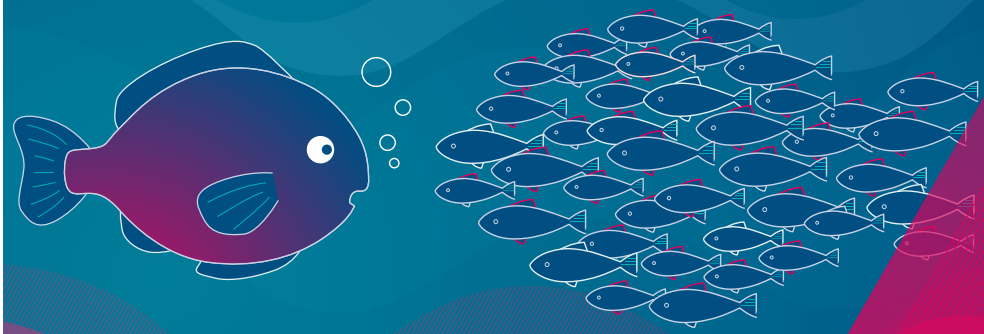
KONRAD ADENAUER STIFTUNG

Designing Data Trustees – A Purpose-Based Approach

Datentreuhänder – Ein problemlösungsorientierter Ansatz

Louisa Specht-Riemenschneider
Wolfgang Kerber



www.kas.de

Impressum

Herausgeberin:
Konrad-Adenauer-Stiftung e. V. 2022, Berlin

Gestaltung und Satz: yellow too, Pasiek Horntrich GbR
Die Printausgabe wurde bei der Druckerei Kern GmbH, Bexbach, klimaneutral produziert und auf FSC-zertifiziertem Papier gedruckt.
Printed in Germany.

Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-039-0

Designing Data Trustees – A Purpose-Based Approach

**Datentreuhänder –
Ein problemlösungsorientierter Ansatz**

Louisa Specht-Riemenschneider
Wolfgang Kerber

Die Autoren

Prof. Dr. Louisa Specht-Riemenschneider ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Informations- und Datenrecht an der Rheinischen Friedrich-Wilhelms-Universität Bonn und Leiterin der Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht (ForTech).

Prof. Dr. Wolfgang Kerber ist Inhaber der Professur für Wirtschaftspolitik an der Philipps-Universität Marburg und Mitglied des Wissenschaftlichen Beirats des Promotionskollegs Soziale Marktwirtschaft der Konrad-Adenauer-Stiftung.

Kontakt:
Pencho Kuzev
Konrad-Adenauer-Stiftung
T +49 30 / 26 996-3247
pencho.kuzev@kas.de

Auf einen Blick

Datentreuhänder und Datenmittler könnten zukünftig eine Schlüsselrolle in der Datenwirtschaft spielen, da sie das Aggregieren und den Austausch erheblicher Mengen einschlägiger Daten erleichtern und dabei gleichzeitig das Potenzial haben, den Schutz kollidierender Rechte und Rechtsgüter sicherzustellen. Es wird gezeigt, dass die jeweils in Betracht kommenden Datentreuhandmodelle völlig unterschiedlich ausgestaltet sein müssen und daher auch eines völlig unterschiedlichen Rechtsrahmens bedürfen, um tatsächlich zur Problemlösung beitragen zu können. In unserer Studie werden verschiedene Probleme in drei verschiedenen Sektoren dargestellt, die unter Einbeziehung von Datentreuhändern gelöst werden können.

Datentreuhänder im Gesundheitssektor

Im Gesundheitssektor stehen wir vor dem Problem der unzureichenden Kombination und Auswertung von Daten für Forschungszwecke. Eine Lösung könnte darin bestehen, die Kombination von Datenbeständen und ihre Verarbeitung zu medizinischen Forschungszwecken in sogenannte Data Clean Rooms, die den höchsten IT-Sicherheitsstandards entsprechen, zuzulassen. Außerdem stellen sie sicher, dass eine Auswertung allein zu Forschungszwecken im Gemeinwohlinteresse stattfindet, und dass die Daten nicht für Dritte zugänglich sind, auch nicht die Datengeber selbst.

Datentreuhänder im Online-Sektor

Im Gegensatz zum Gesundheitssektor existiert im Online-Sektor eine Übernutzung personenbezogener Daten, teilweise unter Verletzung des Datenschutzrechts. Es wird eine Lösung benötigt, die den Nutzern eine bessere Kontrolle über ihre Daten gibt. Personal Information Management Systeme (PIMS) sind diese Lösung. Datentreuhänder in Form von PIMS können die Funktion eines „Einwilligungsassistenten“ übernehmen. PIMS existieren bereits am Markt, aber sie werden nur unzureichend genutzt, weil der Nutzen für die Betroffenen fehlt. Um das zu ändern, brauchen wir Grundsatzentscheidungen, die zu einer Regulierung auf Systemebene führen. Was bedeutet das? Wir brauchen erstens eine Verpflichtung zur Berücksichtigung der Vorgaben, die die PIMS gegen-

über den Datenverarbeitern aufstellen. Erforderlich sind zweitens Interoperabilitätsstandards. Derzeit konzentriert sich der europäische und nationale Gesetzgeber auf die Regelung von Details, insbesondere auf Maßnahmen zur Minimierung der Risiken von PIMS. Diese Maßnahmen zur Risikominimierung sind ebenso erforderlich wie generelle Klarstellungen im datenschutzrechtlichen Rechtsrahmen. Wenn PIMS aber tatsächlich als Problemlösungsoption fungieren können soll, bedarf es zuallererst der angesprochenen Regulierung auf Systemebene. Ohne diese läuft jede Detailregelung Gefahr sinn- und zwecklos zu werden, denn sie wird nicht dazu führen, dass PIMS genutzt werden.

Datentreuhänder im Mobilitätssektor

Auch im Mobilitätssektor können Datentreuhänder ein geeignetes Instrument zur Lösung von Zugangsproblemen in Bezug auf bestimmte Mobilitätsdaten sein. Dort entstehen große Mengen von Daten, die von den Autofahrern durch den Betrieb von vernetzten und automatisierten Fahrzeugen durch eine Vielzahl von Sensoren generiert werden. Diese Daten könnten wiederum von vielen Unternehmen sowie von öffentlichen Institutionen sowie für wissenschaftliche Forschung und damit für Gemeinwohlzwecke genutzt werden.

Es gibt seit Jahren eine intensive Auseinandersetzung um das sogenannte „Extended Vehicle"-Konzept der Autohersteller, mit dem sie die exklusive Kontrolle über diese Daten und über den technischen Zugang zum Fahrzeug ausüben können und damit den Zugang zu dem Ökosystem vernetzten und automatisierten Fahrens kontrollieren (Gatekeeper-Position).

Eine auf einer gesetzlichen Grundlage gegründete Datentreuhand, die diese in den Fahrzeugen generierten Daten unter ihrer Kontrolle hat und sie als „neutrale Instanz" nach gesetzlichen Vorgaben, der Datenwirtschaft sowie öffentlichen Institutionen und der Wissenschaft für Gemeinwohlzwecke zugänglich macht, wäre eine mögliche Lösungsoption. Durch sie würde die Entstehung einer solchen Gatekeeper-Position der Autohersteller präventiv verhindert, wodurch Wettbewerb, Innovationen und die Wahlfreiheit der Autonutzer gesichert werden könnten. Weiterhin könnte mit einer solchen Datentreuhand auch eine

wesentlich bessere Nutzung dieser großen Menge von Mobilitätsdaten erreicht werden (**Daten als Infrastruktur**) als bei einer monopolistischen Kontrolle der Daten durch die Autohersteller. Konkret werden zurzeit noch zwei weitere Datenzugangslösungen zu diesen Mobilitätsdaten diskutiert:

- Regulatorische FRAND (fair, reasonable and non-discriminatory) Zugangslösung: Hierbei handelt es sich um eine strikte Regulierung des Zugangs zu diesen Daten des vernetzten Autos nach sogenannten FRAND-Bedingungen.

- „On-board application"-Plattform: Dabei geht es um die Einführung einer alternativen technischen Lösung, die durch eine standardisierte offene und interoperable Telematiklösung die Möglichkeit eröffnet, dass die Autonutzer selbst die Kontrolle über die von ihnen im Fahrzeug generierten Daten ausüben und anderen Serviceanbietern den Zugang zum vernetzten Fahrzeug ermöglichen können.

Wir sind der Meinung, dass eine Datentreuhandlösung über die Lösung dieses Wettbewerbsproblems hinaus weitere spannende Perspektiven für eine effiziente und an Gemeinwohlzielen orientierte Nutzung dieser zukünftig sehr großen Mengen von Mobilitätsdaten eröffnet.

Inhaltsverzeichnis

1 Einleitung

Datentreuhänder werden als zentrales Element zur Lösung vielfältiger Probleme diskutiert. Schon der Begriff und ihre Abgrenzung von Dateninter-mediären ist jedoch unklar. Die Europäische Datenstrategie beschreibt sie als Werkzeuge und Mittel, um Internetnutzerinnen und -nutzern die Möglichkeit zu bieten, detailliert darüber entscheiden zu können, was mit ihren Daten geschieht. Es handele sich um „neuartige Vermittler im Wirtschaftszweig der personenbezogenen Daten“[1]. Die Europäische Datenstrategie greift damit Gedanken der Datenethikkommission auf. Die Datenethikkommission fasst den Begriff der Datentreuhand eng und versteht darunter Privacy Management Tools und Personal Information Management Systems (PIMS). Sie verbindet mit ihnen sowohl die Chance zur „digitalen Selbstbestimmung“ als auch die Sorge vor „sorgloser Fremdbestimmung“.[2] Auch die deutsche Datenstrategie setzt die Datentreuhand mit dem Begriff des Personal Information Management Systems gleich. In der britischen Rechtsordnung ist dieses Verständnis ebenfalls vorherrschend.[3]

Datentreuhänder werden aber auch in anderen Kontexten erwogen, zum Beispiel im Gesundheitssektor als sogenannte Data Clean Rooms zur Zusammenführung und Auswertung großer Datenbestände. Daten aus automatisiert fahrenden Fahrzeugen werden schon heute im Forschungsdatenzentrum des Kraftfahrtbundesamtes gespeichert, dessen Funktion als Datentreuhand man ebenfalls diskutieren könnte. Eine Datentreuhand ließe sich auch für Mobilitätsdaten aus dem öffentlichen Nahverkehr denken oder für landwirtschaftliche Fahrzeuge, die während des Betriebs Daten, zum Beispiel über die Bodenbeschaffenheit erfassen. Diese Daten sollten nicht allein dem Sensorhersteller oder dem Hersteller des landwirtschaftlichen Fahrzeugs zur Verfügung stehen, sondern über den Datentreuhänder auch anderen Personen, zum Beispiel dem Landwirt, zur Verfügung gestellt werden können.[4]

Es ist nicht nötig, die Datentreuhand ausgehend von den verschiedenen Treuhandbegriffen der mitgliedstaatlichen Rechtsordnungen zu definieren oder zu analysieren. Für eine adäquate Regulierung ist ein solches Vorgehen nicht erforderlich. Erforderlich ist es vielmehr, phänomeno-

logisch zu verstehen, wofür Instrumente, die als Datentreuhand bezeichnet werden, entwickelt werden sollen und über welche Eigenschaften sie dafür verfügen müssen. Die Abgrenzung zwischen Datentreuhand und Datenintermediär kann zu diesem Zweck allein in der Bindung des Datenverarbeiters im Innenverhältnis zu den Interessen des Datengebers liegen. Ein Treuhänder hat sein Handeln an den Interessen der anderen Vertragspartei auszurichten. Seine eigenen Interessen hat er nötigenfalls zurückzustellen.[5] Der Datenintermediär ist dagegen im Innenverhältnis nicht derart gebunden. Damit ist der Datenintermediär der Oberbegriff, die Datentreuhand eine Unterform, die wiederum ihrerseits verschiedentlich ausgestaltet werden kann. Dieses Verständnis zugrunde gelegt, sind Personal Information Management Systems (PIMS) nur eine mögliche Form der Datentreuhand. Auch ein Daten-Escrow in Analogie zum Software-Escrow unterliegt beispielsweise einer treuhänderischen Bindung.[6] Hier können kryptografische Schlüssel (Keys) hinterlegt werden, die autorisierten Dritten den Zugriff auf die verschlüsselten Informationen erlauben.[7]

Potenziell können Datentreuhänder damit eine ganz erhebliche Funktionsbreite aufweisen, die es schwierig macht, einen passenden Rechtsrahmen für Datentreuhänder zu entwickeln. Dieses Gutachten regt an, je nach konkreter Problemlage, für deren Lösung Datentreuhandmodelle herangezogen werden, einen problemlösungsorientierten Rechtsrahmen auszugestalten.

Für eine solche problemlösungsorientierte Ausgestaltung von Datentreuhändern ist eine sorgfältige Analyse der zu lösenden Probleme in Bezug auf die Governance von Daten notwendig. Es stellt sich die Frage, ob eine Datentreuhandlösung geeignet ist, um diese Probleme zu lösen, und wie diese ausgehend von den konkreten technologischen und ökonomischen Bedingungen ausgestaltet werden muss. Zu unterscheiden ist zwischen Datentreuhändern, die durch freie Vereinbarungen beispielsweise zwischen Unternehmen zustandekommen, um gezielt komplexe Data-Governance-Probleme in einer Gruppe von Unternehmen zu lösen. Sowie solchen Datentreuhändern, die Teil von regulatorischen Lösungen des Staates sind, um Marktversagensprobleme, beispielsweise aufgrund von Marktmacht oder Informationsasymmetrieproblemen, zu lösen,

oder andere Gemeinwohlziele zu erreichen, wie die wissenschaftliche Forschung im Medizinbereich. Erkennt man an, dass Datentreuhänder Problemlösungsinstrumente sind, stellt sich immer auch die Frage, ob eine datentreuhänderische Lösung besser geeignet ist als andere mögliche Lösungen. Je nach Problem und konkretem Kontext kann diese Frage unterschiedlich beantwortet werden. Oft erweist es sich, dass eine reine datentreuhänderische Lösung nicht ausreicht, etwa zur Lösung von Wettbewerbsproblemen, und deshalb auch andere Maßnahmen, wie komplementäre Regulierungen zur Lösung von Datenzugangs- und Interoperabilitätsproblemen oder zur Gewährleistung hoher Sicherheit, erforderlich sind, damit es tatsächlich zu einer effektiven Problemlösung kommen kann. Insofern kann eine Datentreuhand auch ein Baustein innerhalb einer komplexen Regulierungslösung für ein bestimmtes Problem sein, die entsprechend in die Gesamtlösung einzupassen ist.[8]

Aus der Vielgestaltigkeit der Datentreuhandlösungen folgt bereits, dass auch die rechtlichen Rahmenbedingungen für solche Datentreuhänder nicht als „One Size Fits All"-Lösung ausfallen dürfen. Ursprünglich sollte der Data Governance Act nur anwendbar sein, wenn er ein Datenteilen auf freiwilliger Grundlage ermöglicht, nicht wenn er als Instrument zur Befriedigung gesetzlich vorgegebener Datenzugangsansprüche verwendet wird.[9] Die ist im Ratsentwurf des Data Governance Acts vom 7. September 2021 allerdings explizit aufgehoben. Auch eine verpflichtende Datenzugangsmittelung als Aufgabe einer Datentreuhand wird gemäß Art. 2 Nr. 7 DGA-E nun erfasst.

Sektorspezifische Regulierung für Datentreuhänder ließe sich entsprechend den von der Kommission angekündigten Datenräumen ausgestalten.[10] Diskutiert werden Datentreuhandmodelle derzeit insbesondere im Gesundheits-[11] und Mobilitätsbereich[12] sowie als Personal Information Management System (PIMS)[13]. Der European Health Data Space Act sowie die Ausgestaltung eines Mobilitätsdatenraumes bieten die Möglichkeit für einen funktionsfähigen Rechtsrahmen sektorspezifischer Datentreuhandmodelle. Die europäische Datenstrategie spricht außerdem davon, „persönliche Datenräume" ausgestalten zu wollen, mit deren Hilfe Einzelne detailliert darüber entscheiden können sollen, was mit ihren Daten geschieht und damit eine verbesserte Kontrolle über

ihre Daten ausüben können sollen.[14] Die europäische Kommission stellt in Aussicht, diese Instrumente, mit denen PIMS gemeint sein dürften, im Data Act zu gewährleisten, der für das vierte Quartal 2021 angekündigt war, nun aber auf das erste Quartal 2022 verschoben wurde.[15]

Am Beispiel der drei zur Ausgestaltung in den entsprechend von der Kommission angekündigten Datenräumen anstehenden Datentreuhandmodellen (Datentreuhandmodelle im Gesundheitssektor, im Mobilitätssektor sowie als PIMS) soll im Rahmen dieser Untersuchung Folgendes gezeigt werden:

a. Welche Probleme mit den entsprechenden Datentreuhandmodellen gelöst werden können;

b. wie ein Datentreuhänder funktional ausgestaltet werden müsste, um die identifizierten Probleme zu lösen;

c. welcher Rechtsrahmen hierfür jeweils erforderlich ist; und

d. ob und inwieweit der Data Governance Act und die gegebenenfalls nationale Gesetzgebung zur Problemlösung beitragen.

1 Europäische Datenstrategie, S. 12.
2 Gutachten Datenethikkommission, Oktober 2019, S. 133, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am: 18.11.2021).
3 Delacroix/Lawrence, International Data Privacy Law, 2019, S. 236 ff.
4 Vgl. z. B. Zech, CR 2015, S. 137.
5 Martinek/Omlor, in: Staudinger, BGB, 2017, Vorb. zu § 662 Rn. 26; vgl. auch Specht-Riemenschneider/Blankertz et al., MMR-Beil, 2021, S. 25 u. 34.
6 Eingehend zum Software-Escrow Auer-Reinsdorff/Kast/Dessler, in: Auer-Reinsdorff/Conrad, *Handbuch IT- und Datenschutzrecht*, 3. Aufl. 2019, § 38 IT in der Insolvenz, Escrow Rn. 58–105.
7 Vgl. etwa: https://www.deposix-software-escrow.de/zugangsschluessel-key-escrow (zuletzt abgerufen am 18.11.2021).
8 Vgl. aus ökonomischer Sicht zu Datentreuhandlösungen als Element in Datengovernance-Systemen Kerber, in: Drexl, *Data Access, Consumer Interests and Public Welfare*, 2021, S. 468–471.
9 So zutreffend: Richter, ZEuP 2021, S. 634 u. S. 666.
10 COM (2020) 66 final.
11 Vgl. etwa Martini/Hohmann, NJW 2020, 3573 (3575).
12 Steinrötter, ZD 2021, S. 513 u. S. 516.
13 Wendehorst/Schwamberger/Grinzinger, in: Pertot (Hrsg.), *Rechte an Daten*, 2020, S. 105; Gutachten Datenethikkommission, Oktober 2019, S. 133, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am 18.11.2021); Golland, NJW 2021, S. 2238; Sesing, MMR 2021, S. 544.
14 Europäische Datenstrategie, S. 23.
15 Ebd.

