaum eine andere Entwicklung ein hohes wirtschaftliches Potenzial. Gleichzeitig sind der Aufenthaltsort und die täglichen Bewegungen einer Person geeignet, sehr viel über ihr Verhalten und ihre Persönlichkeit auszusagen. Mobilitätsdaten von Verbrauchern sind daher besonders sensibel. Zugleich verspricht gerade bei der Mobilität eine zunehmende Datenverarbeitung sehr weitreichende Optimierungs- und Wertschöpfungspotenziale. Es ist daher nicht verwunderlich, dass die gegenwärtig geführte Debatte über ein Dateneigentumsrecht in Deutschland ihren Ursprung in der Automobilindustrie hatte.[78] Die Mobilität ist daher das prädestinierte Referenzgebiet, um sektorspezifisch mögliche Auswirkungen von Ausschließlichkeitsrechten an Daten auf Verbraucher zu untersuchen. Das Bundesministerium für Verkehr und digitale Infrastruktur hat zur Frage einer „Eigentumsordnung für Mobilitätsdaten“ eine sehr umfangreiche Studie erstellen lassen, wodurch die Diskussion in diesem Bereich (vor allem mit einem Fokus auf dem Individualverkehr) besonders weit vorangeschritten ist. Die Studie bereitet die rechtlichen Probleme sehr differenziert auf,

[78] Schulzki-Haddouti, Wem nützt ein neues Eigentum an Daten?, abrufbar unter https://www.golem.de/news/datenschutz-wem-nuetzt-ein-neues-eigentum-an-daten-1805-134162.html, 06.08.2018.

allerdings sind die gefundenen möglichen Handlungsoptionen sehr kritisch zu betrachten, denn ein entsprechender Handlungsbedarf besteht nicht.[79]

1.1 Wertschöpfungsverteilung im regulierten Wettbewerb anstelle fester rechtlicher Zuweisung

Wie oben aufgezeigt wurde, gibt es durchaus rechtlich geschützte tatsächliche Positionen für Inhaber von Datenbeständen, die den Handel mit Daten ermöglichen und demjenigen, der in Datenverarbeitung investiert, die wirtschaftliche Verwertung seiner Daten erlauben. Im Mobilitätsbereich spielt – jedenfalls beim Individualverkehr – der Hersteller eines Fahrzeugs dabei eine zentrale Rolle. Dieser kann die entsprechenden Schnittstellen der Fahrzeugsysteme designen und gegebenenfalls unmittelbar mit seinen eigenen Diensten verknüpfen. Das führt in der Praxis oftmals dazu, dass der Hersteller den faktischen Erstzugriff auf die Daten des Fahrzeugs erhält. Einschränkend wirken primär die datenschutzrechtlichen Vorgaben. Insofern hat auch die im datenschutzrechtlichen Sinne betroffene Person eine durchaus starke Stellung, wenn ihre Einwilligung erforderlich ist. Gerade an der Verarbeitung von Fahrzeugdaten kann jedoch durchaus ein berechtigtes Interesse bestehen, sodass eine Einwilligung zur Datenverarbeitung nicht immer erforderlich ist (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO). Bei anderen digitalen Mobilitätsdiensten wie insbesondere Plattformen der „seamless mobility“, also der intermodalen Verkehrsträgernutzung und deren Verknüpfung über intelligente Algorithmen, hat faktisch der Diensteanbieter den ersten Zugriff auf die mit dem Dienst generierten Daten. Aus datenschutzrechtlicher Sicht ist der Dienstnutzer bei Mobilitätsdiensten fast immer persönlich identifizierbar und damit betroffene Person. Der dienstnutzende Verbraucher hat auch faktisch die Möglichkeit, den genutzten Dienst auszuwählen, sodass er über denjenigen bestimmt, der Zugriff auf die Daten erhält. Über eine informierte und freiwillige Einwilligung stehen ihm noch granularere Steuerungsmöglichkeiten zur Verfügung, wenn seine Daten nicht ausnahmsweise in anonymer Form verarbeitet werden.

Damit liegt die tatsächliche Herrschaft von Daten in den meisten Fällen bereits nach gegenwärtiger Rechtslage bei den dienstnutzenden Verbrauchern, soweit die verarbeiteten Daten sich auf diese beziehen. Voraussetzung für die tatsächliche Selbstbestimmung durch das Instrument der Einwilligung ist dabei aber, dass ein ausreichendes Angebot an digitalen Mobilitätsdiensten vorhanden ist. Problematisch sind daher mono- oder oli-

[79] So schon Kühling/Sackmann, NVwZ 2018, 681, 684, f.

gopolistische Strukturen, weshalb gerade Plattformen einer Kontrolle durch kartellrechtliche Instrumente unterliegen müssen. Dafür reichen aber die gegenwärtigen exekutiven Handlungsmöglichkeiten aus und diese müssen gegebenenfalls konsequenter genutzt werden.[80] Damit gibt die gegenwärtige Rechtslage in struktureller Hinsicht einen sehr sinnvollen Rahmen vor, bei dem keine praktische Dysfunktionalität festgestellt werden kann.

