



Telemedicus e.V. · Zur Dornhiede 38 · 48161 Münster

Bundesministerium für Verkehr und digitale Infrastruktur
Invalidenstraße 44
10115 Berlin

Per Mail an: Fachkonsultation-
Datensouveraenitaet@bmvi.bund.de

Telemedicus e.V.
Zur Dornhiede 38
48161 Münster

www.telemedicus.info
s.telle@telemedicus.info

1. November 17

BMVI-Fachkonsultation „Eigentumsordnung“ für Mobilitätsdaten“

Stellungnahme Telemedicus e.V.

Sehr geehrte Damen und Herren,

Telemedicus e.V. bedankt sich für die Gelegenheit zur Stellungnahme im Rahmen der zuvor genannten Fachkonsultation.

A. Über Telemedicus

Telemedicus ist ein juristisches Internetprojekt zu allen Rechtsfragen der Informationsgesellschaft. Im Fokus unserer Arbeit stehen das Informations-, Medien- und Datenschutzrecht, aber auch das Telekommunikations-, Kartell- und Rundfunkrecht sowie die damit verbundenen sozialen, wirtschaftlichen und politischen Fragen. Getragen und herausgegeben wird das Projekt vom gemeinnützigen Telemedicus e.V., einer neutralen, unabhängigen, wissenschaftlichen Vereinigung. Der Verein fördert satzungsgemäß den freien Austausch von Wissen über Rechtsfragen der Informationsgesellschaft auf juristischer und interdisziplinärer Ebene.



B. Stellungnahme

Die nachfolgende Stellungnahme gliedert sich in fünf inhaltliche Teile. Der erste Teil (I.) setzt sich mit der in der Studie aufgeworfenen Definition von Mobilitätsdaten auseinander. Der zweite Teil (II.) befasst sich mit dem in der Studie angesprochenen Aspekt des Datenschutzrechts als Verfügungshemmnis, woran anschließend der dritte Teil (III.) sich mit den Möglichkeiten rechtlicher Verfügungen über Daten *de lege lata* auseinandersetzt. Anschließend nehmen wir Stellung zu dem diskutierten „Eigentumsrecht“ bzw. Ausschließlichkeitsrechten an Daten (IV.) und dem folgend zum Aspekt der Partizipation (V.).

I. Definition von Mobilitätsdaten

In der Studie wird der neuentwickelte Zuordnungsansatz in einen Normtext überführt und Daten als *„beobachtbare Unterschiede, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“* definiert.¹ Dieser Begriff wird gleichzeitig dahingehend erläutert, dass er zum Teil aus § 202a StGB übernommen und mit einer Definition aus dem Bereich der Informatik („beobachtbare Unterschiede“) kombiniert wurde, um die Einheitlichkeit der Rechtsordnung zu gewährleisten. Innerhalb der Studie wird zusätzlich eine technische Klassifizierung dieser Daten in *„statische wie dynamische Fahrzeugdaten, Verkehrsdaten, statische wie dynamische Nutzerdaten und Positionsdaten“* vorgenommen.² Diese technische Klassifizierung der Daten erfolgt laut Studie ohne Einstufung zum Personenbezug im rechtlichen Sinne, welcher erst durch eine Verknüpfung der sachbezogenen Daten zu anderen personenbezogenen Daten besteht.³

Die Unterscheidung nach technischen Klassifikationen erscheint sinnvoll, wobei dabei die juristische Unterscheidung zwischen personenbezogenen und sachbezogenen Daten zur

¹ Studie des BMVI „Eigentumsordnung“ für Mobilitätsdaten“, S. 108.

² Studie des BMVI „Eigentumsordnung“ für Mobilitätsdaten“, S. 19.

³ Studie des BMVI „Eigentumsordnung“ für Mobilitätsdaten“, S. 21



Festlegung des Schutzniveaus nicht vollständig außer Acht gelassen werden darf. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Unter Art. 4 Nr. 1 DSGVO sind es Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Daten, die einen Personenbezug aufweisen, genießen also unmittelbar mit ihrer Entstehung den Schutz des Datenschutzrechts.

Begriffliche Definitionsansätze sollten deshalb unnötige Kollisionen oder gar rechtliche Konkurrenzen vermeiden. Dies gilt auch, soweit relevante Daten jedenfalls teilweise unter gewerbliche Schutzrechte fallen könnten. Die Einführung eines „Dateneigentums“ nur zum Zwecke einer Definition von „Daten“ lehnen wir somit als überflüssig und missverständlich ab. Insbesondere sehen wir die Begründung einer herzustellenden einheitlichen Rechtsordnung nicht als tauglich an. Zwar mag es ein Klarstellungsinteresse an einem einheitlichen Datenbegriff geben. Dieser kann aber aufgrund der jeweiligen gesetzlichen Schutzzwecke vollkommen unterschiedlich sein. Zum Vergleich sei bereits auf die unterschiedlichen Begriffe „Besitz“ im Zivilrecht und „Gewahrsam“ im Strafrecht hingewiesen.