2 Gang der Untersuchung

Im Folgenden sollen zunächst die Grundmodelle der tatsächlichen Ausgestaltungsoptionen von Datentreuhändern aufgezeigt werden (3), die jeweils verschiedene Chancen und Risiken mit sich bringen. Diese Grundmodellierung ist unabhängig von den spezifischen Funktionen, die Datentreuhänder über die Mittelung von Daten- und Datenanalysezugang hinaus übernehmen können (zum Beispiel Anonymisierung, Pseudonymisierung, Datenauswertung et cetera). Anschließend werden die Ziele und Vorgaben des Data Governance Acts skizziert (4), um anschließend – gewissermaßen spiegelbildlich dazu – einen problemlösungsbasierten Rechtsrahmen (5) für PIMS (5.1), Datentreuhänder im Gesundheitssektor (5.2) und Datentreuhänder im Mobilitätssektor (5.3) zu entwickeln. Die Untersuchung schließt mit einer Zusammenfassung der Ergebnisse in rechtspolitischen Handlungsempfehlungen ab (6).

3 Kategorisierung von Datentreuhandmodellen

Versteht man die Datentreuhand, wie es hier zugrunde gelegt wird, als natürliche oder juristische Person oder eine Personengesellschaft, die den Zugang zu von Datentreugebern bereitgestellten oder bereitgehaltenen Daten oder Datenanalyseergebnissen nach vertraglich vereinbarten oder gesetzlich vorgegebenen Data-Governance-Regelungen im Fremdinteresse mittelt, lassen sich die Ausgestaltungsmöglichkeiten von Datentreuhandmodellen in vier Grundformen denken. Diese unterscheiden sich nach der Art der Datenspeicherung (zentral oder dezentral) sowie nach der Art ihrer Inanspruchnahme (obligatorisch oder fakultativ).[16] Darüber hinaus müssen Datentreuhänder auch danach unterschieden werden, ob sie privatwirtschaftlich oder vonseiten des Staates angeboten werden. Unabhängig von dieser Basismodellierung können Datentreuhänder eine Vielzahl weiterer Funktionen wahrnehmen. Sie könnten beispielsweise die Funktion einer Anonymisierung oder Pseudonymisierung der Daten vornehmen oder die Daten anderweitig aufbereiten. Ebendies gilt für etwaige Befugnisse, Metadaten zu erstellen und/oder zu nutzen.[17]

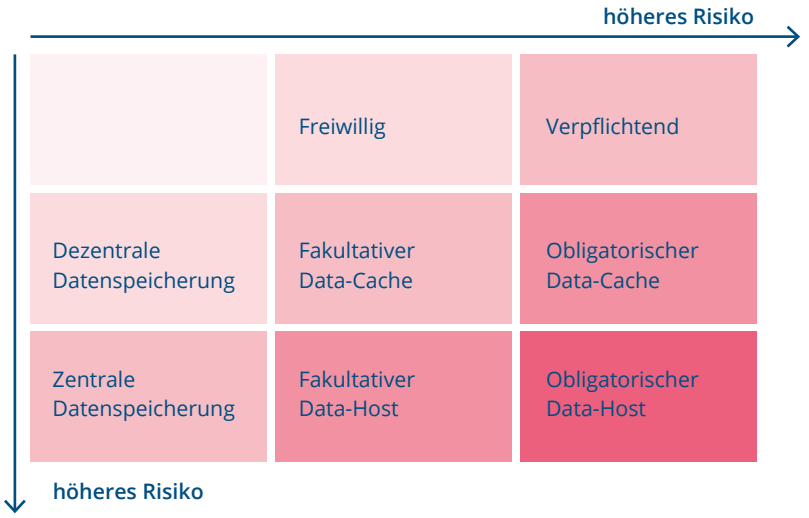
Die dezentrale Speicherung hat für Dateninhaberinnen und Dateninhaber den Vorteil, dass sie die technische Kontrolle über die Daten behalten. Die zentrale Speicherung beim Datentreuhänder verspricht eine einfachere, standardisierte Verwaltung der Daten durch den Datentreuhänder. Gegen die zentrale Speicherung beim Datentreuhänder sprechen in der Regel datenschutzrechtliche Gründe sowie Sicherheitserwägungen. Wenn sich eine große Menge an Daten bei einem Datentreuhänder sammelt, erhöht dies das Missbrauchsrisiko. Zudem ist bei Angriffen gegen den Intermediär der potenzielle Schaden höher. Es kann jedoch mitunter geboten sein, Daten zentral bei einem Datentreuhänder zu speichern, um etwa den Datenverarbeiter vom Zugang auszuschließen, wie dies bei der Microsoft Cloud der Fall war.[18] Möglich ist auch eine kombinierte Lösung, in der die Daten temporär und verschlüsselt zusammengeführt, in der sicheren Sphäre des Datentreu-

händers verarbeitet und anschließend wieder gelöscht werden, wie dies in den Data Clean Rooms verschiedener junger Unternehmen der Fall ist.[19]

Der Einsatz fakultativer Datentreuhandmodelle beruht auf der freien Willensentscheidung der Beteiligten, insbesondere der Betroffenen oder der technisch-faktischen Dateninhaberinnen und -inhaber. Die Parteien schließen in diesem Zuge einen Datentreuhandvertrag, der Grundlage dieses Rechtsverhältnisses wird. Obligatorische Datentreuhandmodelle zeichnen sich dagegen dadurch aus, dass technisch-faktische Dateninhaberinnen und -inhaber gesetzlich verpflichtet werden, die Datentreuhandmodelle in bestimmten Verarbeitungssituationen zu nutzen oder ihre Daten insgesamt in die Datentreuhand auszulagern. Letzteres kann eine wichtige Lösungsoption gerade für solche Fälle sein, in denen die technisch-faktischen Dateninhaberinnen und -inhaber nicht die (einzig) legitimen Dateninhaberinnen und -inhaber sind.[20]

Freiwillige Modelle sind zum Beispiel denkbar für die in der Datenstrategie der Bundesregierung angedachte staatliche Agrardatenplattform, bei Biodatenbanken, für das Teilen von Krankenhausdaten zu Forschungszwecken oder auch zur Schaffung eines Circular Data Space für digitale Produktpässe.[21] Obligatorische Datentreuhandlösungen können für eine oder mehrere Seiten verpflichtend in ihrer Nutzung gemacht werden. Denkbar wäre zum Beispiel eine gesetzliche Pflicht zur Kooperation mit PIMS für Unternehmen, sodass Betroffene Datenverarbeitende dazu anhalten können, Zugang zu Daten, die über die zur Bereitstellung eines Dienstes hinausgehen, über einen PIMS abzufragen. Ein obligatorischer Data Host ist, sofern er über Treubindungen zum Datengeber verpflichtet würde, zum Beispiel Geschäftsgeheimnisse zu wahren, auch das Forschungsdatenzentrum des Kraftfahrtbundesamtes, in dem Daten aus dem automatisierten Auto gespeichert und von dort aus beispielsweise der Forschung zugänglich gemacht werden.

Abbildung 1:



nach Specht/Blankertz et al.[22]

16 Specht-Riemenschneider/Blankertz et al., MMR-Beil, 2021, S. 25.

17 Vgl. zum Begriff der Metadaten Martini, in: Paal/Pauly, 3. Aufl. 2021, DSGVO Art. 30 Rn. 11.

18 Wendehorst/Schwamberger/Grinzinger, in: Pertot (Hrsg.), *Rechte an Daten*, 2020, S. 110.

19 So z. B. Apheris, www.apheris.com und Decentriq, www.decentriq.com. Vgl. dazu auch Specht-Riemenschneider/Radbruch, *Deutsches Ärzteblatt*, Heft 27/28 in 2021, online unter https://www.aerzteblatt.de/archiv/220270/Datennutzung-und-schutz-in-der-Medizin-Forschung-braucht-Daten (zuletzt abgerufen am 18.11.2021); vgl. auch Specht-Riemenschneider/Blankertz et al., MMR-Beil, 2021, S. 25 u. 29 f.

20 Vgl. zu alledem Specht-Riemenschneider/Blankertz et al., MMR-Beil, 2021, S. 25 u. 29 f.

21 Ebd., S. 25 u. 30. Ähnlich Bundesdruckerei, *Der Datentreuhänder*, November 2019, S. 2, online unter: https://www.bundesdruckerei.de/system/files/dokumente/pdf/BDR.de_Datentreuhaender.pdf (zuletzt abgerufen am 18.11.2021).

22 Specht/Blankertz et al., MMR-Beil, 2021, S. 25 u. 32.

4 Vorgaben des Data Governance Acts für Datentreuhänder

Am 25. November 2020 hat die Europäische Kommission ihren Vorschlag für eine Verordnung über europäische Data Governance, (Entwurf des Data Governance Acts, DGA-E), vorgelegt,[23] die einen harmonisierten Rahmen für den Datenaustausch innerhalb der EU schaffen und dadurch die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt verbessern soll (ErwG. 3 f. DGA-E). Datenteilen ist für die Kommission ein wichtiger Faktor zur gesamtgesellschaftlichen Wohlfahrtssteigerung, was auf der Annahme beruht, dass ein verbesserter Datenzugang zu gesteigerter Innovation führt.[24] Es handelt sich um eine horizontale Regelung (ErwG. 3 DGA-E), die jedoch lediglich Mindestvorgaben festlegt und damit durch sektorspezifische Regelungen, zum Beispiel im European Health Data Space, in Regelungen für einen Mobilitätsdatenraum oder für einen persönlichen Datenraum ergänzt werden kann (Art. 1 Abs. 2 DGA-E).[25] Seine insgesamt 35 Artikel sind in acht Kapitel aufgeteilt, die teilweise eher materielle, teilweise eher Verfahrensvorgaben enthalten. Für Datentreuhänder sind dies die folgenden Regelungen:

4.1 Datentreuhänder in staatlicher Trägerschaft

Im zweiten Kapitel des Data Governance Acts wird die Weiterverwendung bestimmter Kategorien von Daten des öffentlichen Sektors geregelt, an denen Rechte Dritter bestehen. Welche Datenkategorien erfasst sind, ist Art. 3 DGA-E zu entnehmen: Positiv werden darin im Zugriff öffentlicher Stellen befindliche Daten genannt, die aus Gründen der geschäftlichen oder statistischen Geheimhaltung geschützt sind oder dem Schutz des geistigen Eigentums oder des Datenschutzes unterliegen (Art. 3 Abs. 1 DGA-E). Hierzu können auch Daten gehören, die bei einem Treuhänder gespeichert sind oder durch diesen vermittelt werden, zum Beispiel Daten aus den Krebsregistern der Länder. Es wird klargestellt, dass die Regelungen des DGA-E die öffentlichen Stellen nicht verpflichten, die Weiterverwendung von Daten zu erlauben und dass diese Regelungen auch bestehende Geheimhaltungspflichten der öffentlichen Stellen nicht berühren (Art. 3 Abs. 3 S. 1 DGA-E). Gestatten öffentliche Stellen die Weiterverwendung von Daten jedoch, müssen sie die Anforderungen des Kapitels II DGA-E einhalten. Entsprechende Abreden dürfen danach grundsätzlich nicht zur Gewährung ausschließlicher Rechte führen (Art. 4 Abs. 1 DGA-E). Nur in Ausnahmefällen kann eine solche Ausschließlichkeitsvereinbarung getroffen werden, die den in Art. 4 Abs. 2–6 DGA-E aufgestellten Anforderungen genügen muss. Dies dient dazu, die Vorgaben des (öffentlichen) Wirtschaftsrechts einzuhalten (ErwG. 9 DGA-E). Art. 5 regelt sodann sowohl die inhaltlichen Anforderungen an die Bedingungen, die öffentliche Stellen für den Zugang zur Weiterverwendung von Daten aufstellen dürfen (siehe insbesondere Art. 5 Abs. 2–5 DGA-E), als auch deren verpflichtende öffentliche Zugänglichmachung (Art. 5 Abs. 1 DGA-E). Nähere Vorgaben finden sich darin auch mit Blick auf den Schutz der Rechte des geistigen Eigentums und sensibler Geschäftsdaten, insbesondere bei einer Weiterverwendung der Daten in einem Drittland (Art. 5 Abs. 7–13 DGA-E). Welche Gebühren öffentliche Stellen für die Weiterverwendung der Daten ansetzen dürfen, regelt Art. 6 DGA-E. Um Anreize für die Weiterverwendung der Daten in Forschung und Innovation zu schaffen, steht es ihnen danach frei, keine oder nur niedrige Gebühren zu verlangen (ErwG. 20 DGA-E). Einen Anreiz zur Weiterverwendung soll auch die nach Art. 7 Abs. 1 DGA-E verpflichtende, sektorübergreifende Einrichtung zuständiger Stellen in den Mitgliedstaaten darstellen, die öffentliche Stellen bei der Zugangsgewährung unterstützen (vgl. dazu Art. 7 Abs. 2 DGA-E; ErwG. 21. DGA-E). Zu diesem Zweck sollen sie ihnen insbesondere moderne Technik zur Verfügung stellen (ErwG. 21 DGA-E). Sie sollen gegebenenfalls auch selbst tätig werden dürfen, um Zugang zur Weiterverwendung zu gewähren (Art. 7 Abs. 3 DGA-E). Das Verfahren, in dem dieser Zugang beantragt werden kann, schreibt Art. 8 DGA-E vor: Es muss eine zentrale Informationsstelle eingerichtet werden, die über die Bedingungen des Zugangs einschließlich der Gebühren informiert und entsprechende Anträge entgegennimmt und an die zuständigen öffentlichen Stellen weiterleitet (Art. 8 Abs. 1, 2 DGA-E). Diese Anträge müssen innerhalb einer angemessenen Frist von maximal zwei Monaten bearbeitet werden (Art. 8 Abs. 3 DGA-E). Gegen die Entscheidung hierüber steht den Betroffenen ein Recht auf einen wirksamen gerichtlichen Rechtsbehelf zu (Art. 8 Abs. 4 DGA-E).

4.2 Datentreuhänder in privater Trägerschaft

Das dritte Kapitel des DGA-E schafft einen Rechtsrahmen für Dienste für die gemeinsame Datennutzung, die sogenannten Datenintermediäre. Ziel ist es, die Verfügbarkeit und Nutzbarkeit von Daten zu fördern. Geschaffen werden soll ein „Europäisches Datenaustauschmodell mit vertrauenswürdigen Datenintermediären für die B2B Datennutzung und für persönliche Datenräume“[26]. Es wird davon ausgegangen, dass Datenverfügbarkeit wirtschaftlich erforderlich ist und dass fehlendes Datenteilen im privaten Sektor im Wesentlichen auf fehlendes Vertrauen in die Nutzung von Datenintermediären zurückzuführen sei.[27] Außerdem soll eine verbesserte Kontrolle über den Zugang zu Daten und ihrer Nutzung im Einklang mit dem Unionsrecht hergestellt werden. Ausgehend von diesem Ziel verpflichtet der Data Governance in Kapitel 2 „Dienste zur gemeinsamen Datennutzung“ im Wesentlichen auf zusätzliche Vorgaben, deren Einhaltung das Vertrauen in die Nutzung der Dienste stärken soll.

4.2.1 Adressierte Datenintermediäre

Adressiert werden zunächst allein Anbieter von Diensten für die gemeinsame Datennutzung, deren Hauptziel in der Herstellung einer geschäftlichen, rechtlichen und möglicherweise auch technischen Beziehung zwischen den Dateninhaberinnen und -inhabern (einschließlich betroffener Personen einerseits, und möglichen Nutzerinnen und Nutzern andererseits) sowie darin besteht, die Parteien bei der Transaktion von Datenbeständen zwischen beiden zu unterstützen. Außerdem ist es erforderlich, dass der angebotene Dienst auf die Vermittlung zwischen einer unbestimmten Zahl von Dateninhaberinnen und -inhabern sowie Datennutzerinnen und -nutzern abzielt, nicht aber auf Dienste für die gemeinsame Datennutzung, die für eine geschlossene Gruppe von Dateninhaberinnen und -inhabern sowie Datennutzerinnen und -nutzern gedacht sind. Nicht erfasst sind außerdem Dienste, die Daten von Dateninhaberinnen und -inhabern einholen, sie aggregieren, anreichern und umwandeln und Lizenzen für die sich daraus ergebenden Daten an Datennutzerinnen und -nutzern vergeben, ohne dabei eine direkte Beziehung zwischen Dateninhaberinnen und -inhabern sowie Datennutzerinnen und -nutzern herzustellen (ErwG. 22). Anbieter, die ohne Erwerbszweck auf Basis des Datenaltruismus tätig werden, werden in Art. 14 DGA-E aber wieder aus dem Anwendungsbereich des Kapitels III ausgenommen.

Erfasst werden also von Kapitel II Plattformen für den Datenaustausch (ErwG. 22), wie zum Beispiel die Datenaustauschplattform Skywise von Airbus, PIMS (ErwG. 23) und Datengenossenschaften (ErwG. 24). In Kapitel III werden außerdem datenaltruistische Organisationen als besondere Datenintermediäre adressiert, die Daten zu Zwecken von allgemeinem Interesse auf Grundlage des Datenaltruismus zur Verfügung stellen.

4.2.2 Anforderungen des Data Governance Acts

Wer Dienste für die gemeinsame Datennutzung im Sinne des Art. 9 Abs. 1 DGA-E erbringen will, muss sich zunächst einem Anmeldeverfahren unterziehen (Art. 10 Abs. 1 DGA-E), das in Art. 10 Abs. 6–10 DGA-E näher ausgestaltet wird. Eine Zulassung der zuständigen Behörde ist jedoch nicht nötig (ErwG. 30 DGA-E); sie bestätigt gegebenenfalls nur die Anmeldung (Art. 10 Abs. 7 DGA-E). Für die Durchführung des Anmeldeverfahrens wurde eine „One Stop Shop“-Lösung gewählt, bei der Datenintermediäre nur der Zuständigkeit desjenigen Mitgliedstaates unterliegen, in dem sie ihre Hauptniederlassung haben beziehungsweise ihr gesetzlicher Vertreter niedergelassen ist (Art. 10 Abs. 2, 3 DGA-E). Die Anmeldung berechtigt den Datenintermediär sodann in der gesamten EU zur Erbringung seiner Dienste nach den in Art. 11 DGA-E vorgegebenen Bedingungen (Art. 10 Abs. 4, 5 DGA-E). Diese Bedingungen sind im Wesentlichen für die drei sehr unterschiedlichen Datenintermediäre in Kapitel II identisch (mit Ausnahme der zusätzlichen Vorgaben für PIMS, siehe unten):

- Neutralitätsvorgaben: Dienste sollen allein als Intermediär tätig werden und die Daten nicht für andere Zwecke verwenden;
- die Metadaten dürfen ausschließlich für die Weiterentwicklung des Dienstes verwendet werden;
- strukturelle Trennung zwischen dem Dienst für die gemeinsame Datennutzung und allen anderen erbrachten Diensten, um Interessenkonflikte zu vermeiden (Verbot vertikaler Integration);

- transparenter und nicht diskriminierender Zugang zum Dienst;
- Anforderungen an Datenformate;
- Bereithaltung von Verfahren, um betrügerische oder missbräuchliche Praktiken in Bezug auf den Zugang zu Daten zu verhindern;
- Ergreifung angemessener technischer, organisatorischer und rechtlicher Maßnahmen, um einen rechtswidrigen Zugang und eine rechtswidrige Übertragung personenbezogener Daten zu verhindern;
- Gewährleistung eines hohen Sicherheitsniveaus bei der Speicherung und Übermittlung nicht personenbezogener Daten;
- Niederlassungspflicht in der EU;
- Anmeldeverfahren;
- Treuhänderische Pflichten für PIMS.