Zu untersuchen ist ferner, ob an dieser tatsächlichen Lage in materieller Hinsicht aus Gemeinwohl- oder sonstigen Gründen etwas geändert werden sollte („ob“). Es ist insbesondere zu prüfen, ob Daten durch rechtliche Instrumente anderen Akteuren zugewiesen werden sollten als denjenigen, die derzeit die Herrschaft darüber ausüben. Nur wenn diese Frage zu bejahen wäre, müsste man sich mit der Art der Umsetzung befassen („wie“). Dabei fällt auf, dass die gegenwärtige Situation gute Anreize schafft, Daten zu generieren. Denn der Datenerzeuger hat im Mobilitätsbereich rein faktisch eine starke Position und im Regelfall den ersten Zugriff auf die generierten Daten und kann diese verwerten. Dadurch hat er ein eigenes Interesse an intensiver und effektiver Datenverarbeitung zur Steigerung der wirtschaftlichen Wertschöpfung. Hinzu treten datenschutzrechtlich geschützte Interessen einer etwaigen betroffenen Person, der – eine konsequente Durchsetzung des mit der DS-GVO geschaffenen Rahmens vorausgesetzt – mit der Einwilligung gute Steuerungsmöglichkeiten offenstehen.

In materieller Hinsicht könnte man allenfalls erwägen, bei KFZ-Daten den Halter in eine stärkere Position zu bringen. Allerdings würde dies wohl der tatsächlichen Lage nicht gerecht, denn ein hinreichendes technisches oder kaufmännisches Verständnis zur Vermarktung der eigenen KFZ-Daten über die Auswahl eines geeigneten Anbieters und die Freigabe einzelner Daten zur Verarbeitung hinaus wird bei den wenigsten KFZ-Haltern vorhanden sein. Im Übrigen dürfte dem KFZ-Halter mit der datenschutzrechtlichen Einwilligung auch ein gutes Instrument zur Freigabe der KFZ-Daten zur Verarbeitung durch Dritte zur Verfügung stehen. KFZ-Daten haben nämlich immer dann einen Personenbezug zum Halter im datenschutzrechtlichen Sinne (dazu oben 1.3.), wenn mit diesen die Fahrgestellnummer oder das Kennzeichen verknüpft ist, oder anderweitig eine Identifikationsmöglichkeit des konkreten Fahrzeugs besteht.[81] Es ist daher schon im Ausgangspunkt nicht erkennbar, welche materiellen Änderungen am gegenwärtigen – durchaus

[80] Zu einem wettbewerbsrechtlichen Zugangsanspruch zu Fahrzeugdaten vgl. auch LG Frankfurt/M, Urteil vom 21.1.2016, Az. 2-03 O 505/13 = ZD 2016, 331.

[81] Vgl. VZBV, Verbraucher als „Eigentümer“ von KFZ-Daten?, abrufbar unter https://www.vzbv.de/sites/default/files/downloads/2017/11/06/17-11-03_stn_mobilitaetsdaten_final.pdf, 06.08.2018.

sinnvollen und schutzzweckorientierten System – indiziert sein sollten. Die Datengenerierung wird gegenwärtig belohnt und die Daten liegen in der faktischen Herrschaft desjenigen, der die höchste technische und kaufmännische Kompetenz besitzt, diese zu verwerten. Dieser hat daher ein großes Interesse an der Datengenerierung, sodass auch die Anreizsetzung beim gegenwärtigen Rechtsrahmen funktioniert. Die Voraussetzungen für einen starken und wünschenswerten Wettbewerb sind vor diesem Hintergrund grundsätzlich gegeben. Bei konsequenter Nutzung der Einwilligung als Verfügungsinstrument werden auch die Verbraucher angemessen an der Wertschöpfung beteiligt. Wo dies gegenwärtig noch nicht geschieht, liegt das Problem in einer mangelnden Nutzung des gegebenen Rechtsrahmens und nicht in fehlenden rechtlichen Instrumenten. Nicht ausgeschlossen scheint es, dass die Fahrzeughersteller eine sehr starke Stellung einnehmen werden, sodass sich die Gefahr monopolistischer Tendenzen hier in besonderer Weise stellen dürfte. Eine Lösung könnte jedoch das gegenwärtige Kartellrecht bieten.[82] Hier hängt es im Wesentlichen an der vorzunehmenden Marktabgrenzung, die Instrumentarien zu aktivieren. Es erscheint überlegenswert, ob für die Frage des Zugangs zu Fahrzeugdaten nicht je Hersteller ein einzelner Markt für Fahrzeugdaten anzunehmen sein könnte, ähnlich wie im Telekommunikationsrecht das sogenannte Ein-Netz-Ein-Markt-Prinzip. Denn der Fahrzeugkäufer wird seine Kaufentscheidung für ein Fahrzeug nicht von den Möglichkeiten der Datennutzung und Drittanbieterangeboten abhängig machen. In der Folge könnten sich durchaus Zugangsrechte, wie etwa für freie Werkstätten, ergeben. Teilweise wurde dies auch schon sektorspezifisch normiert.[83] Allerdings sind die hier relevanten Fragestellungen noch ganz im Entstehen begriffen, sodass Aussagen zur Marktabgrenzung noch verfrüht sind.