II. Datenschutz ist Grundrechtsschutz – kein Verfügungshemmnis

Das Datenschutzrecht gilt nicht für alle Arten von Daten, sondern findet nur beschränkt Anwendung und ist damit für bestimmte Datenarten überhaupt nicht einschlägig. So gilt es beispielsweise nicht für anonymisierte Daten und auch nicht für Daten von juristischen Personen.⁴ Für solche Arten von Daten, die für die vernetzte Mobilität dennoch eine große Rolle spielen können, stellt das Datenschutzrecht also keinerlei Beschränkungen auf. Damit ist es für durchaus relevante und monetarisierbare Datenarten im Kontext vernetzter Mobilität kein Hindernis und kann nicht als Argument zur Schaffung einer Eigentumsordnung herangezogen werden.

⁴ Erwägungsgründe 14 und 26 der DSGVO.



Auf der anderen Seite steht der Datenschutz durch die steigende Informationsdichte bzw. die unzähligen Möglichkeiten der Informationserlangung vor neuen Herausforderungen. Teilweise ist deshalb die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten in der Praxis angesichts von Big Data-Analysen und der Möglichkeit, durch bestimmte Korrelationen empirische Rückschlüsse auf einzelne Personen zu ziehen, schwierig.⁵ Datenschutzrecht stellt jedoch auch Grundrechtsschutz dar, welcher in der Europäischen Union unabdingbar ist. Gesetzliche Entwicklungen sollten daher bei der Diskussion um die Zuordnung von Daten das aktuelle Datenschutzrecht als wesentlichen Grundbeitrag betrachten und einen fairen Interessenausgleich zwischen der Förderung von innovativen Geschäftsmodellen und der Generierung wirtschaftlicher Werte sowie dem Schutz von persönlichen Daten finden.

Abzulehnen sind deshalb Vorschläge, das Datenschutzrecht lediglich zu einem Belastungsrecht eines möglichen Dateneigentumsrechts zu degradieren, da auf diese Weise ein Wertungswiderspruch zur Bedeutung des Datenschutzes eintreten würde. Der Datenschutz leitet sich aus dem informationellen Selbstbestimmungsrecht ab. Ausfluss dieses Grundrechts ist wiederum das Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO, das nunmehr in der DSGVO als bußgeldbewehrte Pflicht in Art. 83 Abs. 5 lit. a) DSGVO postuliert ist. Sobald personenbezogene Daten für einen bestimmten Zweck nicht erforderlich sind, sind sie entsprechend Art. 17 Abs. 1 lit. a) DSGVO unverzüglich zu löschen. Ein irgendwie geartetes „Eigentumsrecht“ dürfte diese Löschpflicht nicht aushebeln. Die Pflicht zur Löschung würde nämlich mit einem vom Recht auf informationelle Selbstbestimmung unabhängig geltendem „Eigentumsrecht“ kollidieren, da personenbezogene Daten bei Wegfall der Verarbeitungserlaubnis zwingend zu entfernen sind, um einen möglichen Wiedergebrauch bzw. Missbrauch zu verhindern. Die Löschpflicht würde das Eigentum damit aber nicht nur belasten, sondern die rechtliche Eigentumsposition zerstören.

⁵ Drexl, NZKart 2017, S. 415 (416).



III. Ausreichende Verfügungsberechtigung de lege lata

Die DSGVO und ihre Begleitgesetze bieten aus Sicht des Datenschutzes ein hinreichendes Verfügungsregime für die Verarbeitung personenbezogener Daten. Dies betrifft sowohl die Erstverarbeitung nach einer erfolgten Erhebung als auch etwaige weitere Verarbeitungen durch Dritte, an die Daten übermittelt werden. Vom datenschutzrechtlichen Standpunkt her betrachtet bedürfte es deshalb keiner neuer Eigentumsordnung für Mobilitätsdaten, da die ab Mai 2018 geltende Rechtslage einen ausreichenden und ausbalancierten Datenfluss garantiert. Aber auch für nicht-personenbezogene Daten sind bereits mit der geltenden Rechtslage hinreichende Verfügungsberechtigungen vorhanden. Folgende Gründe sind für diese Bewertung ausschlaggebend:

1. Datenschutzrecht ist bereits vom Zweck her auch auf Verfügungen ausgerichtet

Das Datenschutzrecht darf nicht nur als Abwehrrecht der Betroffenen betrachtet werden. Vielmehr hat es schon im Grundsatz den Zweck, Regelungen zur Verwendung von personenbezogenen Daten zu treffen und damit letztlich auch Verfügungen über solche Daten zu ermöglichen. Dies ergibt sich für das neue Datenschutzrecht bereits aus Art. 1 DSGVO. Denn nach Art. 1 Abs. 1 DSGVO schützt die DSGVO nicht nur natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten, sondern auch den freien Verkehr solcher Daten. Damit ist bereits in der DSGVO die Zweckbestimmung angelegt, nicht nur primär Belastungen der Daten mit Persönlichkeitsrechten vorzunehmen, sondern auch Erlaubnisse für die Verarbeitung solcher Daten zu ermöglichen. Dies wird auch so in Art. 1 Abs. 3 DSGVO bestätigt, nach dem der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf. Der Europäische Gesetzgeber hat also die beschränkten Wirkungen des Datenschutzes erkannt und sich für einen ausgeglichenen Datenfluss innerhalb der Europäischen Union ausgesprochen.



2. Datenschutzrecht enthält zahlreiche Verfügungsbefugnisse

Darüber hinaus ist das Datenschutzrecht kein reines Verbotsgesetz, das lediglich Beschränkungen aufstellt. Zwar gilt im Datenschutzrecht der Grundsatz des Verbots mit Erlaubnisvorbehalt, d.h. dass zunächst alles verboten ist, was nicht ausdrücklich im Gesetz erlaubt wurde. Aber genau diese Erlaubnisse sind es, die den Datenschutz zu einem sehr flexiblen Regelwerk bei der Suche nach Verarbeitungsbefugnissen mit personenbezogenen Daten machen. Denn das Datenschutzrecht hat zahlreiche gesetzliche Erlaubnisse zu bieten, von denen auch bei den Mobilitätsdaten problemlos Gebrauch gemacht werden kann. So wäre beispielsweise neben der Einwilligung auch eine vertragliche Abrede mit dem Betroffenen oder das Berufen auf überwiegende berechnete Interessen möglich. Gerade letzterer Erlaubnistatbestand eröffnet dem Anwender viele Möglichkeiten von datenschutzrechtlichen Argumentationsspielräumen. So ist es etwa nach Art. 6 Abs. 1 lit. f) DSGVO möglich, sich sowohl auf die berechtigten Interessen der Stelle, welche die Daten verarbeitet, als auch auf die berechtigten Interessen eines Dritten zu berufen. Werbezwecke sollen ausweislich des Erwägungsgrundes 47 DSGVO bereits qua Gesetz als ein Fall der berechtigten Interessen aufgefasst werden können. Damit erlaubt das Datenschutzrecht unter bestimmten Voraussetzungen Verfügungen über personenbezogene Daten, zu denen nicht nur die eigene Nutzung, sondern auch die Übermittlung an Dritte gehören.

3. Granulare Steuerung der Datenfreigaben möglich

In Zukunft wird auch durch die kommenden gesetzlichen Verpflichtungen, wie beispielsweise das *Privacy by Design* nach Art. 25 Abs. 1 DSGVO oder das *Privacy by Default* nach Art. 25 Abs. 2 DSGVO, eine granulare Steuerung von Datenfreigaben zwingend möglich sein müssen. Des Weiteren stellt Erwägungsgrund 32 der DSGVO klar, dass Einwilligungen für jeden gesonderten Zweck separat eingeholt werden müssen. Damit wird es nicht mehr



ausreichen, eine „Generaleinwilligung“ vom Betroffenen abzuverlangen. Vielmehr muss dieser die Wahl haben können, einzelnen Zwecken zuzustimmen und andere wiederum abzulehnen.