Art. 12 Abs. 1 DGA-E verpflichtet die Mitgliedstaaten zuletzt, hierfür zuständige Behörden zu bestimmen. Die Überwachungs- und Aufsichtsbefugnisse dieser Behörden legt Art. 13 DGA-E fest. Insbesondere können sie Maßnahmen wie abschreckende Geldstrafen verhängen, um auf die Einhaltung der Vorgaben des DGA-E für Datenintermediäre hinzuwirken (Art. 13 Abs. 4 S. 2 lit. a) DGA-E).

4.3 Datenaltruistische Organisationen

Im vierten Kapitel wird ein Rechtsrahmen für den Datenaltruismus geschaffen, der dazu beitragen soll, bei Dateninhaberinnen und -inhabern das für das freiwillige Teilen ihrer Daten nötige Vertrauen zu schaffen (ErwG. 36 DGA-E). Dadurch soll zur Entstehung so großer Datenbestände in der EU beigetragen werden, dass Datenanalysen und maschinelles Lernen möglich werden (ErwG. 35 DGA-E). Auf nationaler wie auf EU-Ebene soll mit diesem Ziel nach Art. 15 DGA-E ein Register der anerkannten datenaltruistischen Organisationen geführt werden. Jene Organisationen sollen sowohl Daten direkt bei den Betroffenen sammeln als auch von Dritten gesammelte Daten verarbeiten dürfen (ErwG. 38 DGA-E). Die Anforderungen, die eine Institution erfüllen muss, um in das Register eingetragen zu werden, legt Art. 16 DGA-E fest. Sie muss insbesondere ohne Erwerbszweck tätig sein (Art. 16 lit. b) DGA-E). Voraussetzungen und Verfahren der Eintragung regelt Art. 17 DGA-E. Auch für diese Eintragung wird darin ein „One Stop Shop"-Ansatz gewählt (Art. 17 Abs. 2, 3 DGA-E). Anerkannte datenaltruistische Organisationen sind im Interesse der Transparenz verpflichtet, laufend gewisse Informationen aufzuzeichnen, etwa über die Personen, die in ihrem Besitz befindliche Daten verarbeiten konnten (Art. 18 Abs. 1 DGA-E). Auch müssen sie einen jährlichen Tätigkeitsbericht verfassen (Art. 18 Abs. 2 DGA-E). Mitteln sie personenbezogene Daten, erlegt ihnen Art. 19 DGA-E zusätzliche Pflichten zu deren Schutz auf. Sie müssen zum Beispiel sicherstellen, dass die Datenverarbeitung nur zu den Zwecken erfolgt, zu denen ihnen die Daten bereitgestellt wurden (Art. 19 Abs. 2 DGA-E). Zuletzt verpflichtet Art. 20 DGA-E die Mitgliedstaaten zur Benennung der hierfür zuständigen Behörden. Ihre Überwachungs- und Aufsichtsbefugnisse werden in Art. 21 DGA-E geregelt. Insbesondere können Verstöße einer anerkannten datenaltruistischen Organisation gegen die Verordnung zu ihrer Streichung aus dem Register führen (Art. 21 Abs. 5 lit. B) DGA-E). Abschließend sieht Art. 22 DGA-E die Entwicklung eines europäischen Einwilligungsformulars für Datenaltruismus vor, das das Sammeln von Daten erleichtern soll, indem es sowohl Rechtssicherheit für Datennutzerinnen und -nutzer als auch Transparenz für Dateninhaberinnen und -inhaber schafft (ErwG. 39 DGA-E).

Datenaltruistischen Personen werden die folgenden Vorgaben auferlegt:

- Eintragung in das Register anerkannter datenaltruistischer Personen, Art. 15
- Eigene Rechtspersönlichkeit, Art. 16
- Zur Verfolgung von Zielen von allgemeinem Interesse gegründet, Art. 16
- Ohne Erwerbszweck tätig und unabhängig von jeder Organisation, die Erwerbszwecke verfolgt, Art. 17
- Datenaltruismustätigkeiten werden über eine rechtlich unabhängige Struktur ausgeübt, die von anderen Tätigkeiten, die sie durchführt, getrennt ist, Art. 17
- Niederlassung in einem Mitgliedstaat oder Benennung eines gesetzlichen Vertreters in einem Mitgliedstaat, Art. 17
- Transparenzanforderungen, Art. 18
- Informationspflichten und Sicherstellung der Zweckbindung, Art. 19

Anders als im Hinblick auf die Datenintermediäre des zweiten Kapitels werden an die Eintragung der datenaltruistischen Person auch Vorteile geknüpft: Für das Sammeln von Daten auf Grundlage des Datenaltruismus kann die Kommission Durchführungsrechtsakte zur Festlegung eines europäischen Einwilligungsformulars für Datenaltruismus erlassen. Dies könnte der oftmals beklagten fehlenden Rechtssicherheit im Hinblick auf die Einholung datenschutzrechtlicher Einwilligungen entgegenwirken.

23 COM (2020) 767 final.
24 Richter, *Europäisches Datenprivatrecht*, ZEuP 2021, S. 635 u. 639.
25 Auch in den einzelnen Kapiteln (s. etwa Art. 3 Abs. 3, S. 2, 4, Art. 9 Abs. 2 DGA-E) sowie in den Erwägungsgründen (s. etwa ErwG. S. 12 f., 28 f., 34 u. 44) wird wiederholt betont, dass derartige Vorgaben daneben anwendbar bleiben; dies gilt auch für die Gesetzesbegründung, vgl. COM (2020) 767 final, S. 2.
26 COM (2020) 767 final, S. 3.
27 Ebd., S. 7.

5 Problemlösungsorientierte Ausgestaltung von Datentreuhändern

Neben den horizontalen Vorgaben des Data Governance Acts bleibt, wie gezeigt, Raum für sektorspezifische und problemlösungsorientierte Regulierung, die die Mindestvorgaben des DGA-E einhält. Von den Vorgaben der DSGVO ließe sich theoretisch durch lex posterior abweichen, es soll aber gezeigt werden, dass sich ein problemlösungsorientierter Rechtsrahmen im Onlinesektor wie auch im Gesundheits- und Mobilitätssektor ohne derartige Abweichungen realisieren ließe. Es bedürfte aber jedenfalls Klarstellungen. Im Folgenden wird zunächst ein problemlösungsorientierter Rechtsrahmen für Datentreuhänder im Onlinesektor entworfen, sodann für den Gesundheitssektor und abschließend für den Mobilitätssektor.

5.1 Datentreuhänder im Onlinesektor

Insbesondere im Onlinesektor kommt es derzeit zu einer ganz erheblichen Übernutzung personenbezogener Daten, zum Teil unter Verstößen gegen das Datenschutz- und Verbraucherschutzrecht. Dies ist maßgeblich auf eine Informationsüberlastung der Nutzerinnen und Nutzer sowie auf ein datenschutzrechtliches Durchsetzungsdefizit zurückzuführen. Diese zwei Probleme führen beispielsweise dazu, dass Cookie-Banner häufig schlicht weggeklickt und Datenschutzerklärungen nicht gelesen werden. Die Lösung dieser zwei Probleme würde also bereits erheblich helfen. Beide Probleme ließen sich über PIMS einhegen.

Daneben existiert aber, wenn datenschutzrechtliche Einwilligungen gegenüber großen Onlineplattformen erklärt werden, auch ein wettbewerbliches Problem.[28] Die Behebung der datenschutzrechtlichen Funktionsdefizite allein wird daher in diesem Bereich nicht zu einem funktionierenden Datenschutzrecht führen: Selbst bei vollständiger Aufnahme der datenschutzrechtlichen Information durch die Betroffenen und Kenntnis der datenschutzrechtlichen Risiken werden Betroffene

jedenfalls gegenüber großen Onlineplattformen weiterhin in die Verarbeitung der sie betreffenden personenbezogenen Daten einwilligen, wenn sie den datenverarbeitenden Dienst, zum Beispiel eine Social-Media-Plattform, weiterhin nutzen wollen, weil Freunde und Bekannte diesen Dienst aufgrund seiner Marktdominanz ebenfalls nutzen. Dadurch lässt es sich auch erklären, dass Betroffene angeben, sich erheblich um den Umgang mit den sie betreffenden personenbezogenen Daten zu sorgen, sie in der Praxis aber dennoch umfassend in die Verarbeitung dieser Daten einwilligen, vor allem wenn dies zu Zwecken der Nutzung großer Onlineplattformen erforderlich ist.[29] Alle drei Problemkomplexe sollen im Folgenden zunächst erläutert werden.

5.1.1 Problemanalyse

5.1.1.1 Informationsüberlastung

Das informationelle Selbstbestimmungsrecht behält es dem Einzelnen vor, über die Preisgabe und Verwendung der personenbezogenen Daten selbst zu bestimmen.[30] Einzelnen steht es dabei grundsätzlich frei, Daten anderen gegenüber zu offenbaren, solange tatsächlich frei und eigenverantwortlich gehandelt wird.[31] Frei über die Preisgabe der personenbezogenen Daten und die Einwilligung in die Datenverarbeitung entscheiden kann aber nur, wer eine Entscheidung in Kenntnis der entscheidungsrelevanten Umstände, zum Beispiel Zweck und Reichweite der Datenverarbeitung trifft. Zu diesem Zweck normiert das Datenschutzrecht erhebliche Informationspflichten, die der Datenverarbeiter erfüllen muss. Den Informationserfolg allerdings müssen die Datenverarbeiter nicht gewährleisten. Die Betroffenen selbst sind dafür verantwortlich, dass sie die datenschutzrechtlichen Informationen zur Kenntnis nehmen. Auch deshalb scheint sich die Mehrheit der Datenschutzerklärungen nicht an dem Ziel der Nachvollziehbarkeit zu orientieren, sondern stellt lediglich eine rechtliche Absicherung der Datenverwertung dar.[32] Eine Studie, in der Facebook-Nutzerinnen und -nutzer dazu befragt wurden, ob sie ihre Einwilligung in die von Facebook praktizierte Datenverarbeitung erteilt hätten, kommt beispielsweise zu dem Ergebnis, dass lediglich 37 Prozent der Nutzerinnen und Nutzer der Ansicht waren, sich gegenüber Facebook damit einverstanden erklärt zu haben, dass ihre Daten gesammelt und verwendet werden können. Etwa 43 Prozent der Befragten erklärten, hiervon keine Kenntnis zu haben

und weitere 20 Prozent waren der Auffassung, sie hätten eine solche Einwilligung nie erteilt.[33] Ein Großteil der datenschutzrechtlichen Einwilligungserklärungen wird also abgegeben, ohne dass Betroffene die datenschutzrechtlichen Informationen zur Kenntnis nehmen. Sie willigen ein, ohne dass sie wissen, in welche Datenverarbeitungsvorgänge sie einwilligen[34] oder dass sie überhaupt einwilligen. Dies wird wesentlich auf das Problem der Informationsüberlastung zurückgeführt: Untersuchungen der Konsumentenverhaltensforschung belegen, dass eine steigende Informationsmenge zunächst zwar zur Erhöhung der subjektiven Entscheidungseffizienz beiträgt.[35] Ab einer bestimmten Informationsmenge sind Betroffene in Anbetracht begrenzter kognitiver Fähigkeiten aber nicht mehr in der Lage, die zur Verfügung gestellte Information auch tatsächlich aufzunehmen.[36] Die Informationsaufnahme sinkt dabei nicht nur insgesamt, es kann sogar zum Abbruch der gesamten Informationsaufnahme kommen.[37] Im datenschutzrechtlichen Kontext ist in der Regel zu beobachten, dass Betroffene den Text der Datenschutzerklärung lediglich nach unten scrollen und einen Haken bei der Einwilligungserklärung setzen, ohne die Datenschutzerklärung tatsächlich zu lesen.[38] 78 Prozent der befragten Facebook-Nutzerinnen und -Nutzer in der oben genannten Studie gaben an, dass sie die Datenschutzbestimmungen nicht gelesen oder lediglich überflogen hätten.[39] Dies wird auch als „Clicking Without Reading"-Phänomen[40] bezeichnet und ist bereits entsprechend aus dem Bereich der Allgemeinen Geschäftsbedingungen bekannt.[41] Zu ähnlichen Zahlen gelangt eine Befragung der Europäischen Kommission, nach der 26 Prozent der Nutzerinnen und Nutzer Datenschutzerklärungen nie lesen und 55 Prozent sagten, dass sie diese nur teilweise lesen würden. Als Grund wurde überwiegend angegeben, dass die Datenschutzerklärungen zu lang seien (70 Prozent) sowie dass diese unklar formuliert und schwer zu verstehen seien (43 Prozent).[42] Datenschutzerklärungen jeder Webseite zu lesen, die Nutzerinnen und Nutzer im Laufe eines Jahres besuchen, würde circa 76 Arbeitstage à acht Stunden kosten.[43] Verbunden mit dem niedrigen Nutzen der Wahrnehmung von Datenschutzerklärungen kann die fehlende Kenntnisnahme daher sogar rational sein. Man spricht von rationaler Apathie.

Zur Lösung dieses Problems bislang herangezogene Mittel, wie etwa der vom Bundesministerium der Justiz und für Verbraucherschutz in der Erprobung unterstützte Onepager oder auch die von der Carnegie Mellon University in Pittsburgh erarbeitete Etikettierungslösung,[44] zeigten in der Praxis nicht den erhofften Erfolg.[45] Visualisierungslösungen befinden sich derzeit noch in der Entwicklung, nachdem sie in die DSGVO nicht unmittelbar aufgenommen wurden.[46] PIMS könnten wesentlich helfen, das Problem bislang scheiternder Informationsvermittlung zu lösen, indem sie die datenschutzrechtlichen Informationen für die Betroffenen aufbereiten und diese beraten. Hierbei können sie auch auf Visualisierungslösungen zurückgreifen, ohne den langwierigen Prozess einheitlicher Bildsymbolgestaltung auf Unions- oder mitgliedstaatlicher Ebene abwarten zu müssen.

Visualisierungslösungen machen sich den Bildüberlegenheitseffekt zunutze: Empirische Studien belegen, dass die kognitiven Fähigkeiten des Menschen deutlich besser auf Bilder als auf Texte ansprechen,[47] was sich insbesondere daraus erklärt, dass Bilder ganzheitlich aufgenommen werden, Texte dagegen sequenziell.[48] Bilder werden erkannt, lange bevor ein Text erfasst wird. Für die Aufnahme eines Bildes in einer Form, dass es später wiedererkannt werden kann, benötigt das menschliche Gehirn für ein Bild mittlerer Komplexität im Durchschnitt etwa eine bis zwei Sekunden, während sich in derselben Betrachtungszeit nur etwa fünf bis zehn Worte eines einfachen Textes aufnehmen lassen.[49] Bilder sind außerdem in besonderer Form geeignet, zu aktivieren und damit Aufmerksamkeit zu erzeugen. Hierfür kommen in erster Linie Signalfarben wie Rot, Orange und Gelb in Betracht.[50] Darüber hinaus werden Bilder auch deutlich besser erinnert als Text.[51] Über diese Informations- und Beratungsfunktion würden PIMS also einen Service für Nutzerinnen und Nutzer anbieten, der deutlich über die technischen Einwilligungsmitteilungsmöglichkeiten hinausgeht, die derzeit diskutiert werden.[52] Diese Funktionalität könnte dabei auch über die datenschutzrechtlichen Problemlösungsoptionen hinausgehen und eine Problemlösung für das Verbraucherschutzrecht insgesamt anbieten, indem über die datenschutzrechtlichen Informationen hinaus diejenigen Informationen über ein Unternehmen, eine Webseite oder einen Datenverarbeiter zur Verfügung gestellt werden, die die Nutzerinnen und Nutzer durch persönliche Voreinstellungen wünschen,

zum Beispiel zur Nachhaltigkeit oder zu Details der Produktion, etwa wo ein Produkt produziert wird und welche Arbeitsbedingungen vorherrschen. Dies setzt freilich voraus, dass die Informationen verfügbar sind, wofür der Gesetzgeber zu sorgen hätte, sofern der Markt dies nicht selbst zu regeln in der Lage ist. Damit könnten PIMS auch zu einer echten (und datenschutzfreundlichen) Alternative zur derzeit vor allem in den USA diskutierten personalisierten Informationsvermittlung werden.

5.1.1.2 Datenschutzrechtliches Durchsetzungsdefizit

Die DSGVO leidet weiterhin an einem Durchsetzungsdefizit. Für die behördliche Rechtsdurchsetzung ist dies bereits umfassend diskutiert, es gilt aber gleichermaßen für die private Rechtsdurchsetzung. Und dies dürfte wesentlich an zwei Dingen liegen: Erstens, ist auch hier die erfolglose Informationsvermittlung ein wesentlicher Grund. Wird in den Datenschutzerklärungen zwar darauf hingewiesen, dass Betroffenenrechte existieren und wie von ihnen Gebrauch gemacht werden kann, nehmen die Betroffenen diese Informationen aber nicht wahr, so hindert sie bereits dies an der Ausübung dieser Nutzerrechte, es sei denn, sie erfahren auf anderem Weg von der Gebrauchsmöglichkeit.

Zweitens, ist die Aktionslast der Rechtsdurchsetzung für die Nutzerinnen und Nutzer ein wesentlicher Grund, von ihren Rechten keinen Gebrauch zu machen, selbst wenn sie Kenntnis von der Rechtsdurchsetzungsmöglichkeit haben. Denn die Entscheidung zur Rechtsdurchsetzung hängt letztlich stets vom persönlichen Kosten-Nutzen-Kalkül der Nutzerinnen und Nutzer ab: Nur soweit der erwartete Nutzen die erwarteten Kosten der Rechtsdurchsetzung übersteigt, werden Nutzerinnen und Nutzer von ihren außergerichtlichen und gerichtlichen Möglichkeiten Gebrauch machen.[53] Unterliegen die Nutzerinnen und Nutzer, haben sie die Kosten des Verfahrens nach zivilprozessualen Grundsätzen zu tragen, was sie als Risiko in die Kosten-Nutzen-Abwägung einspeisen werden. Hinzu kommt, dass Nutzerinnen und Nutzer die Erfolgswahrscheinlichkeit der Geltendmachung von Betroffenenrechten auch deshalb als gering einschätzen könnten, weil sie von einem Kräfteungleichgewicht zumindest gegenüber großen Datenverarbeitern ausgehen.[54] Letztlich ist aber auch der zeitliche Aufwand der Rechtsdurchsetzung ein wesentlicher Faktor, der das Nutzungsverhalten beeinflusst, was empirische

Untersuchungen aus den USA und dem Vereinigten Königreich für den Bereich des Urheberrechts belegen.[55] Auch hier könnten PIMS unterstützend wirken, indem sie die Rechte der Betroffenen (außergerichtlich) für die Betroffenen geltend machen und dabei zumindest den Zeitaufwand für die Betroffenen minimieren.