1.2 Rechtsunsicherheit und Transaktionskosten durch hohe Regelungskomplexität

Die Regelungskomplexität im Datenschutzrecht ist bereits jetzt außergewöhnlich hoch. Das zeigt sich besonders bei Sachverhalten mit Bezug zur Mobilität. Ortsveränderungen als Wesensmerkmal der Mobilität bedingen auch vermehrte Fragen des örtlichen Anwendungsbereichs einer Regelung. Obgleich der örtliche Anwendungsbereich des Datenschutzrechts in Art. 3 DS-GVO vergleichsweise klar geregelt ist und die DS-GVO in

[82] Vgl. dazu auch Specht/Kerber, Datenrechte, S. 84, die allerdings eher eine Ex-ante-Regulierung befürworten, abrufbar unter: http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf, 06.08.2018.

[83] Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typengenehmigung von Kraftfahrzeugen hinsichtlich der Emission von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge, ABl. EU 2007 v. 29.06.2007, Nr. L 171/1; vgl. dazu auch Specht/Kerber, Datenrechte, S. 55, abrufbar unter: http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf, 06.08.2018.

der gesamten Europäischen Union und teils darüber hinaus Gültigkeit beansprucht, spielen Landesgrenzen im Datenschutzrecht nach wie vor eine wichtige Rolle. Dies gilt vor allem für die Binnengrenzen der einzelnen Mitgliedstaaten und in Deutschland auch die Grenzen der Bundesländer. Aufgrund der Konstruktion als Datenschutz*grund*verordnung regelt diese datenschutzrechtliche Sachverhalte nicht abschließend, sondern enthält an zahlreichen Stellen Öffnungsklauseln. Diese haben die Mitgliedstaaten mit teils sehr heterogenen Regelungen ausgefüllt. Das gilt insbesondere für die Betroffenenrechte. Auch die Vorgaben zur Videoüberwachung, die besonders für öffentliche Verkehrsflächen und damit mobilitätsbezogen relevant werden, sind keineswegs einheitlich normiert.[84] Dieses in diesem Teilsegment des Datenschutzrechts besonders komplexe Regelungssystem führt zu einer auch für versierte Fachleute nur schwer zu überblickenden Rechtslage. Gleichzeitig sorgt die Allgegenwärtigkeit von Datenverarbeitung gerade auch in der Mobilitätswirtschaft für einen sehr weiten Bereich, der von Datenschutznormen betroffen ist. Die Komplexität der Regelungen und damit einhergehend der hohe Beratungsbedarf, der qualifiziert nur von spezialisierten Juristen geleistet werden kann, sorgt für hohe Transaktionskosten bei der Datenverarbeitung.[85] Diese Problematik ergibt sich aber keineswegs aus den ursprünglichen Zielen der DS-GVO, sondern aus der Tatsache, dass der Kommissionsentwurf in großen Teilen abgeschwächt wurde und nun ein komplexes Regelungssystem in einer Mehrebenenlogik entstanden ist, das – im Bereich der Videoüberwachung besonders plastisch – auch noch durch problematische nationale Bestimmungen unnötig verkompliziert wurde.

Diese überbordende normative Komplexität ließe sich verringern, wenn von den Öffnungsklauseln der DS-GVO möglichst zurückhaltend Gebrauch gemacht würde. Das sollte in einem ersten Schritt durch Abbau nationaler Regelungen im Rahmen der fakultativen Öffnungsklauseln der DS-GVO verfolgt werden und in einem zweiten Schritt durch eine Reduktion der Öffnungsklauseln in der DS-GVO selbst erfolgen. Die Antwort auf die Schwierigkeiten der Anwendung der DS-GVO kann also keineswegs ein Schritt zurück zur alten Ordnung sein, sondern muss vielmehr darin gesucht werden, die Harmonisierung des Datenschutzregimes weiter voranzutreiben und normativ mehr materielle Inhalte auf der unionalen Ebene zu regeln.

Kontraproduktiv wäre es hingegen, wenn neben der datenschutzrechtlichen Ordnung noch weitere Ausschließlichkeitsrechte normiert würden, zumal nur auf nationaler

[84] Vgl. dazu bereits die exemplarischen Ausführungen bei Kühling/Sackmann, NVwZ 2018, 681, 682.

[85] Vgl. Max Planck Institut für Innovation und Wettbewerb, Argumente gegen ein „Dateneigentum“ – 10 Fragen und Antworten, S. 4, abrufbar unter https://www.ip.mpg.de/fileadmin/ipmpg/content/forschung/Argumentarium_Dateneigentum_de.pdf, 06.08.2018.

Ebene. Diese müssten zusätzlich zu datenschutzrechtlichen Aspekten bei jeder Datenverarbeitung geprüft werden und ließen die Transaktionskosten weiter steigen. Eine Prüfung könnte sich dann auch nicht mehr auf personenbezogene Daten beschränken, sondern müsste tatsächlich vor jeglicher Datenverarbeitung durchgeführt werden. Mit zunehmender Datenabhängigkeit der Mobilität würde der Bedarf an rechtlicher Beratung noch weiter ansteigen. Gerade Start-Ups, die eine detaillierte Prüfung oftmals nicht selbst leisten können und auch externen Rechtsrat durch budgetäre Restriktionen nicht in dem erforderlichen Umfang einholen können, werden sich im Zweifel mit juristischen Problemen konfrontiert sehen oder aber Produkte weniger datenintensiv ausgestalten (müssen). Eine verminderte Innovationskraft dürfte die Folge sein.