4. Verfügungen über nicht-personenbezogene Daten

Soweit ein Personenbezug nicht vorliegt, unterfallen Daten nicht dem Datenschutzrecht. Dies kann besonders häufig bei maschinengenerierten Daten zutreffen, wenn die Information lediglich Zustände einer Sache oder besondere Umstände beschreibt, ohne dass ein Rückschluss auf eine natürliche Person möglich wäre. In diesen Fällen würde das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt nicht gelten. Verfügungen über diese Daten unterliegen damit dem Grundsatz der Privatautonomie im Rahmen der geltenden Gesetze.⁶ Das bedeutet, dass grundsätzlich zunächst jeglicher Umgang und sämtliche Verfügungen über Daten als erlaubt angesehen werden müssen, wenn und soweit nicht besondere vertragliche oder gesetzliche Verbote oder Einschränkungen gelten. Gesetzliche Einschränkungen der Verfügungsmacht über Daten ergeben sich aus den in der Studie genannten immaterialgüterrechtlichen Regelungen, aber auch aus lauterkeits- und strafrechtlichen Vorschriften. Außerhalb dieser Verbote oder Einschränkungen wirken Vereinbarungen über Daten grundsätzlich nur relativ zwischen den Vertragsparteien.⁷

5. Unsicherheit bei Verfügungen über Daten

In der Praxis besteht aber eine erhebliche Unsicherheit im Zusammenhang mit Verfügungen über Daten, die auch Auslöser der Debatte über ein „Eigentum“ an Daten ist. Zum einen ist dabei häufig nicht klar geregelt, wer in welchem Umfang über Daten verfügen kann. Dies gilt umso mehr für Verfügungen in Ketten und wenn lediglich vertragliche Vereinbarungen über nicht-personenbezogene Daten vorliegen. Zum anderen ist auch unklar, wer in welchem Umfang mit Daten umgehen darf. Dies hat Einfluss auf die Vereinbarungsintentionen bei

⁶ Vgl. dazu auch *Sattler*, in Sassenberg/Faber (Hrsg.), IoT, S. 46.

⁷ Umfassend dazu auch *Sattler*, in Sassenberg/Faber (Hrsg.), IoT, S. 46 ff.



Verträgen über Daten und führt häufig zu intransparenten Regelungen oder den auf S. 14 der Studie genannten „Alles-oder-Nichts-Regelungen“. Derartige Verträge bei Anbietern von Mobilitätsdiensten entsprechen deshalb nicht nur dem häufig unterstellten Datenkraken-Profil, sondern spiegeln die bestehenden Unsicherheiten und Risiken der Unternehmen wider.

Da aber offensichtlich ein erhebliches wirtschaftliches wie auch gesellschaftliches Interesse an der grundsätzlichen privatautonomen Verfügung besteht, ist auch der Anlass für eine dies ermöglichende und absichernde gesetzliche Regelung nachvollziehbar. Gleichwohl müssen diese Regelungen in sich konsistent sein, sodass sie einerseits die Interessen hinreichend abbilden und andererseits nicht in einem Wertungswiderspruch mit geltenden zivilrechtlichen und wettbewerblichen Regelungen stehen. Die in der Studie angesprochenen Mittel des „Datenausweises“ oder von Standardlizenzen könnten geeignete Mittel darstellen, um diese Unsicherheiten zu beseitigen.

IV. Sinn und Zweck der Diskussion zum „Dateneigentum“

Die Diskussion um die Schaffung eines möglichen „Dateneigentums“ wird seit geraumer Zeit in Deutschland und der Europäischen Union geführt. Die Europäische Kommission stellte daher bereits 2015 ihre Strategie für einen digitalen Binnenmarkt für Europa vor, in welcher die aufkommende Informations- und Kommunikationstechnologie als Grundlage aller modernen, innovativen Wirtschaftssysteme angepriesen wird.⁸ Anfang 2017 schloss sich hieran die Mitteilung „Building a European Data Economy“ der EU-Kommission nebst einem umfangreichen Arbeitspapier hier an, das verschiedene Ideen und Vorschläge für rechtliche Rahmenbedingungen im Zusammenhang mit der europäischen Datenwirtschaft unterbreitet.⁹

⁸ Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Strategie für einen digitalen Binnenmarkt in Europa, 06.05.2015, COM (2015), 192 final S. 3, <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52015DC0192&from=EN> (zuletzt abgerufen 15.10.2017).

⁹ Commission, COM(2017) 9 final; Commission, SWD(2017) 2 final.