5.1.1.3 Wettbewerbliches Problem

Das wettbewerbliche Problem stellt sich allein bei der Erklärung der datenschutzrechtlichen Einwilligung in die Verarbeitung personenbezogener Daten gegenüber großen Onlineplattformen. Sie verfügen sowohl über große Marktmacht, die sich durch sehr große Skalenerträge sowie direkte und indirekte Netzwerkeffekte mit dem daraus resultierenden Tipping-Problem auszeichnet, als auch durch große Informationsasymmetrien gegenüber Nutzerinnen und Nutzern, die wiederum unter anderem aus einer Informationsüberlastung der Nutzerinnen und Nutzer entsteht. Die wirtschaftliche Macht großer digitaler Plattformen beruht daher auf einer Kombination von zwei gleichzeitig bestehenden schweren Marktversagensarten, die sich gegenseitig verstärken:[56] Erstens, können Informationsasymmetrien auf digitalen Märkten Wettbewerbsprobleme verstärken. Wenn Nutzerinnen und Nutzer die datenschutzrechtliche Information nicht wahrnehmen und daher nicht verstehen, wie datenschutz(un)freundlich ein Dienst ist, kann der Wettbewerb in Bezug auf die Qualität der datenschutzfreundlichen Lösungen nicht gut funktionieren. Zweitens, können (umgekehrt) quasi monopolistische Dienste intransparente und weitreichendere Bedingungen für die Erhebung und Verwendung personenbezogener Daten verwenden, weil die Nutzerinnen und Nutzer keine realistischen Alternativen haben. Beide Marktversagen verstärken sich gegenseitig.[57]

5.1.2 Problemlösungsoption: PIMS

Als Lösung des Informationsüberlastungsproblems sowie zur Behebung des datenschutzrechtlichen Durchsetzungsdefizites kommen Personal Information Management Systeme (PIMS) in Betracht. Zur Lösung des wettbewerblichen Problems können sie potenziell elementar beitragen. Personal Information Management Systeme sind im Ausgangspunkt technische Hilfsmittel, die helfen können, Datenverarbeitungen besser durch die Nutzerinnen und Nutzer kontrollieren zu können. Es

handelt sich um „Technologien und Ökosysteme, mit denen Menschen in die Lage versetzt werden sollen, über die Erhebung und Weitergabe ihrer personenbezogenen Daten Kontrolle auszuüben“[58] und damit um eine Privacy Enhancing Technology.[59] Sie können aber auch deutlich über diese technische Lösungsoption hinausgehen und einen Service für Nutzerinnen und Nutzer in Gestalt einer verbesserten Informationsvermittlung und Beratungsleistung (auch außerhalb des datenschutzrechtlichen Bereichs) sowie zur Durchsetzung datenschutzrechtlicher Befugnisse anbieten. Auch taugen sie zur Behebung von Dark Patterns. Hierunter versteht man Mittel und Methoden, die die Verhaltensbeeinflussung von Menschen durch Heuristiken und Biases zum Vorteil des Unternehmens, das Dark Pattern verwendet, oder Dritter (bewusst) ausnutzt (Dark Nudging),[60] zum Beispiel durch Hinterlegung des Einwilligungsbuttons in grüner Farbe, während die Ablehnung der Einwilligungserteilung in der Signal- und Warnfarbe Rot eingefärbt ist.

Auch PIMS-Nutzerinnen und -Nutzer werden freilich nie mit absoluter Gewissheit prognostizieren können, welche Konsequenzen ihre Einwilligung haben wird, wenn zum Beispiel Daten an Dritte weitergegeben werden.[61] Das deutsche Rechtssystem fordert für eine selbstbestimmte Entscheidung eine solche absolute Gewissheit der Entscheidungskonsequenzen nicht. Der Patient oder die Patientin, der oder die beispielsweise in die ärztliche Heilbehandlung einwilligen, können ebenso wenig sämtliche Risiken eines Fehlers des Arztes oder der Ärztin überschauen, wie die Betroffenen, die in die Datenverarbeitung einwilligen, jede unbefugte Verwendung von Daten vorhersehen können. Selbstbestimmung fordert statt dieser Gewissheit über die Konsequenzen vielmehr eine freie Entscheidung in Kenntnis möglicher Risiken. Dies setzt voraus, dass über die Risiken adäquat aufgeklärt wird und – an dieser Stelle muss angesetzt werden – dass die Information wahrgenommen und verstanden wird. Zu diesem Zweck können PIMS wesentlich beitragen.

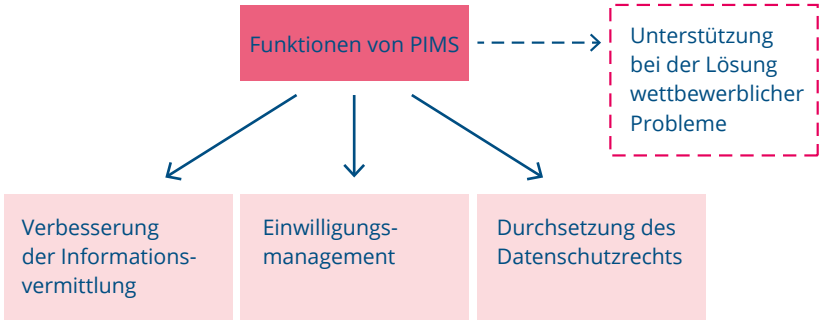
Als ein solches Schutz- und Selbstbestimmungsinstrument weisen PIMS drei Funktionen auf: Sie erfüllen, erstens, eine Informations- und Beratungsfunktion,[62] indem sie Betroffenen beispielsweise veranschaulichen, welche Daten von wem und zu welchen Zwecken über sie erhoben werden, diese Informationen aufbereiten, visualisieren

oder auch erläutern. Auch darüberhinausgehende Informationen zum Datenverarbeiter könnten zur Verfügung gestellt werden, und zwar auch solche, die mit dem Datenschutzrecht nichts zu tun haben, zum Beispiel Informationen über die Arbeitsbedingungen in dem datenverarbeitenden Unternehmen oder die Nachhaltigkeit der angebotenen Dienstleistung oder des angebotenen Produktes. PIMS könnten also eine wesentliche Servicefunktion erfüllen und Betroffenen die Informationen zur Verfügung stellen, die sie benötigen und wünschen.

Zweitens, sollen PIMS den Betroffenen helfen, tatsächlich nur in solche Datenverarbeitungen einzuwilligen, die ihren datenschutzrechtlichen Präferenzen entsprechen. Dazu könnten sie die Funktion einer „Einwilligungsassistenz“[63] wahrnehmen: Sie erteilen nach den im Treuhandvertrag vorgegebenen Bedingungen[64] Einwilligungen im Namen der Betroffenen. Dafür speichern sie in der Regel personenbezogene Daten ihrer Nutzerinnen und Nutzer zentral und geben diese an Dritte nur dann weiter, wenn die Nutzerinnen und Nutzer in die Datennutzung durch den Datenempfänger einwilligen.[65] Helfen könnten sie in dieser Funktion insbesondere bei der Reduzierung von Cookie-Bannern, indem sie Einwilligungen der Nutzerinnen und Nutzer nach deren einmal getätigten Vorgaben automatisiert erklären und individuell einzustellende Cookie-Präferenzen somit entbehrlich machen. Dies gilt nur, sofern nicht eine Ausnahme zum Einwilligungserfordernis nach § 25 Abs. 2 Nr. 2 TTDSG vorliegt. Die Tauglichkeit von PIMS zur Reduzierung von Cookie-Bannern hängt darüber hinaus von ihrer konkreten gesetzgeberischen Ausgestaltung ab, die an späterer Stelle diskutiert wird.

PIMS können, drittens, aber sogar bei der Durchsetzung des Datenschutz- und Verbraucherschutzrechtes unterstützen, indem sie beispielsweise Betroffenenrechte ausüben und Einwilligungen widerrufen.[66] Auch die automatisierte Meldung von Verstößen gegen das Datenschutz- und Verbraucherschutzrecht, die ein PIMS bei einem Tätigwerden für die Nutzerinnen und Nutzer feststellt (zum Beispiel unzulässige Koppelungen) ließe sich umsetzen. Die Tauglichkeit von PIMS für diese Problemlösung hängt aber ebenfalls maßgeblich von ihrer konkreten gesetzgeberischen Ausgestaltung ab, die an späterer Stelle erörtert wird.

Abbildung 2: Funktionen von PIMS



Der Data Governance Act versteht PIMS dagegen primär als Mittel, über das Daten der Wirtschaft zur Verfügung gestellt werden können. Diese verschiedenen Perspektiven auf PIMS als Schutz- und Teilhabeinstrument einerseits und als Instrument einer besseren Datenteilungsmöglichkeit andererseits beeinflussen, nach welchen Grundsätzen PIMS ausgestaltet werden. Versteht man PIMS primär als Datenteilungsinstrument, das zur Gefahr für das informationelle Selbstbestimmungsrecht werden kann, sorgt die Regulierung sich in erster Linie um die Sicherheit der Daten, untersagt die Verwendung der Nutzerdaten zu anderen Zwecken und sucht darum, Anreize für das Datenteilen zu verhindern. Geschäftsmodelle, die dieses Datenteilen incentivieren, werden kritisch gesehen. Versteht man PIMS dagegen als Schutz- und Teilhabeinstrument, muss die Regulierung neben dieser Missbrauchsprävention darum bemüht sein, alles daran zu setzen, um diese Technologien zu ermöglichen. Aufgabe des Gesetzgebers ist es, beide Perspektiven auf PIMS miteinander in Einklang zu bringen,[67] indem sowohl die Chancen als auch die Gefahren, die von ihnen für das informationelle Selbstbestimmungsrecht ausgehen, angemessen berücksichtigt werden.

5.1.2.1 Wesentliche Elemente eines problemlösungsorientierten Rechtsrahmens für PIMS

Ein funktionsfähiger Rechtsrahmen für PIMS erfordert Entscheidungen auf Systemebene, nicht im Rahmen von Insellösungen. Ist es gewollt, dass PIMS funktionieren sollen, sind auf dieser Systemebene zwei

Voraussetzungen zu gewährleisten: Erstens, eine Kooperationspflicht der Datenverarbeiter mit PIMS sowie, zweitens, eine Standardisierung der technischen Voraussetzungen zur Kooperation. Sind diese zwei Systemvoraussetzungen erfüllt, bedarf es zwar weiterer Feinjustierungen des Rechtsrahmens, die die Funktionsfähigkeit von PIMS absichern, ohne die Entscheidungen auf Systemebene sind diese Feinjustierungen aber nutzlos. Daneben gilt es, die mit PIMS verbundenen Risiken durch adäquate Regulierung zu minimieren und die Organisations- und Finanzierungsfrage zu beantworten.

5.1.2.2 Regulierung auf Systemebene

Pflicht zur Berücksichtigung von PIMS-Vorgaben

Bereits die Datenethikkommission forderte in ihrem Gutachten eine verpflichtende Berücksichtigung von PIMS-Vorgaben.[68] Auch der Verbraucherzentrale Bundesverband (VZBV), die Stiftung neue Verantwortung (SNV) sowie weitere Stimmen in der Literatur sprechen sich für eine solche verpflichtende Berücksichtigung von PIMS-Vorgaben aus.[69] Eine Berücksichtigungspflicht von PIMS-Vorgaben für die Datenverarbeiter bedeutet, dass Vorgaben, die der Betroffene gegenüber dem PIMS macht, vom Datenverarbeiter zwingend zu berücksichtigen sind und es ihm untersagt ist, am PIMS vorbei mit dem Betroffenen zu interagieren, soweit Vorgaben an den PIMS getroffen wurden. Tatsächlich ist eine solche Berücksichtigungspflicht von PIMS-Vorgaben absolut zwingend, denn nur dann besteht ein hinreichender Nutzen ihrer Inanspruchnahme: Wird eine Berücksichtigungspflicht von PIMS nicht etabliert, könnten Onlineakteure die Vorgaben von PIMS unberücksichtigt lassen und die Nutzerinnen und Nutzer weiterhin um ihre Einwilligung bitten. Insbesondere würde es sich für die Nutzerinnen und Nutzer nicht lohnen, einen PIMS zu benutzen, wenn nur ein begrenzter Teil der Einwilligungen darüber abgewickelt werden kann. Dann hätte er immer noch einen sehr begrenzten Überblick über seine gegebenen Einwilligungen. Das Informationsüberlastungsproblem würde nicht behoben. Nur bei verpflichtender Berücksichtigung der PIMS-Vorgaben könnten PIMS darüber hinaus eine Marktdurchdringung erreichen, die ein Gegengewicht zur Marktmacht großer Onlinedienste etablieren kann und PIMS daher langfristig in die Position versetzen könnte, die Bedingungen der Datenverarbeitung aktiv zu verhandeln.

Technische Standardisierung
Überdies ist technische Standardisierung für die automatisierte Verarbeitung von Einwilligungen und entsprechenden Datentransfers unumgänglich. Erforderlich sind gemeinsame technologische Standards zwischen allen Akteuren der Digitalwirtschaft. Das Problem standardisierter und offener Schnittstellen, (APIs et cetera), aber auch semantischer Standardisierungen stellt sich ebenso bei Datenzugangsfragen und Datenportabilitätsfragen und ist daher nicht neu. In der Standard-Setting-Literatur wird betont, dass solche Standards entweder in klassischen (kollektiven) Standardsetzungsverfahren gesetzt werden können oder durch marktmächtige Unternehmen.[70] Ein solches System kann nicht dezentral von unten durch viele PIMS entstehen. Es handelt sich insofern um ein klassisches Standard-Setting-Problem mit den typischen Marktversagensproblemen. Insofern kommt Standardisierungspolitik und der Verpflichtung auf bestimmte Standards eine Schlüsselrolle zu, wenn nicht gewollt ist, dass es die großen Digitalkonzerne sind, die diese Standards setzen.

5.1.2.3 Feinjustierungen im Rechtsrahmen

Feinjustierung zur Lösung der datenschutzrechtlichen Problemlage
Ist eine verpflichtende Berücksichtigung der PIMS-Vorgaben und technische Standardisierung gewährleistet, bedarf es lediglich weiterer Feinsteuerungen im Rechtsrahmen, die sich aber im Wesentlichen in Klarstellungen erschöpfen. Dies betrifft einerseits die Unterstützung der Informationsfunktion von PIMS (a) und andererseits die Herstellung von Rechtssicherheit für das Einwilligungsmanagement (b) sowie für die Möglichkeit, datenschutzrechtliche Betroffenenrechte durchzusetzen (c). Letztlich ist Missbrauchsgefahren adäquat vorzubeugen, Interessenkonflikten des PIMS zu begegnen und damit das Risiko für die informationelle Selbstbestimmung insgesamt zu minimieren (d).

Unterstützung der Informationsfunktion
Sollen PIMS dabei unterstützen, die datenschutzrechtliche Information zu vermitteln, erfordert dies keinen unmittelbaren gesetzgeberischen Handlungsbedarf, denn eine Hilfestellung bei der Informationsvermittlung ist gesetzlich nicht untersagt. Die PIMS werden auch nicht für den Verantwortlichen tätig. Die Frage, ob der Verantwortliche die

Informationspflichten korrekt umgesetzt hat, wird durch ihre Tätigkeit nicht beeinflusst, sofern dies nicht explizit vereinbart wird. Die Informationsvermittlung über die beim Verantwortlichen erfolgenden Datenverarbeitungen müssen daher nicht den Anforderungen nach Art. 13, 14 DSGVO genügen (etwas anderes gilt für die Information über die beim PIMS erfolgende Datenverarbeitung). Insofern kommt es für die Frage der unterstützenden Informationsvermittlungstätigkeit durch PIMS nicht darauf an, in welcher Form diese Informationsvermittlung nach dem Gesetz erfolgen muss. PIMS kann daher problemlos auch auf Visualisierungslösungen zurückgreifen.[71] Positiv wäre es aber, wenn die Informationsvermittlungsmöglichkeiten insgesamt (also auch im Anwendungsbereich nach Art. 13, 14 DSGVO) verbessert werden würden. Dies wäre zum Beispiel über ein Schichtenmodell der Informationsvermittlung möglich, das auch visuelle Elemente beinhaltet.[72] Bilder werden aufgrund des Bildüberlegenheitseffektes besser wahrgenommen und erinnert[73] und sind aus diesem Grund der rein textbasierten Informationsvermittlung vorzuziehen. Um Visualisierungslösungen aber hinreichend effizient zu gestalten, wäre die Entwicklung einheitlicher Bildsymbole wünschenswert.[74]

Einwilligungsmanagement rechtssicher ermöglichen und effektivieren
Handlungsbedarf besteht dagegen für den Bereich des Einwilligungsmanagements. Insgesamt sollte hier durch ermöglichende Regulierung innerhalb der DSGVO unterstützt werden. Dies beinhaltet einerseits die Klarstellung, dass eine Stellvertretung bei der Abgabe der Einwilligung möglich ist, und andererseits die Ermöglichung einer breiteren Einwilligung gegenüber PIMS. Die Möglichkeit der Stellvertretung sowie der breiten Einwilligung sollte für solche PIMS vorgesehen werden, die festgelegte Anforderungen, zum Beispiel IT-sicherheitsrechtliche Vorgaben, erfüllen. Diese Anforderungen können zum Teil dem Data Governance Act entnommen werden. Ihre Einhaltung könnte im Rahmen eines staatlichen Zertifizierungssystems oder Anerkennungsverfahrens (wie im TTDSG vorgesehen) überprüft werden.

Ob Dritte überhaupt Einwilligungen für die Betroffenen erklären können, ist streitig.[75] Auch im Datenschutzrecht lässt sich eine Einwilligung nicht nur als Rechtfertigungsinstitut denken, sondern ebenso als rechts-

geschäftliche Erklärung.[76] Stellvertretungskonstellationen sind zwar nicht expressis verbis in der DSGVO verankert, aber doch dem Unionsrecht grundsätzlich bekannt.[77] Auch die Entscheidung für eine solche Stellvertretungslösung ist letztlich eine Ausübung des Rechts auf informationelle Selbstbestimmung und daher anzuerkennen.[78] An die Vollmachtserteilung sollten aber dieselben Anforderungen zu stellen sein wie an die Einwilligung selbst.[79] Dies widerspricht zwar § 167 Abs. 2 BGB, die Einwilligung nach der DSGVO ist aber auch nicht nach den Maßstäben des nationalen Rechts, sondern unionsrechtlich autonom auszulegen.[80] Die hohen Voraussetzungen der Einwilligung, die eine echte Selbstbestimmung der Betroffenen gewährleisten sollen, würden unterlaufen, wenn die Voraussetzungen nicht auch für die Vollmachtserteilung gelten würden.[81]

Auch die Tätigkeit als Erklärungsbote ist möglich, und viele PIMS werden derzeit allein auf Grundlage einer Botenschaft tätig, weil ihnen der eigene Entscheidungsspielraum fehlt. Abseits von der Überbringung der konkreten Einwilligungserklärung – einen eigenen Handlungsspielraum für PIMS gewährleisten würde nur eine Stellvertretungslösung. Sinn machte eine solche Stellvertretungslösung aber wohl nur in Kombination mit der Möglichkeit einer breiten Einwilligung. Sinn und Zweck einer Einwilligungsassistenz ist es schließlich, nicht für jede Einwilligung erneut bei den Betroffenen nachfragen zu müssen, ob sie diese erteilen möchten, sondern den Betroffenen die Möglichkeit zu geben, vorab zu definieren, für welche Fälle und unter welchen Voraussetzungen eine Einwilligung erteilt werden soll und bei Vorliegen der Voraussetzungen ohne erneute Rückfrage für die Betroffenen einzuwilligen. Der Entscheidungsspielraum des stellvertretenden PIMS läge also hier insbesondere in der konkreten Auswahl des Datenverarbeiters. Dass er im Innenverhältnis engen Weisungen unterliegt, schadet nicht. Auch der Verkäufer wird schließlich als sogenannter „Vertreter mit gebundener Marschroute“ auf Basis des Stellvertretungsrechts tätig.[82] Aus Rechtssicherheitserwägungen heraus sollte die Möglichkeit der Stellvertretung gesetzlich verankert werden, das Unionsrecht lässt sie, wie dargelegt, schon heute zu.