1.3 Zwischenfazit

Das Beispiel Mobilität zeigt die wachsende Bedeutung von Daten auf, ist gleichzeitig aber auch ein Beispiel für einen an sich funktionierenden gegenwärtigen Rechtsrahmen. Die Zuweisungen von Daten erfolgt auf der Grundlage rechtlich geschützter tatsächlicher Positionen gegenwärtig tendenziell an die Akteure, die daraus die größtmögliche Wertschöpfung erzielen können. Gleichzeitig werden Verbraucher effektiv vor dem Missbrauch ihrer personenbezogenen Daten geschützt und haben auf der Basis des Datenschutzrechts – etwa als Halter oder Fahrer von Fahrzeugen oder als Nutzer sonstiger Mobilitätsdienste – gute Gestaltungs- und Verwertungsmöglichkeiten hinsichtlich ihrer Daten. Ein zusätzlicher dateneigentumsrechtlicher Ansatz wäre insoweit eine überflüssige „Störquelle“. Die Frage des Zugangs zu Daten kann gleichwohl abhängig von der weiteren Entwicklung einen gesetzgeberischen Handlungsbedarf auslösen. Aus gegenwärtiger Sicht könnte diese Problematik allerdings auch mit den Instrumentarien des Kartellrechts lösbar sein.

2. SEKTORSPEZIFISCHES REFERENZGEBIET II: GESUNDHEITSSEKTOR

Der Gesundheitssektor ist zunehmend von Datenverarbeitungsprozessen geprägt, da auch hier die Digitalisierung Einzug hält. Das gilt nicht nur für die medizinische Forschung, die in ihren Studien ganz wesentlich auf eine hohe Datenqualität angewiesen ist. Auch die zunehmend technisierte Patientenbehandlung generiert laufend Daten mittels der eingesetzten Geräte. Dies kann zu einer stetigen Verbesserung der gesundheitlichen Versorgung und damit zum Gemeinwohl beitragen. Ergänzend erfolgen auch die komplexen Abrechnungssysteme zunehmend digitalisiert. Dabei ist das Gesundheitswesen ein wichtiger Wirtschaftszweig mit einer hohen Wertschöpfung und Umsätzen in Milliardenhöhe, sodass den generierten Gesundheitsdaten eine hohe Bedeutung beizumes-

sen ist. Zugleich sind Gesundheitsdaten besonders sensibel. Dies hat auch der europäische Gesetzgeber erkannt und in Art. 9 Abs. 1 DS-GVO Gesundheitsdaten einem besonderen Schutz unterstellt. Die Verbraucher haben berechtigterweise ein hohes Interesse daran, dass ihre Gesundheitsdaten ausschließlich für die notwendige Behandlung und die Verbesserung der Gesundheitsleistungen verwendet werden.

Daher spielt bei Gesundheitsdaten die oben skizzierte Anonymisierung (oben 1.5.) eine besondere Rolle. Bei anonymisierten Daten stellt sich die Frage, wer Zugriff auf diese erhält. So könnten beispielsweise Medizingeräte Daten in anonymisierter Form an ihren jeweiligen Hersteller übermitteln, der damit Zugriff auf sehr umfangreiche Datenbestände gewinnen könnte. Demgegenüber kann auch der Krankenhausbetreiber diese Daten selbst auswerten und nutzen wollen.

Soweit personenbezogene Daten – gerade mit Blick auf den absehbaren Trend zu einer personalisierten Medizin – verarbeitet werden müssen, hat dies selbstredend unter strenger Beachtung der datenschutzrechtlichen Vorgaben zu erfolgen. Eine zusätzliche Dateneigentumsordnung ist in diesem Bereich nicht erforderlich.

2.1 Wertschöpfungsverteilung im regulierten Wettbewerb anstelle fester rechtlicher Zuweisung

Die Verteilung der durch Daten generierten Wertschöpfung muss gerade bei Gesundheitsdaten in hohem Maße an den Erfordernissen des Allgemeinwohls ausgerichtet sein. Allerdings gehört aufgrund der in Europa vorherrschenden öffentlichen Finanzierung des Gesundheitssystems beziehungsweise im Rahmen öffentlich-rechtlich organisierter Körperschaften auch die Finanzierbarkeit des Gesundheitswesens zu den Allgemeinwohlinteressen. Jede Datenverarbeitung, die die medizinische Versorgung auch nur mittelbar preiswerter macht, kann somit zum Allgemeinwohl und zur Entlastung der Verbraucher beitragen. Insofern kann abhängig vom Einzelfall grundsätzlich ein berechtigtes Interesse daran bestehen, dass derjenige Zugriff auf Daten erhält, der eine Wertschöpfung damit generieren kann, wenn seine Interessen diejenigen der betroffenen Person überwiegen. Im Zweifel ist es also besser, dass mehrere Akteure (verschiedene an der Behandlung beteiligte Ärzte und Institutionen; Entitäten, die Verbesserungspotenziale in der Versorgung untersuchen) Zugriff auf Daten erhalten. Im eingangs skizzierten Beispiel der Medizingeräte sollte also jeder Zugriff auf die Daten erhalten können, der damit umzugehen weiß. Entsprechende rechtliche Vereinbarungen können allerdings bilateral beim Kauf der Medizingeräte durchaus wirksam privatautonom vereinbart werden. Vielmehr ist eine hohe Wertschöpfung am besten gewährleistet, wenn derjenige, der die Technik beherrscht, auch Zugang zu den Daten hat. Insofern ist nicht ersichtlich, weshalb in das derzeit herrschende natürliche Gefüge der tatsächlichen Datenherrschaft

durch die künstliche Normierung von Dateneigentumsrechten eingegriffen werden sollte beziehungsweise welche ökonomischen Vorteile daraus erwachsen könnten. Ein gesetzgeberischer Regelungsbedarf ist insoweit nicht erkennbar.