Verschiedene Faktoren wirken dabei zusammen, die bei der Schaffung eines Ausschließlichkeitsrechts an Daten in Erwägung gezogen werden sollten:

1. Wirtschaftliche Bedeutung der Diskussion

Daten haben sich im Rahmen der Digitalisierung zu einem wichtigen Wirtschaftsgut entwickelt, weshalb sich bereits auch andere Studien und Gutachten mit der Frage beschäftigen, wie Daten als Handelsware rechtlich abgesichert werden können.¹⁰ Die in Daten verfügbaren Informationen über Personen und Sachen führen zur Entwicklung neuer Geschäftsmodelle. Teilweise werden Daten auch als das „Öl des 21. Jahrhunderts“ bezeichnet, was jedoch insofern irreführend erscheint, als dass Daten gerade nicht von einer Knappheit geprägt sind, sondern eher als ein in Massen generiertes Gut erscheinen.¹¹ Sie haben durch Bezüge zu Einzelpersonen und Personengruppen, Gegenständen oder auch bloßen Zuständen im Handel einen erheblichen Wert erhalten, da sie beispielsweise zur Bestimmung möglichen Konsumverhaltens Aussagen treffen oder gleiches beeinflussen können.¹² Derartige wirtschaftliche Werte werden in anderen Bereichen - wie beispielsweise dem Immaterialgüterrecht - mit dem Erhalt von bestimmten Rechten belohnt. Denkbar und diskussionswürdig wäre aufgrund dieser wirtschaftlichen Bedeutung deshalb die Schaffung eines ähnlichen Ausschließlichkeitsrechts als rechtlichem Gegenwert. Dies könnte eine Möglichkeit darstellen, Anreize zur Schaffung weiterer Geschäftsmodelle und Innovationen im digitalen Binnenmarkt zu setzen.

2. Belohnung von Investitionen, Förderung von Innovation

Die Studie erkennt an, dass in der Praxis ein zunehmendes Bedürfnis einer Güterzuordnung in Bezug auf Daten zu beobachten ist und ein Interesse an einer dinglichen Berechtigung daran

¹⁰ Beispielsweise erörtert in der Studie des DIVSI 2016, „Daten als Handelsware“, <https://www.divsi.de/wp-content/uploads/2016/03/Daten-als-Handelsware.pdf> (zuletzt abgerufen am 15.10.2017).

¹¹ Drexler, NZKart 2017, S. 415 (416).

¹² Bisges, MMR 2017, S. 301 (301).



bestünde.¹³ Ob gerade ein Ausschließlichkeitsrecht die interessensgerechte Methode zur Lösung des Problems ist, erscheint fraglich. Dies lässt sich insbesondere im Vergleich zur Entwicklung von Immaterialgüterrechten bezweifeln.

Historisch wurden Immaterialgüterrechte geschaffen, um die Investition in die Erzeugung eines immateriellen Gutes mit wirtschaftlichem Wert zu belohnen, wie die Studie richtig feststellt.¹⁴ Nicht richtig folgert die Studie jedoch, dass Daten heute stets ein Immaterialgut seien und „deren gewachsene Bedeutung mit einem eigenständigen Ausschließlichkeitsrecht zu Gunsten des Investors“¹⁵ belohnt werden müsse. Dieser Rückschluss ist nicht zwingend und bedarf jedenfalls einer erheblichen Rechtfertigung. Hier ist darauf hinzuweisen, dass Daten lediglich „Rohmaterialien“ sind, die noch nicht derart bearbeitet wurden, um in den Schutzbereich eines möglichen Immaterialgüterrechts zu gelangen.¹⁶ Immaterialgüterrechte setzen aber eine schöpferische, technische oder einzigartige Weiterentwicklung eines normalen Gutes voraus. Es ist daher wesentlich, sich mit diesen Ansätzen zur Belohnung der sinnvollen Datengenerierung auseinanderzusetzen und eine alle Interessen berücksichtigende Lösung zu finden, die nicht in der einfachen und voraussichtlich wettbewerbshemmenden Erstellung eines „Eigentumsrechts“ liegt. Dabei könnte eine zugunsten der Einführung eines Immaterialgüterrechts sprechende zu belohnende Investition auch in dem Aufbau der für die Mobilitätsdienste erforderlichen Infrastruktur zu sehen sein.

3. Sachenrechtliche Zweifel an einem „Dateneigentum“

Ein rechtlich eigenständiges „Dateneigentum“ wäre zudem nur schwer mit geltenden sachenrechtlichen Grundsätzen in Einklang zu bringen. So wäre der Grundsatz der Publizität aufgrund der „digitalen Flüchtigkeit“ von Daten nur schwer einhaltbar, ohne dass damit in andere absolute Rechtspositionen wie das Eigentum oder den berechtigten Besitz an einer Sache

¹³ Studie des BMVI „Eigentumsordnung“ für Mobilitätsdaten“, S. 89.

¹⁴ Studie des BMVI „Eigentumsordnung“ für Mobilitätsdaten“, S. 89.

¹⁵ Studie des BMVI „Eigentumsordnung“ für Mobilitätsdaten“, S.90.