Datenverarbeitungen, die durch PIMS erfolgen, müssen derzeit (und zwar auch unter den Vorgaben des neuen TTDSG) in der Regel durch

eine Einwilligung gerechtfertigt werden, die, auch wenn sie gegenüber PIMS erklärt wird, einer engen Zweckbindung unterliegt.[83] Einwilligungen, in denen entweder ein konkreter Zweck, aber kein konkreter Verantwortlicher, oder ein konkreter Verantwortlicher, aber keine konkreten Zwecke bestimmt werden, sind unwirksam.[84] Eine Datenübermittlung, die ein PIMS vornimmt, muss daher in der Regel von einer Einwilligung der Betroffenen, die konkret für den Einzelfall getroffen wird, gerechtfertigt sein. Eine wirksame Einwilligung durch PIMS abzugeben, ist aber bereits de lege lata über einen sogenannten Dynamic Consent möglich. Hier werden in einem ersten Schritt die Datenschutzpräferenzen der Betroffenen abgefragt, das heißt die Nutzerinnen und Nutzer legen fest, für welche breiten Zwecke sie die betreffenden Daten zur Verfügung stellen möchten (zum Beispiel nicht für personenbezogene Werbung, wohl aber für Zwecke der Forschung). Für den Fall, dass eine passende Datenverarbeitungssituation auftritt, werden die Nutzerinnen und Nutzer über das PIMS um ihre Einwilligung für den konkreten Fall gebeten.[85] Erwägenswert de lege ferenda scheint aber auch die Aushandlung der Voraussetzungen einer breiten Einwilligung entsprechend dem standardisierten Einwilligungsformular, das die Medizininformatikinitiative und die DSK für den Gesundheitssektor abgestimmt haben.[86] Eine Meta-Einwilligung scheint für den Gesundheitssektor denkbar, in dem PIMS Daten für Forschungszwecke zur Verfügung stellen könnten.[87] Sie erlaubte es den Einwilligenden, unabhängig von einem konkreten Anlass zu entscheiden, für welche Art von Forschungsvorhaben die Betroffenen in welchem Forschungskontext welche Art von Einwilligung (spezifische oder breite Einwilligung) abgeben möchten.[88] Die Datenethikkommission empfiehlt die Prüfung der Möglichkeit einer solchen Meta-Einwilligung.[89]

Durchsetzung des Datenschutzrechts durch PIMS ermöglichen

Letztlich sollten PIMS auch datenschutzrechtliche Befugnisse ausüben und Datenschutzverstöße (automatisiert) anzeigen können. Muss beispielsweise die Einwilligung erklärt werden, um einen Dienst in Anspruch zu nehmen, kann das Koppelungsverbot, Art. 7 Abs. 4 DSGVO, verletzt sein. Ein solcher Datenschutzverstoß kann automatisiert an die zuständigen Datenschutzbehörden gemeldet werden. Dies erfordert jedoch keine Anpassung des Rechtsrahmens.

Klarstellungen im Rechtsrahmen erscheinen jedoch wünschenswert für die Geltendmachung datenschutzrechtlicher Befugnisse durch PIMS. Denn ob die Art. 15 ff. DSGVO von Dritten geltend gemacht werden können, wird in der DSGVO nicht geregelt. Aus Art. 80 DSGVO, der die Wahrnehmung spezifischer Rechte auch Dritten gestattet, ließe sich zwar der Rückschluss ziehen, dass eben dies für die Art. 15 ff. DSGVO nicht zulässig ist. Andererseits ließe sich aber begründen, der Gesetzgeber habe hierzu gerade keine Aussage treffen wollen und eine Ausübung der Betroffenenrechte durch Dritte sei daher nicht ausgeschlossen.[90] Hier sollte insofern eine Klarstellung seitens des Gesetzgebers erfolgen.

Feinjustierungen zur Lösung des wettbewerblichen Problems
Sollen nicht allein datenschutzrechtliche Probleme adressiert werden, sondern geht es zudem um die Lösung wettbewerblicher Probleme, so sollte es PIMS zusätzlich zu den oben genannten Vorgaben auch ermöglicht werden, einen Anbieterwechsel hin zu einer datenschutzfreundlicheren Plattform zu vollziehen, das heißt Kündigungen des entsprechenden Plattformnutzungsvertrages auszusprechen und neue Plattformnutzungsverträge abzuschließen. Dies sollte aber bereits mit den derzeitigen Vorgaben des Bürgerlichen Rechtes möglich sein.

Das wettbewerbliche Funktionsdefizit kann aber nicht allein durch einen funktionierenden Rechtsrahmen für PIMS gelöst werden. Es bedarf vielmehr zweier weiterer materiell-rechtlicher Vorgaben: Erstens, einer Interkonnektivitätsverpflichtung für große Onlineplattformen sowie, zweitens, einer Bezahloption für die Inanspruchnahme der Dienste von großen Onlineplattformen als Alternative zur Erklärung der datenschutzrechtlichen Einwilligung, sofern dies nicht bereits durch das Koppelungsverbot vorgegeben ist. Große Onlineplattformen sollten also verpflichtet werden, den Nutzerinnen und Nutzern anderer Plattformen die unmittelbare Interaktion mit ihren Kundinnen und Kunden zu ermöglichen, ihnen zum Beispiel im Falle von Messenger-Diensten sozialer Netzwerke das Versenden und Empfangen von Nachrichten zu ermöglichen.[91] Aber auch den Nutzerinnen und Nutzern die Wahl zu geben, ob sie statt eine datenschutzrechtliche Einwilligung zu erklären, den Dienst monetär bezahlen möchten, um ihn in Anspruch zu nehmen.[92]

Gelingt es, für PIMS einen funktionierenden Rechtsrahmen zu etablieren, so könnten diese bei Inanspruchnahme durch eine Vielzahl von Personen ein Gegengewicht zu großen Onlineplattformen bilden. Besteht sowohl auf Anbieter- als auch auf Nachfrageseite Marktmacht (oder zumindest Verhandlungsmacht), wären Plattformen nicht länger in der Lage, die Bedingungen der Datenverarbeitung zu diktieren. Die Möglichkeit, Verhandlungsmacht zu gewinnen, kann und muss das Fernziel sein, das es mithilfe von PIMS zu erreichen gilt. Darüber hinaus ist es eine zentrale Aufgabe der Wettbewerbspolitik, das Problem der Marktmacht von digitalen Plattformen zu lösen, beispielsweise über den Digital Markets Act (DMA), der zurzeit auf der EU-Ebene diskutiert wird, oder den neuen Paragrafen 19a GWB im deutschen Wettbewerbsrecht.

5.1.2.4 Risiken minimieren

PIMS nehmen bei der Lösung der aufgezeigten Probleme eine wichtige Rolle ein, indem sie zum Beispiel informierte Entscheidungen über die Verarbeitung von Daten oder aber das Eingehen eines Vertrages insgesamt und die Ausübung von Betroffenenrechten ermöglichen. Sie lösen damit Probleme der informationellen Selbstbestimmung aber nur, soweit sich diese durch eine informierte Einwilligung lösen lassen. Ob die Einwilligung jede Form der Datenverarbeitung legitimieren können sollte, ist eine andere Frage, die durch den Gesetzgeber zu klären ist. Besonders gefahrgeneigte Verarbeitungstätigkeiten ließen sich beispielsweise an zusätzliche Voraussetzungen knüpfen oder gänzlich untersagen. Dazu könnte beispielsweise die Zusammenführung von Daten durch sehr große Onlineplattformen im Sinne des Art. 5 (a) DMA gehören.

Die Datenethikkommission empfiehlt außerdem die Einführung eines Zertifizierungs- und Überwachungssystems für PIMS. Blankomandate an PIMS sollten ausgeschlossen werden, Vorkehrungen für den Fall der Insolvenz oder Auflösung der PIMS getroffen werden. Außerdem sind die Vorgaben des Data Governance Acts einzuhalten.[93]

5.1.2.5 Finanzierung und Organisation

Für die Finanzierung von PIMS existieren zwei Möglichkeiten: Entweder werden PIMS allein staatlicherseits angeboten oder es werden (auch) privatwirtschaftliche Modelle ermöglicht. Staatliche Datenverarbeitungen sind nicht per se deshalb zu bevorzugen, weil der Staat besonders vertrauenswürdig im Umgang mit personenbezogenen Daten erscheint. Im Gegenteil wurde das informationelle Selbstbestimmungsrecht als Abwehrrecht gegen den Staat konzipiert. In einer Vielzahl von Rechtsordnungen gehen mit einer Datenverarbeitung durch den Staat sehr viel erheblichere Risiken einher als mit einer Datenverarbeitung durch private Unternehmen. Gleichwohl ist ein Rechtsstaat geeignet dazu, als Anbieter von PIMS aufzutreten. Dies bedarf aber der expliziten gesetzgeberischen Entscheidung. Bislang ist der Gesetzgeber bei der Entwicklung von PIMS nicht in ausreichendem Maße tätig geworden, was nahelegt, dass er eine private Entwicklung von PIMS nicht ausschließen möchte.[94] Die privatwirtschaftliche Tätigkeit von PIMS kann allerdings nur gelingen, wenn die Tätigkeit profitabel ist. Dabei stellen sich zwei Fragen: Erstens, von wem ist das PIMS zu bezahlen (vonseiten des Datenverarbeiters oder vonseiten der Nutzerinnen und Nutzer)? Und zweitens, wofür ist das PIMS zu bezahlen (für die Volumina der Datenmittelung oder für den von ihm angebotenen Service)?

Beide Fragen lassen sich nicht unabhängig voneinander beantworten: Als Schuldner einer Gegenleistung für die Tätigkeit des PIMS kommen der Datenverarbeiter sowie die einzelnen Nutzerinnen und Nutzer in Betracht. Schuldet der Datenverarbeiter die Tätigkeit, wird ein Anreiz für das PIMS zur Mittelung möglichst vieler Daten an das Unternehmen gesetzt, um einen möglichst hohen Preis zu erzielen (wenn man davon ausgeht, dass das Datenvolumen den Preis bestimmt). Ein solcher Anreiz zur Mittelung möglichst vieler personenbezogener Daten ist im Hinblick auf die effektive Gewährleistung des informationellen Selbstbestimmungsrechts kritisch zu sehen.[95] Es würde ein Anreiz für PIMS geschaffen, die Nutzerinnen und Nutzer zur Einwilligung in die Mittelung möglichst vieler Daten an die Datenverarbeiter zu bewegen. Das würde dazu führen, dass PIMS weniger Kontroll- und Teilhabeinstrument als Instrument zum vermehrten Datenteilen wäre. Das läge weniger im Nutzerinteresse als im Datenverarbeiterinteresse.

Haben die Nutzerinnen und Nutzer hingegen für die Tätigkeit des PIMS zu zahlen, wäre der Schutz der informationellen Selbstbestimmung abhängig vom Einkommen der Nutzerinnen und Nutzer,[96] wobei schwächere Einkommen benachteiligt würden. Letztlich offerieren PIMS aber einen Service für die Nutzerinnen und Nutzer, für den diese zumindest im Ausgangspunkt auch die Gegenleistung erbringen sollten, um die oben beschriebene falsche Anreizsetzung zu vermeiden. Auch eine Reduktion der zu zahlenden Vergütung durch eine Monetarisierung personenbezogener Daten der Betroffenen, zum Beispiel durch eine Rückvergütung, wird zwar umfassend diskutiert,[97] ist jedoch im Hinblick auf ihre Anreizwirkung hoch problematisch. Um sicherzustellen, dass auch weniger finanzstarken Personen PIMS zur Verfügung gestellt werden kann, sollte eine staatliche Subventionierung anerkannter oder zertifizierter PIMS in Betracht gezogen werden.

5.1.3 Geeignetheit von DGA-E und § 26 TTDSG zur problemlösungsorientierten Regulierung von PIMS

5.1.3.1 Data Governance Act

Der Data Governance Act verfolgt auch und gerade das Ziel, eine bessere Kontrolle über Daten und ihre Nutzung im Einklang mit dem Unionsrecht zu gewährleisten. Als Mittel dieses Ziel zu erreichen, wird die Herstellung von Vertrauen gewählt. Der europäische Gesetzgeber geht davon aus, dass bislang am Markt fehlende oder nur gering am Markt verfügbare Datenintermediäre zur Verbesserung der Kontrolle der Datennutzung – in der Regel PIMS – entstehen beziehungsweise in größerem Umfang vorhanden sind, sobald nur das Vertrauen in diese Dienste gestärkt wird. Wie gezeigt wurde, ist für PIMS aber fehlendes Vertrauen nicht das wesentliche Problem, das eine stärkere Etablierung am Markt verhindert. Die fehlende Marktdurchdringung ist vielmehr darauf zurückzuführen, dass die Inanspruchnahme von PIMS derzeit für die Betroffenen nur begrenzte Vorteile mit sich bringt, da erstens, keine Berücksichtigungspflicht für PIMS-Vorgaben und keine technische Standardisierung existiert, und zweitens, PIMS allein nicht das Problem lösen können, wenn Nutzerinnen und Nutzer sich aufgrund von Marktmacht vielfach gezwungen fühlen, in Datenverarbeitungen vor allem großer Plattformen einzuwilligen. Entsprechende Geschäftsmodelle konnten sich daher noch nicht am Markt etablieren. Erst wenn die notwendigen Funktionsbedingungen für PIMS in der

beschriebenen Form durch Regulierung hergestellt werden, werden sie einen Vorteil für die Nutzerinnen und Nutzer bieten können, der die Nutzung fördert. Die zusätzlichen Anforderungen des DGA-E dienen zwar der Missbrauchsprävention, erschweren die Tätigkeit von PIMS aber zusätzlich. Zur Verwirklichung einer verbesserten Kontrolle über den Zugang und die Nutzung von Daten ist der DGA-E so lange gänzlich ungeeignet, wie er ausschließlich diese zusätzlichen Voraussetzungen vorsieht, ohne ergänzend Verpflichtungen zur Berücksichtigung der PIMS-Vorgaben und eine technische Standardisierung vorzugeben. Darüber hinaus ist eine entsprechende Feinjustierung des Rechtsrahmens vorzusehen, der Rechtssicherheit gewährleistet und dabei anreizbasiert ausgestaltet ist. (Die Erfüllung der Vorgaben zur Missbrauchsprävention muss zu datenschutzrechtlicher Rechtssicherheit führen.) Die Forderung nach datenschutzrechtlicher Rechtssicherheit hatte bereits die Datenethikkommission erhoben.[98]

5.1.3.2 § 26 TTDSG

Mit § 26 TTDSG soll ein „verlässlicher und glaubwürdiger“[99] Rahmen für Dienste zur Verwaltung von nach § 25 Absatz 1 TTDSG erteilten Einwilligungen geschaffen werden, der dazu führt, dass „Endnutzer solchen Diensten ihre Daten auch anvertrauen“,[100] um im Ergebnis Cookie-Banner zu reduzieren. § 26 TTDSG beschränkt sich auf die Einwilligung zur Speicherung von Cookies oder zum Abruf von Informationen aus bereits gespeicherten Cookies nach § 25 TTDSG. Die Reduzierung der Cookie-Banner zielt auf die Reduzierung der Informationsüberlastung der Nutzerinnen und Nutzer und damit auf die Lösung des datenschutzrechtlichen Informationsüberlastungsproblems in einem spezifischen Fall. Der nationale Gesetzgeber geht – wie schon der europäische Gesetzgeber – davon aus, dass die bislang fehlende Verbreitung von PIMS am Markt im Wesentlichen auf ein fehlendes Vertrauen zurückzuführen ist und will daher durch § 26 TTDSG dieses Vertrauen stärken. Es fehlt jedoch weniger am Vertrauen der Nutzerinnen und Nutzer in PIMS, sondern am entscheidenden Vorteil einer PIMS-Nutzung (siehe oben). Das Ziel der Reduzierung von Cookie-Bannern durch PIMS wird insofern erst erreicht werden, wenn der Rechtsrahmen PIMS in Funktionsfähigkeit versetzt, indem er es ihnen ermöglicht, sowohl die datenschutzrechtliche als auch die wettbewerbliche Problemlösung zu unterstützen.

Zu dieser Lösung trägt § 26 TTDSG nur wenig bei. Angesetzt wird allein (und auch dies nur marginal) auf Ebene der Feinjustierung des Rechtsrahmens, nicht aber auf Systemebene: Zwar wird es PIMS ermöglicht, selbst ohne eine nach § 26 TTDSG mögliche Anerkennung datenschutzrechtliche Einwilligungserklärungen für Betroffene zu übermitteln. Die übrigen datenschutzrechtlichen Grauzonen werden indes nicht angetastet. Darüber hinaus reguliert § 26 TTDSG ebenso wenig die der DGA-E auf Systemebene. Er dient allein der Reduktion von Missbrauchsrisiken, indem er eine Anerkennung von PIMS durch eine unabhängige Stelle nach Maßgabe des § 26 Abs. 2 TTDSG ermöglicht, wenn die Dienste

1. nutzerfreundliche und wettbewerbskonforme Verfahren und technische Anwendungen zur Einholung und Verwaltung der Einwilligung haben;

2. kein wirtschaftliches Eigeninteresse an der Erteilung der Einwilligung und an den verwalteten Daten haben und unabhängig von Unternehmen sind, die ein solches Interesse haben können;

3. personenbezogene Daten und die Informationen über die Einwilligungsentscheidungen für keine anderen Zwecke als die Einwilligungsverwaltung verarbeiten; und

4. ein Sicherheitskonzept vorlegen, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglicht und aus dem sich ergibt, dass der Dienst sowohl technisch als auch organisatorisch die rechtlichen Anforderungen an den Datenschutz und die Datensicherheit, die sich insbesondere aus der Verordnung (EU) 2016/679 ergeben, erfüllt.

Die von den Diensten zur Einwilligungsverwaltung zwecks Anerkennung konkret zu erfüllenden Voraussetzungen sollen durch eine Rechtsverordnung festgelegt werden.

Browserhersteller sollen die Einstellungen in PIMS zu Cookies berücksichtigen. Eine Befolgungspflicht der PIMS-Einstellungen ergibt sich aus dem TTDSG aber nicht.[101] Telemedienanbieter können daher auch

weiterhin die Einzelnutzerinnen und -nutzern um eine individuelle Einwilligung bitten. Zu einer Reduzierung von Cookie-Bannern und damit zur Reduzierung der Informationsüberlastung der Nutzerinnen und Nutzer wird die Regelung nicht beitragen.[102] Eine Berücksichtigungspflicht von PIMS-Vorgaben kann in der Rechtsverordnung selbst, die derzeit ausgearbeitet wird, wohl nicht untergebracht werden, weil § 26 TTDSG dafür wohl keinen Raum lässt. Eine Verpflichtung zur Befolgung der PIMS-Vorgaben müsste im § 26 TTDSG selbst als Folge der Anerkennung normiert werden, die datenschutzrechtlich erforderlichen Klarstellungen (siehe oben) entweder ebenfalls im TTDSG als Folge der Anerkennung oder aber für einen breiteren Anwendungsbereich im BDSG beziehungsweise der DSGVO normiert werden.