Gegenwärtig besteht zudem das Problem, dass die Digitalisierung (noch) vielfach außerhalb des stark regulierten Gesundheitssektors stattfindet. Zu nennen sind hier beispielsweise Gesundheits-Apps, die von Unternehmen angeboten werden und von Verbrauchern teils ohne Qualitätssicherung Daten erheben. Auch der sogenannte zweite Gesundheitsmarkt (Stichwort „Google-Health“ etc.) wirft die Frage nach einem gesetzgeberischen Handlungsbedarf mit Blick auf die Sensibilität von Gesundheitsdaten auf.[86] Aus daten(schutz)rechtlicher Sicht gilt insofern: Derartige Dienste müssen selbstredend datenschutzkonform erbracht werden (und werden es bisher allzu oft nicht). Allerdings ist das primär eine Frage des Vollzugs der Datenschutzgesetze, der mit der DS-GVO maßgeblich verbessert wurde. Ein weitergehender Handlungsbedarf besteht hier abseits der im Folgenden (sogleich 2.2) zu skizzierenden Komplexitätsreduktion nicht. Denn die datenschutzrechtlichen Belange werden vom gegenwärtigen Rechtsrahmen gut erfasst und nun (hoffentlich) zunehmend auch effektiv durchgesetzt. Die Einführung sonstiger Datenrechte abseits des Datenschutzrechts vermögen diese Probleme jedenfalls keineswegs zu lösen.

2.2 Rechtsunsicherheit durch hohe Regelungskomplexität

Das Regelungsgefüge im Gesundheitsdatenschutzrecht zählt zu den komplexesten überhaupt.[87] Dabei rührt diese Komplexität anders als bei der Mobilität nicht in erster Linie aus dem Mehrebenensystem, sondern aus der Vielzahl an bereichsspezifischen Regelungen. Die Zuständigkeitsverteilung von Bund und Ländern ist im Gesundheitswesen besonders ausdifferenziert geregelt. Vor allem aber gibt es zahlreiche Spezialregelungen, wie beispielsweise in den Landeskrankenhausgesetzen. Das gilt auch vor dem Hintergrund, dass das Gesundheitswesen in großen Teilen öffentlich-rechtlich überformt ist. An anderer Stelle wurde umfassend aufgezeigt, dass die komplex ineinander greifenden Regelungen zur Erbringung und Abrechnung von Leistungen in Krankenhäusern und durch Vertragsärzte und zur Steuerung der Verwendung der dabei erhobenen Daten zu wissenschaftlichen Zwecken insbesondere im Rahmen der Versorgungsforschung

[86] Dazu und zum Folgenden umfassend die Untersuchung von Weichert, Big Data im Gesundheitsbereich, 2018, passim und insbesondere S. 57 ff. und S. 205 ff., abrufbar unter http://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf, 06.08.2018.

[87] Vgl. dazu ganz allgemein die verschiedenen Beiträge in Kingreen/Kühling, Gesundheitsdatenschutzrecht, Reihe Studien zum öffentlichen Recht, 1. Aufl. 2015, Nomos Verlag.

und der Qualitätstransparenz alles andere als klar sind.[88] Verteilt auf Vorgaben im Krankenhausentgeltgesetz (§ 21) und im SGB V (u.a. §§ 95, 295 und 301) – ergänzt um die Vorgaben der Datentransparenzverordnung – bestehen nicht unerhebliche Hürden, um eine sinnvolle Forschung zu ermöglichen. Im Dickicht der mannigfaltigen gesundheitsdatenschutzrechtlichen Regelungen ließen sich eine Vielzahl weiterer Beispiele anführen. Letztlich bedürfte es hier einer umfassenden Reform des normativen Rahmens für den Umgang mit Gesundheitsdaten – nicht nur zu Forschungszwecken und zur Patienteninformation, beides wichtige Anliegen im Sinne der Verbraucher. Eine derartige Reform ließe sich auch ohne Änderungen des unionalen Rechtsrahmens und unter konsequenter Beachtung der materiellen Datenschutzvorgaben umsetzen. Soweit Akteure im Gesundheitsmarkt Zugang zu Daten erhalten, muss dies stets unter Beachtung der datenschutzrechtlichen Vorgaben erfolgen, um Persönlichkeitsrechte nicht auszuhöhlen.