¹⁶ *Ensthaler*, NJW 2016, S. 3473 (3474).



eingegriffen würde. Hilfreich könnte es zwar sein, sich zunächst an den tatsächlichen Umständen zu orientieren. Erster Anknüpfungspunkt für die Bewertung einer Inhaberschaft über Daten wird im Zusammenhang mit einem „Dateneigentum“ stets das jeweilige physische Speichermedium sein. Hiernach wird allerdings häufig eine faktische Verfügungsmacht desjenigen anzunehmen sein, der auch der tatsächliche Inhaber der die Daten verarbeitenden Sachen ist, also gegebenenfalls der Anbieter der Mobilitätsdaten als Inhaber von Speichern oder Servern. In vielen Fällen werden eindeutige rechtliche Feststellungen hierzu jedoch nicht möglich sein, insbesondere wenn Daten im Zusammenhang mit der Erbringung von Mobilitätsdiensten nicht nur an einem Ort gehalten, sondern notwendigerweise zur bestimmungsgemäßen Erbringung des Dienstes transferiert werden müssen. Hinzu kommt, dass die Speicherorte für Daten in vernetzten Systemen sehr schnell wechseln können.

Auch sind Daten in der Regel in tatsächlicher Hinsicht nicht rival, schließen sich also gegenseitig nicht aus. Wenn aber bereits in tatsächlicher Hinsicht keine gegenseitige Ausschlussmöglichkeit besteht, erschließt sich auch eine rechtliche Absolutheit nicht. Das gilt vor allem bei personenbezogenen Daten, die auch die in der Studie angesprochene Mehrrelationalität aufweisen. In diesem Fall wären die verschiedenen datenschutzrechtlichen Befugnisse sogar geeignet, gegenseitige Blockaden zu provozieren. Aber auch bei nicht-personenbezogenen Daten lässt sich außerhalb des bestehenden Rechtsrahmens aus spezifischen sachlich bezogenen Schutzregelungen nur schwer ein eigenständiges absolutes Schutzrecht rechtfertigen. Denn ähnlich wie bei den Anforderungen, die an die Einführung eines immaterialgüterrechtlichen Schutzes gestellt werden, besteht in sachenrechtlicher Hinsicht kein Bedürfnis nach einem absoluten Schutz von Daten, soweit dieser nicht bereits durch Datenschutz- oder sektorspezifische Regelungen gewährt wird. Auch hinsichtlich des sachenrechtlichen Spezialitätsgrundsatzes und des Typenzwangs erscheint eine eigenständige sachenrechtsähnliche Regelung über Daten nur schwer ohne Konfliktlagen mit dem geltenden auf physische Sachen ausgerichteten Sachenrecht nachvollziehbar.



4. Wettbewerbsrechtliche Aspekte

Neue digitale Geschäftsmodelle und -ideen werden am laufenden Band entwickelt und vermarktet. Grundsätzlich führt dies zu und zeugt von einem ausgeprägten Wettbewerb, der an sich bereits Anreize zur Innovationsförderung bietet. Gerade jedoch bei auf der Erhebung und Verarbeitung von Datenmengen basierenden Geschäftsmodellen sind von den Beteiligten viele verschiedene rechtliche Vorgaben zu beachten, die in ihrer aktuellen Komplexität bei Marktakteuren abschreckend und somit innovationshindernd wirken können. Eine einheitliche Regelung zur Nutzung der Daten und zur vorrangigen Zuordnung des wirtschaftlichen Gutes „Datum“ könnte somit wettbewerbsfördernd wirken.

Viele Unternehmen haben ein Interesse an international einheitlichen Bestimmungen (z.B. im Datenschutzrecht), um Rechtssicherheit bei der Erhebung, Verarbeitung und Verwendung der Datenmassen zu erlangen. Dies zeigt sich vor allem darin, dass Datenschutzbestimmungen einzelner Länder mittlerweile einen großen Wettbewerbsfaktor innerhalb der Staatengemeinschaft bilden.¹⁷ Eine einheitliche Beantwortung der Frage nach Zuordnung des wirtschaftlichen Wertes könnte damit wettbewerbslich günstig wirken. Insbesondere könnte durch eine neu zu schaffende Regelung verhindert werden, dass sich bestehende Datenmächte verfestigen oder ganz neue Datenmächte geschaffen werden, soweit diese in kartellrechtlich relevanter Weise Marktzutrittsschranken bilden würden und insoweit Monopole begünstigen.¹⁸

Gerade die Vielzahl der beteiligten Akteure zeigt aber auch, dass die Diskussion über Ausschließlichkeitsrechte an Daten vorausschauend Fragen im Zusammenhang mit der Offenhaltung von Märkten an Daten berücksichtigen sollte. So könnten sich unter den engen Voraussetzungen des kartellrechtlichen Missbrauchsverbots marktbeherrschender Stellungen

¹⁷ Studie des DIVSI 2016, „Daten als Handelsware“, S. 10, <https://www.divsi.de/wp-content/uploads/2016/03/Daten-als-Handelsware.pdf> (zuletzt abgerufen am 15.10.2017).