5.2 Datentreuhänder im Gesundheitssektor

Anders als im Onlinewirtschaftssektor besteht im Gesundheitssektor nicht das Problem einer Übernutzung, sondern einer Unternutzung von Daten, zumindest für Forschungszwecke. Zwar existieren auf nationaler Ebene verschiedener Mitgliedstaaten Register, die für Forschungszwecke genutzt werden können, wie in Deutschland das Krebsregister oder das Forschungsdatenzentrum. Der Zugriff auf die Daten ist aber nicht oder nur wenig koordiniert. Das macht es für Wissenschaftlerinnen und Wissenschaftler schwierig, den richtigen Zugangsadressaten zu identifizieren. Benötigt wird daher eine zentrale europäische oder mitgliedstaatliche Koordinierungsstelle, an die Anträge auf Forschungsdatenzugang im Wege eines standardisierten elektronischen Formulars gestellt werden können und die über das Vorliegen der Antragsvoraussetzungen sowie Art und Umfang des Datenzugangs entscheidet. Entsprechende Koordinierungsstellen existieren beispielsweise in Finnland und Australien.[103]

Es werden aber niemals sämtliche Daten in derartigen Registern gespeichert werden können, weil die Register in der Regel krankheitsspezifische Daten (zum Beispiel Krebsdaten) oder zweckspezifische Daten (zum Beispiel Abrechnungsdaten) vorhalten. Insofern bedarf es neben einer als Datentreuhand ausgestalteten Koordinierungsstelle flexibler staatlicherseits oder privatwirtschaftlich angebotener Datentreuhandlösungen, mit deren Hilfe auch heterogene Daten im Einklang mit dem Datenschutzrecht geteilt und ausgewertet werden können.

Letztlich ließe sich zur Lösung des Problems der Unternutzung von Daten für die Forschung auch durch eine Datenspendefunktion in einer elektronischen Patientenakte beitragen. Elektronische Patientenakten, wie sie zum Beispiel in Schweden und Dänemark, aber auch in Deutschland (ePa) oder Österreich (ELGA) ausgestaltet werden, fungieren ebenfalls als Datentreuhand, weil sie Daten von Patientinnen und Patienten in deren Interesse den Anbietern von Gesundheitsdienstleistungen mitteln. Damit lösen sie in erster Linie ein bislang existierendes Effizienzproblem in der Gesundheitsversorgung, das auch und gerade daraus resultiert, dass Daten bislang beim Gesundheitsdienstleister gespeichert werden und damit anderen Gesundheitsdienstleistern, die von Patientinnen und Patienten aufgesucht werden, häufig nicht zugänglich sind. Zur Lösung dieses Effizienzproblems sind Nutzungsanreize und Vorkehrungen gegen unberechtigten Zugriff auf Daten sowie Datenmissbrauch erforderlich. Zur Lösung des Problems der Datenunternutzung ist hingegen eine Datenfreigabeoption/Datenspendeoption auf Grundlage einer informierten Einwilligung und ihre technische Gewährleistung gesetzlich zu verankern.

Im Folgenden wird zunächst der Ansatz einer zentralen Koordinierungsstelle in Finnland und Australien als der am weitesten fortgeschrittene Ansatz für eine derartige Koordinierungsstelle erläutert. Eine entsprechende Stelle wird auch von einem aktuellen Gutachten im Auftrag des Bundesministeriums für Bildung und Forschung (BMBF) vorgeschlagen.[104] Anschließend werden die daneben benötigten flexiblen Datentreuhandlösungen vorgestellt, die entweder privatwirtschaftlich angeboten oder staatlich aufgesetzt werden können. In einem dritten Schritt sollen die konkreten Ausgestaltungsparameter dieser verschiedenen Datentreuhandlösungen erörtert werden.

5.2.1 Koordinierungsstelle für den Datenzugang

5.2.1.1 Findata

In Finnland werden Datenzugangsansprüche aus dem Secondary Use Act über eine Data Permit Authority, Findata, koordiniert, das am Finnish Institute for Health and Welfare betrieben wird, von den übrigen Aktivitäten des Instituts allerdings unabhängig ist. Sie untersteht der Aufsicht des Ministry of Social Affairs. Wird eine Erlaubnis des Datenzugangs durch Findata erteilt,[105] sammelt Findata die Daten von den datenhaltenden Instanzen, kombiniert und pseudonymisiert und anonymisiert sie gegebenenfalls und stellt sie dem Antragsteller anschließend über einen spezifisch einzurichtenden sicheren Hosting-Service zur Verfügung, vgl. Sect. 10 No. 6 Secondary Use Act. Wurden die Daten auf Grundlage einer datenschutzrechtlichen Einwilligung zur Verfügung gestellt, darf Datenzugang nur gewährt werden, wenn dies von der Reichweite der Einwilligung gedeckt ist, vgl. Sect. 43. Datenhalter sind öffentliche Stellen, wie National Data Repositories, Healthcare and Social Welfare Care, Data Archives, aber auch registrierte Daten privater Anbieter von Sozial- und Gesundheitsdienstleistungen.[106]

5.2.1.2 My Health Systems

In Australien ist der Zugang zu Forschungsdaten über den My Health Records Act gewährleistet – ein staatlich betriebenes System zur Bereitstellung von Gesundheitsinformationen über Gesundheitsversorgungsempfängerinnen und -empfänger für die Zwecke der Gesundheitsversorgung der Empfängerinnen und Empfänger (Primärnutzung) sowie für andere Zwecke, zum Beispiel Zwecke von Wissenschaft und Forschung (Sekundärnutzung). Die Gesundheitsversorgungsempfängerinnen und -empfänger haben eine Gesundheitsakte in diesem System, sobald sie sich entweder registriert oder, für den Fall, dass ein Opt-Out-Modell vom Ministerium angeordnet wird, sie nicht ausoptierten. Der Systembetreiber betreibt den National Repositories Service, der die wichtigsten Datensätze der Gesundheitsakte speichert. Andere Datensätze werden von registrierten Repository-Betreibern gespeichert. Zusammen bilden diese Datensätze die persönliche Gesundheitsakte der Gesundheitsversorgungsempfängerinnen und -empfänger.

Gesundheitsdaten können aus der persönlichen Gesundheitsakte von Empfängerinnen und Empfängern der Gesundheitsfürsorge zum Zweck der Forschung durch den Systembetreiber zur Verfügung gestellt werden, wenn es sich um anonymisierte Daten handelt oder aber um (personenbezogene) Gesundheitsdaten, sofern die Betroffenen zustimmen, Sect. 15 und 83.

Erforderlich ist dafür aber, dass das Data Governance Board, das mit verschiedenen Expertinnen und Experten besetzt ist und von verschiedenen Gremien beraten wird, einen Antrag auf die Nutzung von Daten zu Forschungszwecken positiv bescheidet, Sect. 33 und 109 A. Die Antragstellerinnen und -steller müssen zuvor den Nutzungsbedingungen zustimmen[107] und einen Risikomanagementplan beifügen, auf dessen Grundlage das Board insbesondere das Risiko eines Verlustes oder Missbrauchs der Daten beurteilt.[108] Für den Zugang zu personenbezogenen Daten ist außerdem stets die Einwilligung der Betroffenen erforderlich. Sofern das Board feststellt, dass eine ethische Prüfung angezeigt ist, muss es die Zustimmung vom Australian Institute of Health and Welfare (AIHW) einholen.[109]

Findata sowie das My Health Record System sind Datentreuhänder, die Daten sowohl zentral speichern als auch als Datenintermediäre zwischen dezentralen Drittspeichern und Datennachfragern agieren. Wesentlich dürfte vor allem ihre Koordinierungsfunktion sein.

5.2.1.3 Ausgestaltung europäischer Koordinierungsstellen

Einer solchen Koordinierungsstelle bedarf es sowohl auf europäischer Ebene als auch in den einzelnen Mitgliedstaaten, wobei die europäische Koordinierungsstelle für einen mitgliedstaatübergreifenden Datenzugang zuständig sein sollte und die mitgliedstaatlichen Stellen für den auf den jeweiligen Mitgliedstaat beschränkten Datenzugangsanspruch. Für die europäische Stelle genügt die Erfüllung einer Maklerfunktion zwischen den mitgliedstaatlichen Koordinierungsstellen. Die mitgliedstaatlichen Koordinierungsstellen aber müssten auch für die Zurverfügungstellung der Daten über entsprechende sichere Serverlösungen zuständig sein, wie dies etwa in den Forschungsdatenzentren in Deutschland geschieht. Außerdem könnte die Koordinierungsstelle

entweder auf europäischer oder aber auf nationaler Ebene die Datenzugangsentscheidung sowie die Entscheidung über die Modalitäten des Datenzugangs und der Anschlussnutzung von Daten und Forschungsergebnissen treffen, sofern der Gesetzgeber einen Entscheidungsspielraum belässt. Zu definieren ist auch, an wen Daten weitergegeben werden dürfen, und es sind Maßnahmen gegen Missbrauch vorzusehen. In Australien etwa findet eine Datenweitergabe an Versicherer nicht statt, Sect. 16 und 109 A. Auch spezifische Zwecke der Anschlussnutzung sind untersagt, Sect. 70 A und 70 B. Die Nutzung von Daten für untersagte Zwecke ist eine Straftat, Sect. 71 A sowie ein Verstoß gegen den Privacy Act 1988, Sect. 72 und 73. Das Data Governance Board führt ein öffentlich einsehbares Register, aus dem unter anderem ersichtlich ist, wer Datenzugang beantragt hat.[110]

5.2.2 Flexible Datentreuhandlösungen

5.2.2.1 Datenspendetreuhand

Bedarf

Neben die Einzelregister und der Koordinierungsstelle müssen flexible Datentreuhandlösungen treten, um das Problem einer Datenunternutzung in der Forschung gesamtheitlich zu lösen.[111] Diese können einerseits Datenspendefunktion und andererseits Datenteilungsfunktion haben. Datenspendefunktion hat etwa die elektronische Patientenakte, die über die Telematikinfrastruktur der gematik von den gesetzlichen Krankenkassen zur Verfügung gestellt wird. Die Krankenkassen sind als Körperschaften des öffentlichen Rechts datenschutzrechtlich verantwortlich für die Datenverarbeitung in der elektronischen Gesundheitsakte, jedenfalls in Deutschland, vgl. § 341 Abs. 4 S. 1 SGB V.[112] Eine „Datenspende" könnte helfen, Daten im Einklang mit dem Datenschutzrecht für die Forschung zugänglich zu machen. Auch in Australien und Finnland sind derartige Datenspenden vorgesehen.[113] Eine Vorbildregelung findet sich im nationalen Recht auch in § 363 SGB V. Das Konzept der Datenspende ist für die medizinische Forschung so wichtig, weil es auf große Zustimmung in der Bevölkerung trifft. Nach einer Forsa-Umfrage im Auftrag der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF) sind knapp 79 Prozent der Deutschen zu einer solchen freiwilligen Datenspende bereit.[114]

Ebenso kommt in Betracht, dass private Stellen Datenspendefunktion erfüllen. Dann sind sie als PIMS einzustufen und unterliegen den oben genannten Regulierungsanforderungen. Vorstellbar ist es beispielsweise, dass PIMS Daten mit Relevanz für Gesundheitsdienstleister freigeben, etwa Daten aus Fitness-Trackern und Gesundheits-Apps. Diese Daten könnten auf Basis einer informierten Einwilligung in die elektronische Gesundheitsakte und von dort aus zu Zwecken der wissenschaftlichen Nutzung freigegeben werden. Sowohl die elektronische Patientenakte als auch privatwirtschaftlich organisierte PIMS zur Freigabe von Gesundheitsdaten zu Zwecken der Forschung könnten und sollten ihren Platz in einem europäischen Gesundheitsdatenraum finden.

Regulierungsanforderungen

Vorgaben zur Überführung der Daten in die Datentreuhand sowie zur Datenverarbeitung in der Datentreuhand

Hinsichtlich der Überführung der Daten in eine Datentreuhand sowie zur Datenverarbeitung in einer Datentreuhand sollte eine datenschutzrechtliche Verantwortlichkeitszuweisung vorgenommen werden, wie Art. 4 Nr. 7 DSGVO dies zulässt.[115] Auch die datenschutzrechtliche Verarbeitungsgrundlage zur Einspeisung von Daten in die Treuhand und zur Verarbeitung der Daten in der Treuhand ist zu klären. In Österreich beruht sie für die elektronische Gesundheitsakte auf einer gesetzlichen Erlaubnisnorm mit Widerspruchsmöglichkeit,[116] in Deutschland auf einer Einwilligung. Während eine gesetzliche Erlaubnisnorm mit Widerspruchsmöglichkeit schon aufgrund des Status-quo-Bias[117] zu einer erhöhten Datenverfügbarkeit führen würde, trägt die Einwilligungslösung der informationellen Selbstbestimmung in größerem Umfang Rechnung. Es ist am Gesetzgeber zu entscheiden, welchem Interesse der Vorzug gegeben werden soll: Forschungsfreiheit, Gesundheit und Wohlbefinden der Allgemeinheit bei gleichzeitiger Wahrung des informationellen Selbstbestimmungsrechts durch Widerspruchsmöglichkeit oder umfassende Gewährleistung des informationellen Selbstbestimmungsrechts bei Zurückstellung von Forschungsfreiheit und Gesundheit und Wohlbefinden der Allgemeinheit. Eine gesetzliche Erlaubnisnorm mit Widerspruchsmöglichkeit ließe sich etwa auf die Öffnungsklausel des Art. 9 Abs. 2 lit. h DSGVO stützen (wie dies in Österreich getan wurde). Insofern wäre sowohl eine unionale als auch eine nationale Verarbeitungsgrundlage möglich.

Wird die Überführung der Daten und die Datenverarbeitung in der elektronischen Gesundheitsakte oder einer elektronischen Patientenakte auf Grundlage einer Einwilligung gewährleistet, so sollte eine größtmögliche Granularität der Einwilligung gewährleistet werden, um datenschutzrechtlichen Bedenken aus dem Weg zu gehen.[118] Sowohl im Hinblick auf eine Einwilligungslösung als auch im Hinblick auf einen gesetzlichen Erlaubnistatbestand sollte vorgegeben werden, welche Gesundheitsdiensteanbieter unter welchen Voraussetzungen auf welche Dokumente und Daten Zugriff erhalten. Die Patientinnen und Patienten sollten unbedingt die Hoheit über die sie betreffenden Daten behalten, unabhängig davon, ob eine Einwilligungs- oder eine Widerspruchslösung gewählt wird.

Datenspende

Um eine Datennutzung für die Wissenschaft zu gewährleisten, ist es vor allem erforderlich, eine Datenfreigabe an existierende Register und antragsbefugte Wissenschaftlerinnen und Wissenschaftler vorzusehen. Auch diese Datenfreigabe kann sowohl auf Grundlage einer informierten Einwilligung als auch auf Grundlage eines gesetzlichen Erlaubnistatbestandes mit Widerspruchslösung vorgesehen werden, mit den bereits benannten Anreizen und Auswirkungen auf Forschungsfreiheit, Allgemeingesundheit/Allgemeinwohl und informationelle Selbstbestimmung.

Zusätzlich zu den datenschutzrechtlichen Anforderungen ist hier insbesondere vorzusehen, welche Anforderungen die Wissenschaftlerinnen und Wissenschaftler zu erfüllen haben, an die die Daten freigegeben werden. Untersuchungen haben gezeigt, dass der Kreis der Wissenschaftlerinnen und Wissenschaftler nicht zwingend auf die nicht kommerzielle Forschung zu beschränken sein muss, solange der Forschungszweck an das Gemeinwohlinteresse gebunden wird.[119] Gemeinwohl in diesem Sinne ließe sich definieren als Tätigkeit, deren Erbringung nicht allein durch individuelle – wirtschaftliche, eigennützige, freundschaftliche oder familiäre – Ziele motiviert ist, sondern sich zumindest auch als Ausdruck gesellschaftlicher Verantwortung erweist.[120] Die Voraussetzungen für eine Datenspende sollten ebenso definiert werden wie die erlaubte Anschlussnutzung der Daten sowie der Forschungsergebnisse (Veröffentlichungspflicht). Gleichermaßen sollten Maßnahmen gegen den

Missbrauch von Daten, zum Beispiel der Verlust der Approbation eines Arztes oder einer Ärztin, der Ausschluss von der Nutzung der auf Grundlage der Datenspendeoption bereitgestellten Daten für einen gewissen Zeitraum et cetera, getroffen werden. Es bedarf einer Institution, die die Entscheidung darüber trifft, ob die Voraussetzungen für die Datennutzung durch die antragstellenden Wissenschaftlerinnen und Wissenschaftler vorliegen, oder nicht, und die über die Modalitäten und den Umfang des Datenzugangs entscheidet.[121]

Wird die Datenspende auf Grundlage einer Einwilligung ermöglicht, so sollte eine breite Einwilligung, etwa auf Grundlage der Medizininformatik-Initiative möglich sein.[122]

Darüber hinaus sind die Anforderungen an die technische Infrastruktur zu definieren. Die Sicherheitsvorkehrungen sollten aufgrund der besonderen Sensibilität der verarbeiteten Daten besonders hoch werden.[123]

PIMS

PIMS zur Datenteilung im Gesundheitssektor könnten Daten auf Grundlage einer informierten Einwilligung zum Beispiel in die elektronische Patientenakte freigeben. Ihr Regulierungsbedarf ergibt sich grundsätzlich aus den obigen Ausführungen im Kapitel „PIMS“. PIMS zur Datenteilung im Gesundheitssektor weisen aber einen entscheidenden Unterschied zu außerhalb des Gesundheitssektors tätigen PIMS auf: Das schutzwürdige Interesse an der Gewährleistung von Forschungsfreiheit im Gemeinwohlinteresse und das Interesse an der Verbesserung der Allgemeingesundheit rechtfertigen es, in diesem Bereich einen Anreiz zum Datenteilen mit Wissenschaft und Forschung im Gemeinwohlinteresse zu gewährleisten. Insbesondere eine Rückvergütung der Nutzerinnen und Nutzer sollte daher nicht per se ausgeschlossen werden. Es ist außerdem nicht ersichtlich, weshalb allein datenaltruistische Organisationen die Möglichkeit einer standardisierten und möglicherweise breiteren Einwilligung (sofern diese, wie im Data Governance Act vorgesehen, durch delegierten Rechtsakt für zulässig erklärt wird) in Anspruch nehmen können sollten. Datenaltruistische Organisationen müssen im Unterschied zu nicht datenaltruistischen PIMS ihre Dienste auf einer unentgeltlichen Basis anbieten, vgl. Art. 16 DGA-E, der gesamtgesellschaftliche Nutzen einer

Datenspendetreuhand ist in beiden Fällen aber identisch, sofern die Datenverarbeitung, zu deren Zweck die Daten gespendet werden, an die Bedingung des gesamtgesellschaftlichen Nutzens geknüpft wird.

5.2.2.2 Datenteilungstreuhand

Andererseits lässt sich die Datentreuhand aber auch als Stelle zum Teilen und Auswerten großer Datenbestände von zwei oder mehreren Dateninhabern denken.