Hinzu kommt, dass auch aufgrund des besonderen Risikos der Diskriminierung der betroffenen Person, das gerade bei Gesundheitsdaten virulent wird, ein verglichen mit den allgemeinen Datenschutzregeln anspruchsvoller und strengerer Rechtsrahmen greift. Das zeigt sich etwa bei der Einwilligung. Zwar sieht Art. 9 Abs. 2 lit. a DS-GVO die Möglichkeit vor, in die Verarbeitung dieser besonderen Kategorien personenbezogener Daten einzuwilligen. An die Einwilligung sind jedoch insofern erhöhte Anforderungen zu stellen, als sie sich ausdrücklich auf diese Daten beziehen muss. In Ergänzung und Verschärfung der bereits erläuterten inhaltlichen Wirksamkeitsvoraussetzungen (dazu oben 2.3.) sind die zu verwendenden sensiblen Daten genau zu benennen und der konkrete Verwendungszusammenhang aufzuzeigen. Denn es lässt sich das Risiko der Verwendung eines sensiblen Datums erst im konkreten Verwendungskontext beurteilen. Insgesamt ist an den Inhalt der Einwilligung ein erhöhtes Maß an Bestimmtheit und Genauigkeit zu stellen. Dies gilt insbesondere für die verbraucherschutzsensiblen vorformulierten Vertragsbedingungen (AGB). Die betroffene Person muss zweifelsfrei erkennen können, welche sensiblen Daten für welchen genau umschriebenen Verwendungszweck in welchem Verwendungskontext verarbeitet werden sollen und darin explizit einwilligen.[89] Das bedeutet etwa für die Forschung mit Gesundheitsdaten, dass eine ausführliche Erläute-

[88] Siehe dazu Kingreen/Kühling, Rechtsfragen der externen Nutzung von Datensätzen aus der Leistungserbringung durch Vertragsärzte und Krankenhäuser, 2017, abrufbar unter https://www.bertelsmann-stiftung.de/fileadmin/files/Projekte/43_Weisse_Liste/VV_Rechtsgutachten_Datennutzung_Kingreen_Ku__hling.pdf, 06.08.2018.

[89] Vgl. Holznagel/Sonntag, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.8, Rn. 56; zum BDSG a.F. Simitis, in: Simitis (Hrsg.), Kommentar zum BDSG, 8. Aufl. 2014, § 4a Rn. 87; ferner Schiff in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 9 Rn. 28 f.

rung der Verwendung der Daten und der zugriffsberechtigten Personen sowie der indizierten Risiken erfolgen muss.[90] Erfüllt die Einwilligung nicht diese erhöhten Ansprüche, ist sie unwirksam. Der Umgang mit den betreffenden sensiblen Daten ist unzulässig und bereits gespeicherte sensible Daten sind grundsätzlich zu löschen.

Art. 9 Abs. 2 lit. a DS-GVO enthält zudem eine Öffnungsklausel**,** wonach das nationale Recht die Einwilligung als Legitimationstatbestand für die Verarbeitung besonders sensibler Daten ausschließen kann. Bislang hat Deutschland davon in den bereits erwähnten zahlreichen Spezialgesetzen Gebrauch gemacht. Möglich wäre es aber, an die Einwilligung anstelle eines vollständigen Ausschlusses an diese spezifischen Anforderungen zu stellen.[91] Diese wären dann wiederum nach nationalem Verfassungsrecht vor dem Hintergrund zu beurteilen, dass die Legitimation einer Datenverarbeitung durch eine Einwilligung gerade Ausdruck des Rechts auf informationelle Selbstbestimmung ist. Eine Beschränkung wäre also ein Eingriff und müsste gerechtfertigt, insbesondere verhältnismäßig sein.

Jedenfalls zeigen diese Ausführungen schlaglichtartig, dass die normative Komplexität des Ordnungsrahmens für Gesundheitsdaten nochmals erhöht und damit auch die Rechtsunsicherheit nochmals gesteigert ist. Müssten nun neben den datenschutzrechtlichen Vorgaben noch weitere Rechte an Daten systematisch geprüft werden, würde das die Komplexität wiederum erhöhen und die ohnehin schon problematische Rechtssicherheit in diesem Bereich weiter schwächen. Gerade bei Gesundheitsdaten zeigt sich, dass eine dateneigentumsrechtliche „Passepartout"-Regelung völlig utopisch ist, da sich in den nur angedeuteten, komplexen einfachgesetzlichen Strukturen jeweils auch Regelungen von Zugriffsberechtigungen finden, die mit einer „grobschlächtigen" Dateneigentumsregelung zwangsläufig kollidieren würden. Umgekehrt ist eine dateneigentumsrechtliche Regelung in all den Spezialnormen noch weniger wünschenswert. Das Referenzgebiet des Gesundheitsdatenschutzrechts in seiner jetzigen – sehr unbefriedigenden – realen Situation zeigt daher besonders deutlich, wie wenig funktionstüchtig und sektorbezogen „abgeglichen" der Vorschlag einer Dateneigentumsregelung ist.

2.3 Zwischenfazit

Die Verarbeitung von Gesundheitsdaten ist besonders verbrauchersensibel und schutzwürdig. Dabei schützt die gegenwärtige Rechtslage die Verbraucher sehr gut vor dem

[90] Dazu etwa Gerling, DuD 2008, 733 (734), mit Blick auf die Genomforschung; zu den Schwierigkeiten, das richtige Ausmaß der Aufklärung zu finden, plastisch Menzel, DuD 2008, 400 (407 f.).