¹⁸ *Drexel/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytè/Wiedemann*, GRUR Int. 2016, S.914 (915), Rn. 29; Kritisch dazu: *Telle*, in: Taeger (Hrsg.), DSRITB 2017, S. 421 (429) m.w.N.; *Telle*, in: Hennemann/Sattler (Hrsg.), Tagungsband Assistententagung Grüner Bereich 2017 [im Erscheinen].



Ansprüche auf Geschäftsabschluss bezüglich der Daten ergeben.¹⁹ Dies erfordert erstens, dass die Zugangsverweigerung die Entwicklung eines weiteren Angebots auf einem nachgelagerten Markt verhindert, zweitens müssen die Daten selbst für diesen nachgelagerten Markt unersetzlich sein, drittens muss diese Zugangsverweigerung effektiven Wettbewerb verhindern und viertens darf keine objektive Rechtfertigung für die Zugangsverweigerung bestehen.²⁰ Hinsichtlich personenbezogener Daten dürfte es aufgrund der beschriebenen Rivalität an einer Exklusivität mangeln. Zudem stellen datenschutzrechtliche Verbote eine auch nicht durch das Kartellrecht übersteuerbare objektive Rechtfertigung für eine Zugangsverweigerung dar.²¹ Hinsichtlich komplexer Datenpools mit Selbstverstärkungs- und Rückkoppelungstendenzen im Zusammenhang mit Netzwerkeffekten dürfte der Nachweis schwer fallen. Jedenfalls bei nicht-personenbezogenen und insbesondere sachbezogenen Daten könnten aber diese engen Voraussetzungen für einen Geschäftsabschlusszwang vorliegen.²² Dieser könnte zu einem Ausschließlichkeitsrecht an den Daten in einem rechtlichen Verhältnis von Einwendungen, Schranken oder sonstigen Gegenrechten stehen. Anzudenken könnte deshalb die Schaffung einer speziellen Regulierung des Zugangs zu Rohdaten sein, um mögliches Marktversagen zu verhindern und Innovation im stetigen Wettbewerb zu fördern.²³

V. Partizipation an der Nutzung der Betroffenenendaten

Wir teilen die Einschätzung nicht, dass Betroffene an der Nutzung ihrer Daten unter dem geltenden Recht nicht partizipieren könnten. So kann beispielsweise mithilfe des Instruments der Einwilligung zwischen Betroffenenem und verantwortlicher Stelle eine Vereinbarung im Sinne von „Geld gegen Daten“ bereits jetzt geschlossen werden. Darüber hinaus wird dies auch

¹⁹ *Telle*, in: Hennemann/Sattler (Hrsg.), Tagungsband Assistententagung Grüner Bereich 2017 [im Erscheinen].

²⁰ *Telle*, in: Taeger (Hrsg.), DSRITB 2017, S. 421 (429); vgl. EuGH, 6.4.1995 - C-241/91 P und C-242/91 P - Magill; EuGH, 26.11.1998 - C-7/97 - Oscar Bronner; EuGH, 29.4.2004 - C-418/01 - IMS Health; EuG, 17.9.2007 - T-201/04 - Microsoft Interoperabilitätsinformationen; EuGH, 16.7.2015 - C-170/13 - Huawei Technologies.

²¹ *Telle*, in: Taeger (Hrsg.), DSRITB 2017, S. 421 (430).

²² *Telle*, in: Taeger (Hrsg.), DSRITB 2017, S. 421 (428); *Telle*, in: Taeger (Hrsg.), DSRITB 2016, S. 835 (841).