Bedarf

Die Forschung an großen Datenbeständen in der Medizin ist unerlässlich. Mit sogenannten Radiomics-Analysen von Bilddaten können zum Beispiel wiederkehrende Texturmarker identifiziert werden, die Rückschlüsse auf Pathologien, Gewebeeigenschaften oder Krankheitsverläufe von Patientinnen und Patienten ermöglichen.[124] Aus der Zusammenschau großer Datenmengen aus unterschiedlichen medizinischen Disziplinen können Biomarker generiert werden, die zum Beispiel bei der Krebserkennung, der Diagnose, der Beurteilung der Prognose, der Vorhersage des Ansprechens auf eine Behandlung und der Überwachung des Krankheitsstatus helfen könnten. Die Einsatzmöglichkeiten und der Erfolg dieser Datenauswertung hängen maßgeblich davon ab, dass möglichst große Datenbestände systematisch analysiert werden können. Aus rein medizinischer Sicht wäre insofern die Erstellung von Datenbanken, die große Mengen an medizinischen Daten aller medizinischer Disziplinen (Bilddaten, Labordaten, Pathologiedaten) kombinieren, wünschenswert. Das Datenschutzrecht aber stellt für derartige Kombinationen von Daten und Analyseverfahren großer Datenbestände hohe Hürden auf.[125] Eine Datentreuhand böte die Option, Datenschutz und Datenauswertung zusammen zu denken, indem ein sicherer Raum zur Datenauswertung geschaffen würde, in welchem die Daten zwar geteilt würden, jedoch weder die Datengeber selbst noch der Datentreuhandanbieter auf diese Daten real zugreifen und sie weiterreichen könnten. Technisch ermöglicht wird lediglich die algorithmisierte Auswertung der Daten und allein die Auswertungsergebnisse würden anschließend an die Datengeber herausgegeben. Die Daten in der Datentreuhand würden hingegen wieder gelöscht.[126]

Verschiedene Lösungen zur Ermöglichung eines solchen Datenaustausches werden zwar derzeit am Markt erprobt. Ein freiwilliges Datenteilen zu Zwecken von Wissenschaft und Forschung kommt dennoch nicht voran. Das mag einerseits an fehlender Rechtssicherheit liegen, andererseits aber auch an einem nicht unerheblichen technischen Aufwand. Denn sollen Daten zwischen verschiedenen Akteuren geteilt werden, müssen Voraussetzungen geprüft, Datenstandards vereinheitlicht und die Bedingungen der Datenzugangsgewährung erörtert werden. Dies dürfte für die zur Datenteilung angefragten Personen und Einrichtungen, zum Beispiel entsprechende Kliniken, ein nicht unerheblicher Aufwand sein, den sie kaum auf freiwilliger Basis ohne entsprechende Kostenerstattung erfüllen werden wollen.[127] Neben der rechtlichen Ermöglichung von Datentreuhandmodellen muss also zwingend gleichzeitig über die Vereinheitlichung von Datenstandards und Schnittstellen nachgedacht werden.[128]

Verhältnis zum Federated Learning

Federated Learning bedeutet, dass Algorithmen auf dezentral gespeicherten Daten trainiert werden. Die Notwendigkeit einer zentralen Infrastruktur besteht in Fällen des Federated Learnings ausschließlich in der Bereitstellung der technischen Plattform und anwendungsspezifischer Verschlüsselung[129] sowie gegebenenfalls in der anschließenden Bündelung der Auswertungsergebnisse. Federated Learning stößt aber an seine Grenzen in Fällen vertikal verteilter Daten (beispielsweise unterschiedliche Daten derselben Personengruppe, die an unterschiedlichen Orten – zum Beispiel verschiedenen Krankenhäusern – gespeichert sind). Der Bedarf für eine zentrale Datentreuhandlösung bleibt insofern auch neben Federated Learning Modellen bestehen.[130] Die Auswertung vertikal verteilter Daten beispielsweise zu Zwecken der Covid-19-Nebenwirkungsforschung gelingt sehr viel besser in derartigen zentralen Datentreuhandstrukturen, die auch als Data Clean Rooms bezeichnet werden.

Regulierungsanforderungen

Eine Datenteilungstreuhand kann sowohl als privatwirtschaftliche als auch staatliche Lösung angeboten werden. Für beide Konzepte existieren bereits Regulierungsvorschläge, die im Folgenden erläutert werden. Ziel muss es jeweils sein, durch die Gewährleistung IT-sicherheitsrecht-

lich höchster Standards einen sicheren Raum zur Auswertung großer Datenbestände zu schaffen und diese Datenauswertung auf eine datenschutzrechtlich sichere Rechtsgrundlage zu stellen.

Privatwirtschaftliche Lösung

Derzeit ist die Zusammenführung und Auswertung von Datenbeständen in einer Serverstruktur, die von einem Dritten angeboten ist, datenschutzrechtlich auf Grundlage einer ausdrücklichen Einwilligung des Patienten oder der Patientin (Art. 9 Abs. 2 lit. a DSGVO) sowie auf Grundlage eines überwiegenden Interesses (Art. 9 Abs. 2 lit. j) DSGVO i. V. m. § 27 BDSG möglich. Beide Rechtsgrundlagen bringen für den Fall der Auswertung großer Datenbestände aber eine ganz erhebliche Rechtsunsicherheit mit sich. Zur Behebung des Unternutzungsproblems von Daten in der medizinischen Forschung ist die Beseitigung dieser Rechtsunsicherheit angezeigt. Werden an Datentreuhandstrukturen erstens hohe Anforderungen mit Blick auf die IT-Sicherheit gestellt, wird zweitens eine Weitergabe der Rohdaten untersagt und unter Strafe gestellt, sind drittens die auszuwertenden Daten technisch und strafrechtlich bereits so geschützt, dass das Risiko für die Rechte und Interessen der Betroffenen minimiert ist, könnte ein gesetzlicher Erlaubnistatbestand die Überführung der Daten in diese Datentreuhand sowie die Auswertung der Daten in der Datentreuhand gestatten. Entsprechende Gesetzgebungsvorschläge wurden bereits unterbreitet.[131] Entsprechend regulatorisch ausgestaltet hat die Datentreuhand auch datenschutzrechtliche Vorteile: Die Daten werden zu keinem Zeitpunkt real geteilt, sondern allein in der sicheren Umgebung der Datentreuhand ausgewertet. Geteilt werden allein die Auswertungsergebnisse, während die ausgewerteten Datenbestände in der Treuhand nach dem Auswertungsvorgang wieder gelöscht werden. Es existiert kein Anspruch Dritter auf Zugang zu den in der Datentreuhand gespeicherten Daten. Die Datentreuhand ist vielmehr allein die Infrastrukturlösung zum risikoarmen Teilen und Auswerten großer Datenbestände.[132] Die Erlaubnis zur Nutzung einer konkreten Datentreuhandstruktur für ein spezifisches Datentreuhandprojekt ließe sich entweder über eine zentrale Permit Authority erteilen, oder aber die Datentreuhandmodelle müssten vorab über eine staatliche Stelle zertifiziert werden und könnten bei Erfüllung der Zertifizierungsanforderungen selbst berechtigt sein, über die Nutzung

der Datentreuhandstruktur für das spezifische Forschungsprojekt zu entschieden. Am Markt finden sich erste Unternehmen, die derartige Dienste anbieten.[133]

Staatliche Lösung

Andere Vorschläge gehen hin zu einer staatlichen Datentreuhandlösung. Die *Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten (NGD)* hat bereits 2018 ein solches staatliches Modell zur Teilung und Auswertung von Datenbeständen entwickelt[134] und auch ein aktuelles Gutachten im Auftrag des BMBF sieht eine solche Lösung vor.[135] Darin wird vorgeschlagen, eine Organisationsstruktur zu schaffen, in die Einrichtungen des Gesundheitswesens die bei ihnen vorgehaltenen Gesundheitsdaten einbringen und auswerten können. Dafür soll eine „neutrale Stelle" geschaffen werden, die der staatlichen Aufsicht unterliegt. Sowohl öffentliche als auch private Einrichtungen des Gesundheitswesens könnten diese nutzen. Dazu gehören nationale Einrichtungen des Gesundheitswesens wie das Robert-Koch-Institut (RKI), Krankenversicherungen und Forschungsinstitutionen; es ließen sich aber durchaus auch europäische Einrichtungen an das NGD anschließen. Das Modell sieht vor, dass die Nutzung des NGD, sofern sie im Bereich der öffentlichen Gesundheitsversorgung erfolgt, dazu verpflichtet, Daten auf Anfrage anderer Nutzerinnen und Nutzer zu Analysezwecken an das NGD zu übermitteln. Die in der freien Wirtschaft agierenden Unternehmen hingegen sollen freiwillig partizipieren.[136] Es ließe sich aber darüber nachdenken, ob in einem solchen Modell auch Datenzugangsansprüche zu privaten Gesundheitsdiensteanbietern begründet werden sollten.[137] Allein die Analyseergebnisse werden aus der Datentreuhand ausgespielt, die ausgewerteten Daten werden anschließend gelöscht.[138]

Das Konzept ist ähnlich dem privatwirtschaftlichen Modell ausgestaltet: Datenschutzrechtlich stellen sich dieselben Fragen und auch bei der Wahl dieses Datentreuhandmodells bedarf es einer Entscheidung über die datenschutzrechtliche Verarbeitungsgrundlage. Auch hier kommen die Einwilligungs- und Erlaubnistatbestandslösung mit der Widerspruchsmöglichkeit in Betracht. Eine Zentralinstanz zur Datenteilung und -auswertung – egal, ob auf europäischer, nationaler oder Bundeslandebene – birgt allerdings stets höhere Risiken für das infor-

mationelle Selbstbestimmungsrecht der Betroffenen als dezentrale Lösungen, wie sie derzeit privatwirtschaftlich entstehen. Andererseits speichert NGD die Daten lediglich für einen kurzen Zeitraum zentral, im Grundsatz bleiben sie dezentral bei den Nutzerinnen und Nutzern gespeichert. Technisch dürfte sowohl der europäische Gesetzgeber als auch der Bundes- und Landesgesetzgeber in der Lage sein, höchsten IT-Sicherheitsanforderungen zu entsprechen. Auch für privatwirtschaftlich tätige Datentreuhänder ließe sich ein entsprechend hohes Sicherheitsniveau aber gesetzlich vorschreiben und staatlich zertifizieren. Es spricht aus problemlösungsorientierter Sicht nichts dagegen, sowohl staatliche als auch privatwirtschaftliche Lösungen zuzulassen.

5.2.3 Geeignetheit von DGA-E und EHDS zur problemlösungsorientierten Regulierung von Datentreuhändern im Gesundheitssektor

Auch zur problemlösungsorientierten Regulierung von Datentreuhändern im Gesundheitssektor trägt der Data Governance Act wenig bei. Die Vorgaben von Kapitel 2 sehen immerhin vor, dass „Daten im Besitz der öffentlichen Hand", worunter insbesondere in staatlichen Registern vorgehaltene Daten fallen dürften, keinen Ausschließlichkeitsvereinbarungen unterworfen werden dürfen. Die Vorgaben greifen damit potenziell entstehenden Konflikten der Datennutzung aus der öffentlichen Hand vor. Auf die private Datenteilungstreuhand findet der DGA-E keine Anwendung, weil sie lediglich zwischen geschlossenen Anbieter- und Nachfragegruppen Datenzugang und Zugang zu Datenanalyseergebnissen mittelt.[139] Die staatliche Datenteilungstreuhand lässt der DGA-E jedenfalls nicht ohne Weiteres zu, denn Daten in staatlicher Hand, die die Voraussetzungen des Art. 3 DGA-E erfüllen – und damit zumindest potenziell auch in der Hand staatlicher Lösungen sind – dürfen im Grundsatz nicht lediglich einem beschränkten Personenkreis zugänglich gemacht werden. Etwas anderes gilt nur, wenn dies für die Erbringung eines Dienstes im allgemeinen Interesse erforderlich ist, Art. 4 Abs. 2 DGA-E. Dies sollte zwar für die medizinische Datenteilungstreuhand begründbar sein, ist aber auf europäischer Ebene abzuklären. Für diese Lesart dürfte auch sprechen, dass Kapitel 2 des DGA-E auf Daten gerichtet ist, die mithilfe öffentlicher Gelder generiert wurden und nicht auf solche, die lediglich mithilfe öffentlicher Gelder ausgewertet wurden.

Für die Auswertungsergebnisse greift letzteres Argument aber freilich nicht. Allerdings gelten die Vorgaben des Data Governance Acts nicht für Daten, die bereits zu Zwecken der Weiterverwendung erhoben wurden, sondern nur für solche Daten, deren Verwendungszweck sich ändert.

Interessant ist die Frage, ob die ePA den Vorgaben des Datenaltruismus oder denen für Datenintermediäre unterliegt, also einen Dienst zur gemeinsamen Datennutzung im Sinne des (Art. 9 Abs. lit. b) DGA-E bereitstellt. Als von den gesetzlichen Krankenkassen angebotener Service dürfte es sich allerdings schon deshalb nicht um einen Commercial Service im Sinne des Art. 2 Abs. 2a DGA-E handeln, weil die gesetzlichen Krankenkassen Körperschaften des öffentlichen Rechts sind. Damit unterliegen sie nach der Ratsfassung der DGA-E vom 24. September 2021 nicht den Vorgaben für Datenintermediäre, vgl. Art. 2 Abs. 2a lit. d DGA-E.[140] Insofern stellt sich die Frage einzig für ePA-Angebote privater Krankenkassen, die derzeit aber noch nicht am Markt existieren (aber in Paragraf 341 IV, V SGB V angelegt sind). Diese fielen zumindest potenziell entweder unter die Vorgaben für Datenintermediäre aus Kapitel 3 des DGA-E oder aber unter die Vorgaben für altruistische Datenintermediäre aus Kapitel 4 DGA-E. Weil es für die datenaltruistischen Organisationen aber Voraussetzung ist, dass diese selbst ohne Erwerbszweck tätig sind und dies auf in privater Rechtsform organisierte Krankenkassen[141] nicht zutreffen dürfte, kann eine solche privat angebotene ePA einzig den Vorgaben des Kapitels 3 DGA-E unterliegen, sofern dessen Anwendungsbereich eröffnet ist. Die ePA stellt eine rechtliche und technische Beziehung zwischen den Dateninhaberinnen und -inhabern (den Versicherten) einerseits und möglichen Datennutzerinnen und -nutzern andererseits her. Ihrer Eigenschaft als Intermediation Service gemäß Art. 2 Abs. 2a DGA-E[142] könnte allenfalls entgegenstehen, dass die ePA lediglich für den Personenkreis von Versicherten und Nutzungsberechtigten geöffnet ist. Wollte man dies als geschlossenen Personenkreis erachten, wäre die erforderliche Ausrichtung eines Datenintermediärs auf die Vermittlung zwischen einer unbestimmten Zahl an Dateninhaberinnen und -inhabern sowie Datennutzerinnen und -nutzern nicht erfüllt. Auch ließe sich begründen, dass lediglich eine einzige Versicherte oder ein einziger Versicherter die jeweilige ePA nutzt und auch aus diesem Grund keine Vermittlung zwi-

schen einer unbestimmten Zahl an Dateninhaberinnen und -inhabern sowie Datennutzerinnen und -nutzern vorliegt. Dagegen spricht aber, dass potenziell alle bei Erfüllung der Anforderungen zum Kreis der Versicherten und Nutzungsberechtigten zählen können und potenziell jede und jeder Versicherte einer gesetzlichen Krankenkasse eine ePA nutzen kann. Derartige Dienste will der DGA-E gerade nicht vom Anwendungsbereich ausschließen, er fordert lediglich, dass die Dienste für eine im Voraus nicht bestimmte Anzahl sowohl an Datennutzerinnen und -nutzern als auch an Dateninhaberinnen und -inhabern offenstehen. Der DGA-E dürfte daher auch dann anwendbar sein, wenn er bestimmte Anforderungen an Dateninhaberinnen und -inhaber oder Datennutzerinnen und -nutzer stellt.[143] Ob eine von privaten Krankenkassen betriebene ePA ein Datenintermediär im Sinne des Art. 2 Abs. 2a DGA-E wäre, kann aufgrund dieser verschiedenen Auslegungsmöglichkeiten derzeit noch nicht eindeutig beantwortet werden. Insbesondere das von Datenintermediären einzuhaltende Verbot vertikaler Integration gemäß Art. 9 DGA-E würde die die ePA anbietenden privaten Krankenkassen vor erhebliche Herausforderungen stellen. Von diesen Vorgaben könnte auch der EHDS-Act nicht abweichen, da der Data Governance Act Mindestvorgaben setzt, über die lediglich hinausgegangen, nicht aber hinter ihnen zurückgeblieben werden kann.

Gesetzliche Krankenkassen agieren nach dem Urteil des EuGH vom 11. Juni 2009, C-300/07, Rn. 49 ohne Gewinnerzielungsabsicht, weshalb sie grundsätzlich als datenaltruistische Organisation in Betracht kommen. Kapitel IV DGA-E soll die freiwillige Datenbereitstellung durch Einzelpersonen oder Unternehmen zum Wohl der Allgemeinheit (Datenaltruismus) erleichtern (ErwG. 35 nennt in diesem Zusammenhang ausdrücklich die Gesundheitsversorgung). Hierzu sollen sich Organisationen, die Datenaltruismus betreiben oder besser fördern, als „in der Union anerkannte datenaltruistische Organisationen“ eintragen lassen können, um das Vertrauen in ihre Tätigkeit zu stärken. Es kann ein gemeinsames Einwilligungsformular für den Datenaltruismus entwickelt werden, um die Kosten für die Einholung der Einwilligung zu senken und die Übertragbarkeit der Daten zu erleichtern.[144] Insbesondere sollen Rechtsunsicherheiten im Zusammenhang mit Daten, die auf altruistischer Grundlage für die wissenschaftliche Forschung und für Statistikzwecke zur Verfügung gestellt werden, ausgeräumt werden (ErwG. 39).

Der Datenaltruismus weist eine gewisse Nähe zur Datenfreigabe nach § 363 Abs. 1, 8 SGB V auf.[145] Voraussetzung ist aber, dass die Datenaltruismustätigkeiten über eine rechtlich unabhängige Struktur ausgeübt werden, die von anderen Tätigkeiten, die die datenaltruistische Organisation durchführt, getrennt ist, Art. 16 lit. c DGA-E. Ist diese Voraussetzung erfüllt, könnte in Zukunft ein über ein Endgerät bereitgestelltes Einwilligungsformular im Sinne des Art. 22 DGA-E zur Einholung der informierten Einwilligung gem. § 363 Abs. 2 SGB V verwendet werden.