[91] Vgl. Weichert, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 48.

Missbrauch ihrer Daten, indem Gesundheitsdaten in Art. 9 Abs. 1 DS-GVO als besondere Datenkategorie qualifiziert und einem besonders hohem Schutz zugeführt werden. Die Vielzahl der Spezialregelungen stellt den Rechtsanwender im Gesundheitsdatenschutzrecht vor besondere Herausforderungen. Hier zeigt sich die Störanfälligkeit und Dysfunktionalität einer dateneigentumsrechtlichen Regelung besonders deutlich. Der sektorbezogene Kontrollblick verschärft demnach die allgemeinen Bedenken gegen einen solchen Regulierungsansatz.

IV. FAZIT

Die gegenwärtige Rechtsordnung weist Rechte an Daten nach dem jeweiligen Schutzzweck zu. Ein einheitliches Datenrecht kennt die Rechtsordnung nicht. Es würde sich auch nicht in ihre Systematik einfügen. Die Idee einer Dateneigentumsordnung, die in unterschiedlichen Ausprägungen Daten jeweils einem Berechtigten exklusiv die Verfügung darüber zuweisen will, ist daher abzulehnen. Das Problem der gegenwärtigen Rechtslage ist nicht die fehlende materielle Zuweisung von Zugriffsrechten auf Daten oder eine falsche Anreizsetzung, sondern die überbordende Komplexität im datenschutzrechtlichen Regelungsgefüge bei einem gleichzeitig weiten Anwendungsbereich sowie die hohe Breitenwirkung von Normen mit Bezug zur Datenverarbeitung. Ein gesetzgeberischer Handlungsbedarf auf nationaler Ebene besteht dahingehend, diese Komplexität durch eine maßvollere Nutzung der Öffnungsklauseln der DS-GVO zu verringern. In einem weiteren Schritt sollten auf EU-Ebene diese Öffnungsklauseln reduziert werden, um einen vollständig harmonisierten Rechtsrahmen zu erhalten. Neue Rechte an Daten, die diese einzelnen Akteuren in Form eines Ausschließlichkeitsrechts zuweisen, sind unnötig und – auch wegen der dadurch weiter steigenden Komplexität – kontraproduktiv. Die gegenwärtige Rechtslage ist geeignet, die sich stellenden Probleme zu lösen. Das bedingt jedoch eine konsequente Nutzung der gegebenen Möglichkeiten im exekutiven Vollzug insbesondere durch die Datenschutzaufsichts- und Kartellbehörden. Eine Gefahr stellen die sich vor allem bei Plattformdiensten zeigenden Tendenzen zu monopolistischen Strukturen dar. Möglicherweise wird hier abhängig von der weiteren Entwicklung die Normierung von Zugangsrechten durch den Gesetzgeber zweckmäßig werden, um derartige Strukturen aufzubrechen beziehungsweise trotz deren Existenz eine effiziente und gemeinwohlorientierte Datenverarbeitung sicherzustellen. Zuvor sollten allerdings die Möglichkeiten ausgeschöpft werden, die insbesondere das Kartellrecht bietet.

Auf der Basis der gegenwärtigen Rechtsordnung hat durch die rechtlich geschützten tatsächlichen Positionen in erster Linie derjenige Zugriff auf Daten, der eine Datenverarbeitungsanlage betreibt oder herstellt. Das ist auch sachgerecht, denn dort besteht die höchste Wertschöpfungskompetenz. Verbraucher haben bei konsequenter Einhaltung der Vorgaben zur datenschutzrechtlichen Einwilligung und der sonstigen datenschutzrechtlichen Vorgaben auch eine effiziente Möglichkeit zur Kommerzialisierung ihrer Daten und könnten so den ökonomischen Nutzen aus den sie betreffenden Daten ziehen. Um Verbrauchern den Wert ihrer Daten vor Augen zu führen, kann das rechtlich gegebenenfalls gebotene oder andernfalls

freiwillige Angebot von Bezahlmodellen hilfreich sein. Besonders wichtig für die digitale Selbstbestimmung der Verbraucher ist eine hohe Transparenz der Datenverarbeitung und die Einwilligung in diese. Dazu gehört auch, dass Einwilligungen nur für zentrale Fragen nötig sind und alles Weitere vom Gesetzgeber vorgesteuert wird. Bei zu vielen notwendigen Einwilligungen bestünde die Gefahr, die Verbraucher zu überfordern und Einwilligungen entgegen der gesetzgeberischen Intention zur bloßen Formsache zu degradieren. Hier muss die weitere Entwicklung beobachtet werden. Darüber hinaus müssen die Interessen finanzschwächerer Verbrauchergruppen im Auge behalten werden.