²³ *Drexler/Hilty/Desaunettes/Greiner/Kim/Richter/Surblyté/Wiedemann*, GRUR Int. 2016, S. 914 (918).



in Zukunft unter dem neuen Datenschutzrecht möglich sein, da dieses ebenfalls die Abgabe von Einwilligungen im Austausch gegen Leistungen ermöglicht. Ein Beispiel für dieses Geschäftsmodell ist die Mobilfunkmarke Netzclub (<http://www.netzclub.net>). Hier erhält der Vertragspartner einen sogenannten „werbefinanzierten Smartphone-Tarif“. Auf Basis der Einwilligung des Kunden, seine persönlichen Daten für Werbezwecke verwenden zu dürfen, erhält er ein kostenloses Datenvolumen zum Surfen im Internet. In den aktuellen Vertragsbedingungen ist dabei ausdrücklich geregelt, dass sobald die Werbeeinwilligung für Produktwerbung durch Widerruf des Kunden erlischt, dies automatisch zur sofortigen Beendigung des Vertrages führt. Auch in anderen Wirtschaftsbereichen erhalten Betroffene ähnliche Partizipationsmöglichkeiten. Wenn dabei als unbillig empfundene Regeln durch Unternehmen verwendet werden, kann dies bereits jetzt nach geltenden rechtlichen Vorschriften – insbesondere der AGB-Kontrolle sowie dem Wettbewerbsrecht – erfasst werden. Beispiele sind die Unterlassungsklagen des VZBV gegenüber Facebook, Parship oder anderen Plattformanbietern. Soweit dies an einzelnen Stellen nicht ausreichend erscheint, könnte erforderlichenfalls dort nachgebessert werden. Ein „Eigentumsrecht“ an Daten wird jedoch die bestehenden Konflikte an diesen Stellen nicht auflösen.

Darüber hinaus neigt der Einwand fehlender Partizipation in der Debatte zu einer einseitigen Interessenbetrachtung ausschließlich zugunsten der Betroffenen. Dies bildet aber weder die wirtschaftliche Lage ausreichend ab, noch besteht zwingend stets eine Situation fehlender Partizipation im Falle eines bestimmten Geschäftsmodells. Angesichts der Privatautonomie, einer grundsätzlich liberalen Wirtschaftsordnung und dem Bestreben, einen Europäischen Datenmarkt zu schaffen, muss diese Partizipation nicht zwingend in Verbotsrechten oder einer erzwingbaren Monetarisierung gesehen werden. Auch die Nutzungsmöglichkeit eines Dienstes, den es bislang nicht gab, kann einer interessensgerechten Partizipation entsprechen. Gegen das Argument der Partizipation könnte zudem eingewandt werden, dass die Anbieter der Mobilitätsdienste in der Regel ein erhebliches Investitions- und Wettbewerbsrisiko tragen. Viele



dieser Dienste sind als Plattform-Geschäftsmodelle konzipiert. Sie profitieren zwar von gewissen wettbewerblichen Vorteilen wie z.B. Netzwerkeffekten oder Größenvorteilen. Das bedeutet, dass bei einfach skalierbaren Projekten schneller eine Amortisierung der Investitionskosten stattfinden kann. Allerdings sind die Betreiber auf der anderen Seite stark von der Akzeptanz ihres Produktes am Markt abhängig. Damit einher geht das Risiko, dass sich ein Geschäftsmodell möglicherweise nicht durchsetzt und der Betreiber die Kosten nicht amortisieren kann.

VI. Zusammenfassung und Lösungsvorschlag

Angesichts der Fülle der aktuell generierten Datenmengen wird es in Zukunft das wesentliche Ziel sein, Daten an neu zu entwickelnden Wertmaßstäben in verschiedene Kategorien einzuordnen und je nach Schutznotwendigkeit unterschiedlich stark zu schützen.²⁴ Die Diskussion um ein mögliches „Dateneigentumsrecht“ oder eher ein „Datenverfügungsrecht“ muss jedoch im Hinblick auf die unterschiedlichen Interessenslagen geführt werden und insbesondere einen innovations- und wettbewerbsfördernden und gleichzeitig datenschutzbeachtenden Ansatz wählen. Hierbei erscheint uns eine Regelung „entlang“ der derzeitigen Rechtslage zu Daten am ausgewogensten. Diese könnte ähnlich wie eine Regelung über Früchte oder Nutzungen nach den Vorschriften des BGB aussehen, wobei die erwähnten Vorbehalte an einer sachenrechtlichen Lösung gelten.

RA Sebastian Telle

Redakteur und Kernteam-Mitglied bei Telemedicus
Wissenschaftlicher Mitarbeiter am Zentrum Recht der Informationsgesellschaft
an der Carl von Ossietzky Universität Oldenburg

Diana Spikowius

Juristin und Redakteurin bei Telemedicus

RA Boris Reibach, LL.M.

Wissenschaftlicher Mitarbeiter am Zentrum Recht der Informationsgesellschaft
an der Carl von Ossietzky Universität Oldenburg

²⁴ *Ensthaler*, NJW 2016, S. 3473 (3473).