Die Betrachtung der beiden Referenzgebiete verschärft die Einwände gegen einen dateneigentumsrechtlichen Regulierungsansatz. Das Beispiel Mobilität zeigt die wachsende Bedeutung von Daten auf, ist gleichzeitig aber auch ein Beispiel für einen an sich funktionierenden gegenwärtigen Rechtsrahmen. Die Zuweisungen von Daten erfolgt gegenwärtig auf der Grundlage rechtlich geschützter tatsächlicher Positionen an die Akteure, die daraus die größtmögliche Wertschöpfung erzielen können. Gleichzeitig werden Verbraucher effektiv vor dem Missbrauch ihrer Daten geschützt und haben auf der Basis des Datenschutzrechts – etwa als Halter oder Fahrer von Fahrzeugen oder als Nutzer sonstiger Mobilitätsdienste – angemessene Gestaltungs- und Verwertungsmöglichkeiten hinsichtlich ihrer Daten. Ein zusätzlicher dateneigentumsrechtlicher Ansatz wäre insoweit eine überflüssige „Störquelle“.

Bei der Verarbeitung von Gesundheitsdaten zeigt sich umgekehrt, dass ein komplexes und wenig zielführendes Datenschutzrechtsregime besteht. Aber auch hier ist ein dateneigentumsrechtlicher Ansatz dysfunktional. Eine dateneigentumsrechtliche „Passepartout“-Regelung ist zudem völlig utopisch, da sich in den komplexen einfachgesetzlichen Strukturen im Gesundheitswesen jeweils auch Regelungen von Zugriffsberechtigungen finden, die mit einer „grobschlächtigen“ Dateneigentumsregelung zwangsläufig kollidieren würden. Umgekehrt ist eine dateneigentumsrechtliche Regelung in all den Spezialnormen noch weniger wünschenswert. Das Referenzgebiet des Gesundheitsdatenschutzrechts in seiner jetzigen – sehr unbefriedigenden – realen Situation zeigt daher besonders deutlich, wie wenig funktionstüchtig und sektorbezogen „abgeklopft“ der Vorschlag einer Dateneigentumsregelung ist.

Conclusion

In the current legal system, the rights for data are determined according to the respective protective purpose. A consistent data law does not exist (in Germany) within the legal system and such a legislation could not be embedded into the current system. The idea of a data ownership, which seeks in variant degrees to assign data exclusively to an entitled person, must be rejected. In the current legal situation, an exuberant complexity within the data protection law´s system of regulations in combination with the wide range of applications and the widespread impact of all norms concerning data processing pose a challenge. The absence of a material allocation of access rights to data and the misguiding incentives are of lesser concern. In order to make the system less complicated, there is a need for the national legislator to make a more moderate use of flexibility clauses within the frame of the General Data Protection Regulation (GDPR). In a second step, it is recommended to reduce the amount of the flexibility clauses on the EU level to create a fully harmonized legal framework. Assigning new rights to data to single actors by the means of exclusive rights are unnecessary and counterproductive, as they also increase the system´s overall complexity. The present legal situation allows for ways to resolve these problems. However, any solution to the current problems requires the resolute use of relevant options by the respective executive organs (especially data protection and competition authorities) in the field. Chiefly those monopolistic tendencies which can be observed in the business field of platform service providers pose a threat. Depending on future trends, the legislator may be advised to introduce new regulations for access rights to break these monopolistic structures, or, alternatively, to balance the monopolies by ensuring data processing which is efficient and oriented towards the common good. Prior to that, all other possible measurements especially those provided by competition law should be used exhaustively.

Based on the present state of the legal system and due to the de facto positions protected by the law, those actors who offer or produce data processing systems have primarily access to data. This is appropriate as these actors command the greatest expertise in value creation in the field. As long as legal requirements for declarations of consent and other relevant data protection law regulations are consistently met, consumers possess opportunities to efficiently commercialize their own private data and to thereby profit economically. To highlight the economic value of their data to the individual consumer, the duty to offer payment models required by law or otherwise on a voluntary basis may be helpful. To provide for the consumers´ digital self-determination, the transparency of data processing

and declarations of consent to data processing is especially important and needs to equivalently high. The consumer´s self-determination should be strengthened by provisions that make declarations of consent necessary only when central issues are concerned. Issues of lesser concern should be governed by the legislator. If declarations of consent are by law required in too many instances, the amount of declarations may overstrain consumers, thereby creating the threat to render declarations of consent mere formalities and thus countering the intention of the legislator. This development needs to be observed. In addition, the interests of financially weaker consumer groups must be kept in mind.

Two reference areas (of data protection law) provide further arguments against a regulatory approach based on data ownership. Mobility as a reference issue highlights the increasing importance of data generally and simultaneously serves as an example for a functioning modern legal framework. In this case data is allocated on the basis of de facto positions protected by law. Presently, those actors process the data which are able to create the greatest value (by using the data). Simultaneously, consumers´ data is effectively protected from abuse. At the same time, the data protection law grants consumers (e.g. keepers / drivers of vehicles or users of other mobility services) appropriate opportunities to design and use their own data. An additional approach based on data ownership would rather be a redundant source of "disturbance."

On the other hand, the way in which health data is processed highlights the existence of a complex and rather disadvantageous data protection regime. Nevertheless, a data ownership approach would be a dysfunctional solution in this case as well. Such a "coarse" or "passe-partout" regulatory approach is unrealistic anyways as it collides with regulations on access rights found in the complex structures of sub-constitutional law within the healthcare sector. Additionally, a data ownership legislation which takes into account all special norms is not desirable. Health data protection law in its current (and rather dissatisfactory) actual state as a reference area for data protection law serves as an example for how proposals for a data ownership regulation are not very functional and have not been tested carefully enough for their applicability to different sectors.