5.3 Datentreuhänder im Mobilitätssektor

5.3.1 Daten des vernetzten Autos: Die bisherige Diskussion

Ein sehr großer Teil von Mobilitätsdaten entsteht in vernetzten Fahrzeugen, die über eine Vielzahl von Sensoren ständig Daten generieren und verarbeiten, beispielsweise auch für das Betreiben von Fahrassistenzsystemen. Gleichzeitig sind die Autos über mobile Kommunikation mit anderen Akteuren verbunden (Konnektivität), mit denen sie ständig (auch in Echtzeit) Daten austauschen können. Insofern sind vernetzte Fahrzeuge vergleichbar mit vielen anderen smarten Geräten (Internet der Dinge). Die dabei gesammelten Daten können sich auf vielfältige Aspekte beziehen: Technische Daten des Betriebs des Fahrzeugs (und seiner Komponenten), Daten über den Standort, Geschwindigkeit, Fahrverhalten der Autofahrerinnen und Autofahrer, Daten über äußere Bedingungen wie Wetter, Verkehr (inklusive Staus), Straßenzustand, aber auch Daten über die Nutzung von Entertainmentangeboten und anderen online über das Auto angebotenen Services durch die Autoinsassen. Mit der zunehmenden Verbreitung von vernetzten Autos entsteht durch den Betrieb dieser Fahrzeuge eine immer größere Menge von Mobilitätsdaten, die (auch in Realzeit) von einer Vielzahl von Akteuren genutzt werden könnten. Neben den Autoherstellern, ihren Zulieferern sowie Kfz-Reparatur- und Wartungsbetrieben (Ferndiagnose und Fernwartung) sowie Versicherungen (mit neuen Versicherungsmodellen) können solche Mobilitätsdaten aber auch interessant für viele weitere innovative Serviceanbieter sein, die ihre Dienstleistungen innerhalb des Ökosystems vernetzten Fahrens den Autonutzerinnen und -nutzern anbieten können (Navigation, Entertainment, Onlineshopping et cetera). Besonders wichtig

können solche Daten aber auch zur Erfüllung öffentlicher Aufgaben sein, wie Verkehrssicherheit, Unfallforschung, Verkehrssteuerung, Aufklärung von Unfällen, Umweltschutz sowie für die wissenschaftliche Forschung.[146]

Seit Jahren gibt es in der EU eine intensive wettbewerbspolitische Auseinandersetzung über die Frage des Zugangs von Firmen, Autonutzerinnen und -nutzern sowie öffentlichen Institutionen zu diesen im Fahrzeug generierten Daten („access to in-vehicle data and resources").[147] Der Ausgangspunkt dieses Konflikts liegt in der Entscheidung der Autohersteller für ein bestimmtes Governance-Konzept für das vernetzte Auto („Extended Vehicle"-Konzept), das ihnen die exklusive Kontrolle über die in den Autos generierten Daten sichert. Viele andere Serviceanbieter, die den Autonutzerinnen und -nutzern ihre Dienstleistungen im vernetzten Auto anbieten möchten, befürchten, dass die Autohersteller diese exklusive Kontrolle über die Daten des vernetzten Autos dazu benutzen werden, um sie von dem lukrativen Geschäft mit den neuen vielfältigen Dienstleistungen zu verdrängen beziehungsweise einen hohen Preis für den Zugang zu diesen Märkten verlangen.[148] Die Interessengegensätze zwischen den Autoherstellern einerseits und allen anderen Stakeholdern in dem sich herausbildenden Ökosystem vernetzten Fahrens andererseits wurden bereits auf der von der Kommission initiierten C-ITS Plattform deutlich, auf der sich die Stakeholder nicht auf Lösungen für den Zugang zu diesen Mobilitätsdaten einigen konnten.[149] Eine von der Kommission beauftragte Studie kam 2017 zu dem Schluss, dass das von den Autoherstellern angewendete „Extended Vehicle"-Konzept, unter anderem wegen der daraus folgenden Wettbewerbsprobleme, keine geeignete Problemlösung ist und deshalb andere Lösungen vorzuziehen sind.[150] Eine dieser Lösungen war das sogenannte Shared-Server-Konzept, das einer Datentreuhandlösung entspricht. Obwohl die Kommission die Notwendigkeit einer Lösung dieses Problems des „access to in-vehicle data and resources" anerkannt hat,[151] hat sie bis heute keinen Lösungsvorschlag vorgelegt.

Im Folgenden werden wir zunächst die im Hinblick auf die Daten aus vernetzten Fahrzeugen bestehenden verschiedenen Probleme genauer analysieren und anschließend Lösungsvorschläge diskutieren. Hierbei

sollen für diese Studie insbesondere auch der Vorschlag einer datentreuhänderischen Lösung vorgestellt werden, der in der aktuellen Diskussion bisher nicht genügend berücksichtigt wurde.

5.3.2 Problemanalyse

5.3.2.1 Unfallforschung im vernetzten Fahrzeug

Für Daten im Mobilitätssektor bestehen im Wesentlichen drei Probleme, die jeweils unterschiedliche Problemlösungskonzepte erfordern: Bei vernetzten Fahrzeugen stellt sich, erstens, das Problem der Unfallaufklärung von Fahrzeugen mit automatisierter Fahrfunktion. Dieses Problem wird bereits mit einer Datentreuhand sowie verschiedenen Datenzugangsverpflichtungen zu lösen versucht: Spezifische Daten aus Fahrzeugen mit automatisierter Fahrfunktion müssen an Dritte übermittelt und können für Zwecke der Unfallforschung Dritten zugänglich gemacht werden, § 63a Abs. 3 und 5 StVG. Erfassen soll diese Daten ein zugangsmoderierender Datentreuhänder.[152] Zu unterscheiden ist § 63a StVG von § 1g Abs. 5 StVG, nach welchem das Kraftfahrtbundesamt berechtigt ist, nichtpersonenbezogene Daten aus Fahrzeugen mit autonomer Fahrfunktion für verkehrsbezogenen Gemeinwohlzwecke, u. a. die Unfallforschung, Forschungsstellen zugänglich zu machen.[153] Diese Regelungen sind noch sehr jung und werden erst nach einiger Zeit zeigen, ob sie als Problemlösungsansatz tatsächlich taugen oder ob gesetzgeberisch nachgesteuert werden muss. Entscheidend ist, dass man bei der Aufklärung der Unfallursache bei teilweise automatisiertem Fahren auf Fahrzeugdaten, insbesondere bezüglich des Ein- und Ausschaltens der automatisierten Fahrfunktionen, zurückgreifen muss, die sich jedoch auf den Servern der Autohersteller befinden, welche zugleich interessierte Partei in diesen Streitigkeiten sind. Um folglich die Integrität der zur Verfügung zu stellenden Fahrzeugdaten zu sichern, scheint deshalb eine datentreuhänderische Lösung für diese speziellen Daten sinnvoll, sodass man bei Unfällen auf diese Daten manipulationssicher zurückgreifen kann. Es handelt sich jedoch um einen sehr speziellen Datensatz für einen ganz bestimmten, eng umrissenen Zweck. Selbstverständlich kann es auch andere spezielle Zugangslösungen zu bestimmten Daten des vernetzten Autos geben, bei denen die Daten außerhalb des Zugriffsbereichs der Automobilhersteller gespeichert werden sollten, sodass eine spezielle Datentreuhandlösung sinnvoll sein kann.

5.3.2.2 Datenzugang öffentlicher Institutionen und der Wissenschaft

Im Mobilitätsbereich insgesamt stellt sich, zweitens, das Problem des zunehmend artikulierten Bedürfnisses nach Datenzugang öffentlicher Stellen gegenüber privaten Datenhaltern, zum Beispiel zur Erfüllung von Aufgaben der Daseinsvorsorge. Der Staat begehrt beispielsweise Zugang zu Mobilitätsdaten aus Navigationssystemen, um intelligente Verkehrssysteme zu ermöglichen. Aber nicht nur für die Verkehrssteuerung, sondern auch für andere Gemeinwohlzwecke kann es wichtig sein, dass staatliche Institutionen Zugang zu bestimmten Arten von Mobilitätsdaten bekommen. Weiterhin könnte ein Zugang zu Mobilitätsdaten für Forschungszwecke wichtig sein. Auch hier stellt sich die Frage, ob Datentreuhandlösungen einen Beitrag leisten können.

5.3.2.3 Wettbewerbsproblem durch das „Extended Vehicle"-Konzept

Das im Mobilitätsbereich wesentliche Problem, das auch mit einer Datentreuhand gelöst werden könnte, ist aber, drittens, noch immer das mit den Daten im vernetzten Auto verbundene Wettbewerbsproblem. Es soll daher im Mittelpunkt der nachfolgenden Ausführungen stehen. Um den möglichen Beitrag einer Datentreuhandlösung und deren adäquater Ausgestaltung sinnvoll diskutieren zu können, ist es notwendig, das Problem genau zu analysieren und mit anderen Lösungsoptionen zu vergleichen.

Wichtig für das Verständnis dieses Wettbewerbsproblems ist, dass es sich um ein altbekanntes Problem in der Automobilindustrie handelt. Die Autohersteller haben seit Jahrzehnten immer wieder versucht, den Wettbewerb mit unabhängigen Anbietern auf den Märkten für Reparatur- und Wartungsdienstleistungen sowie Ersatzteilen zu behindern. Insofern sah sich die Wettbewerbspolitik seit Langem genötigt, Maßnahmen zu ergreifen, um einen unverzerrten Wettbewerb zwischen den Autoherstellern (und ihren Vertragswerkstätten) und den unabhängigen Reparatur- und Wartungsbetrieben (sowie Ersatzteilherstellern) zu sichern. Da hierfür der Zugang zu wesentlichen Reparatur- und Wartungsinformationen und Daten (insbesondere Fahrzeugdiagnosedaten), über die nur die Autohersteller verfügen, bereits bisher eine kritische Rolle gespielt hat, gibt es seit 2007 in der Kfz-Typenzulassungsverordnung eine (FRAND-ähnliche) Regulierung, die die Autohersteller dazu verpflichtet, Reparatur- und Wartungsinformationen (einschließlich Diagnosedaten)

zur Verfügung zu stellen, um einen solchen unverzerrten Wettbewerb auf den sogenannten Aftermärkten im Automobilbereich sicher zu stellen.[154] Hierbei handelt es sich um eine umfassende sektorspezifische Regulierung, die ein verpflichtendes Zugangsregime zu diesen Informationen (und Diagnosedaten) für unabhängige Kfz-Reparatur- und Wartungsbetriebe darstellt. Sie umfasst auch verpflichtende technische Schnittstellen (wie den in jedem Fahrzeug befindlichen OBD-Adapter), einheitliche Formate der Informationsbereitstellung, regulatorische Maßnahmen mit Bezug auf die Fahrzeugsicherheit sowie eine Gebührenregelung für die Bereitstellung dieser Informationen. Trotz kleinerer Probleme war diese Regulierung bisher in der Lage, den Wettbewerb auf den Kfz-Reparatur- und -Wartungsmärkten zu sichern.[155] Das Problem ist allerdings, dass diese Informations- und Datenzugangsregulierung bisher nicht adäquat an die neue Technologie vernetzter Fahrzeuge angepasst wurde.[156]

Wie können die mit dem von der Automobilindustrie verwendeten „Extended Vehicle"-Konzept auftretenden Probleme für Wettbewerb, Innovation und die Wahlfreiheit von Verbraucherinnen und Verbrauchern kurz zusammengefasst werden?[157] Nach diesem Governance-Ansatz für das vernetzte Fahrzeug haben die Automobilhersteller die exklusive Kontrolle (1) über die von den Autos generierten Daten, da diese direkt auf proprietäre (Backend-)Server bei den Automobilherstellern übertragen werden. Dies bedeutet, dass ohne Zustimmung der Automobilhersteller weder die Autonutzerinnen und -nutzer noch andere Akteure wie beispielsweise Versicherungen, Reparaturwerkstätten, Navigationsdienste oder auch öffentliche Stellen (zum Beispiel zur Verkehrsregelung) auf diese riesige Menge von Mobilitätsdaten zugreifen können. Zwar sind die Autohersteller bereit, den Zugang zu bestimmten Arten von Mobilitätsdaten gegen Entgelt zu verschaffen, aber nur zu ihren eigenen Bedingungen, das heißt sie können frei darüber entscheiden, welche Daten sie zur Verfügung stellen wollen und zu welchen Preisen und Bedingungen. Darüber hinaus verfügen die Automobilhersteller (2) auch über die exklusive Kontrolle über den technischen Zugang zum IT-System des Fahrzeugs, das heißt ohne Zustimmung der Autohersteller ist es nicht möglich, Ferndiagnosen, -reparaturen und -wartungen (Remote Diagnosis/Repair/Maintenance), beispielsweise durch unabhängige Serviceanbieter, durchzuführen, oder einen Zugang zum Dashboard des Fahrzeugs zu bekommen, um so den Auto-

nutzerinnen und -nutzern Angebote für Serviceleistungen zu machen.[158] Dies bedeutet, dass die Autohersteller die Fahrzeuge als geschlossene Systeme gestaltet haben, über die sie die exklusive Kontrolle ausüben.[159] Insofern besteht nicht nur ein Datenzugangsproblem, sondern auch ein Interoperabilitätsproblem, insbesondere bezüglich zum vernetzten Fahren komplementärer Dienstleistungen.[160]

Die Autohersteller haben sich folglich mit dem „Extended Vehicle"-Konzept eine Gatekeeper-Position für alle Sekundärmärkte im Ökosystem vernetzten Fahrens gesichert, weil ohne ihre Zustimmung kein Zugang zu den von den Autonutzerinnen und -nutzern generierten Daten und dem IT-System der Fahrzeuge möglich ist.[161] Aus einer wettbewerbsökonomischen Sicht folgt hieraus, dass sie damit die vollständige Kontrolle über alle diejenigen Märkte für komplementäre Produkte und Dienstleistungen erhalten können, für die entweder der Zugang zu diesen Daten oder der Zugang zu dem IT-System des Fahrzeugs notwendig ist.[162] Damit können die Autohersteller problemlos ihre Marktmacht auf diese Märkte übertragen, den Wettbewerb verzerren beziehungsweise Wettbewerber vollständig ausschließen. Insbesondere folgen hieraus auch mögliche gravierende negative Auswirkungen auf die Innovationsaktivitäten im Bereich der Sekundärmärkte, da sie Innovationen unabhängiger Serviceanbieter blockieren können sowie eine erhebliche Einschränkung der Autonutzerinnen und -nutzer, bezüglich der freien Wahl von Serviceanbietern auf diesen komplementären Märkten. Denn sie können nur solche Serviceanbieter wählen, die vorher mit den Autoherstellern Verträge abgeschlossen haben. Dies bezieht sich nicht nur auf die traditionellen Aftermarkt-Serviceanbieter wie Reparatur- und Wartungsbetriebe, sondern auch auf die vielfältigen neuen Dienstleistungen, die auf solchen Sekundärmärkten im Ökosystem vernetzten Fahrens angeboten werden können.[163] Besonders bedeutsam ist jedoch, dass das „Extended Vehicle"-Konzept es den Autoherstellern auch ermöglicht, sich die von den Autonutzerinnen und -nutzern durch den Betrieb des Fahrzeugs generierten Daten de facto „anzueignen",[164] um sie in vielfältiger Weise monetarisieren zu können.[165] Autohersteller können damit zu monopolistischen Anbietern der in den von ihnen verkauften Fahrzeugen generierten Mobilitätsdaten werden. Es ist aus ökonomischer Sicht sehr zweifelhaft, ob dies zu einer effizienten und innovationsfördernden Nutzung dieser Mobilitätsdaten führt.[166]

5.3.3 Problemlösungsoptionen

5.3.3.1 Übersicht

Die EU-Kommission hat bereits 2016 die Stakeholder bezüglich des vernetzten und automatisierten Fahrens im Rahmen ihrer „Cooperative Intelligent Transport System"-Initiative zusammengebracht, um die damit verbundenen Probleme zu lösen. In diesem Kontext sind verschiedene Modelle entwickelt worden, wie das Problem des „access to in-vehicle data and resources" gelöst werden könnte. Neben dem „Extended Vehicle"-Konzept der Autohersteller haben sich insbesondere zwei weitere Modelle als Alternativen herausgebildet, die von den anderen Stakeholdern in diesem C-ITS Prozess unterstützt wurden. Hierbei handelt es sich um (1) das Shared-Server-Konzept und (2) die „On-Board Application Platform".[167]

Bei dem Shared-Server-Konzept besteht zunächst die gleiche technische Lösung, das heißt dass die im Fahrzeug generierten Daten auf einen externen Server außerhalb des Fahrzeugs übertragen werden, über den der Datenzugang stattfinden kann. Allerdings ist dieser Server nicht unter der Kontrolle der Autohersteller, sondern einer neutralen Instanz, die diese Daten verwaltet und nach bestimmten Prinzipien diese Daten anderen zugänglich machen kann.[168] Dies kann als eine Datentreuhänderlösung verstanden werden, die wir im Folgenden noch genauer entwickeln werden.

Die „On-Board Application Platform" ist zunächst primär eine andere technologische Lösung, die nicht die Übertragung der Daten auf einen externen Server erfordert, sondern die Speicherung und Verarbeitung der Daten im Auto ermöglicht. Dies erfordert offene und interoperable Telematiksysteme, für deren Entwicklung allerdings ein längerer Zeitraum erforderlich ist. Bei dieser Lösung sind für das gesamte automobile Mobilitätssystem herstellerübergreifende Standardisierungen der Schnittstellen zum Austausch von Daten und der Interoperabilität mit komplementären Dienstleistungen erforderlich, ebenso wie einheitliche Sicherheitsstandards, um die notwendige sehr hohe Sicherheit von Fahrzeugen (inklusive Cybersicherheit) zuverlässig zu gewährleisten. Durch die Offenheit und Interoperabilität einer solchen standardisierten technischen Lösung für das gesamte Mobilitätssystem ist es technisch möglich, dass die Autonutzerinnen und -nutzer selbst die Kontrolle

über die im Fahrzeug generierten Daten ausüben und frei entscheiden können, welchen Serviceanbietern sie Zugang zu ihrem Fahrzeug geben. Sie können dann zwischen allen Serviceanbietern wählen, die die Sicherheitsstandards erfüllen, was durch eine zwingende Zertifizierung sichergestellt werden kann. Neben der Eliminierung der technisch bedingten Gatekeeper-Position der Autohersteller ist die Entwicklung von solchen standardisierten „On-Board Application"-Plattformen längerfristig sowieso erforderlich für den zukünftigen Übergang zu einem integrierten Mobilitätssystem mit automatisiertem (und autonomen) Fahren.[169]

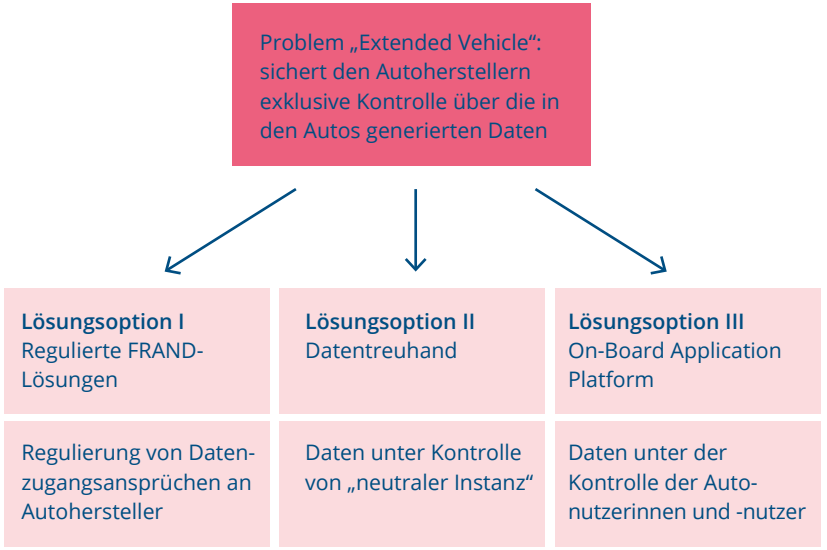
In der bisherigen Diskussion gibt es einen breiten Konsens (mit Ausnahme der Automobilhersteller), dass das „Extended Vehicle"-Konzept gravierende Probleme aufweist bezüglich Wettbewerb auf Sekundärmärkten und weiteren daraus folgenden negativen Auswirkungen für Innovation und die Wahlfreiheit von Konsumentinnen und Konsumenten. Dies war auch das Ergebnis der von der EU-Kommission in Auftrag gegebenen TRL-Studie (2017), die einen umfassenden Vergleich zwischen diesen drei Lösungen vorgenommen hat: Langfristig ist die „On-Board Application Platform" und kurz- und mittelfristig die Shared-Server-Lösung dem „Extended Vehicle"-Konzept der Autohersteller vorzuziehen.[170] In diesem Zusammenhang ist geklärt worden, dass es auch mit diesen Lösungen, insbesondere auch der „On-Board Application Platform", möglich ist, mindestens genauso hohe Sicherheitsstandards zu erfüllen wie durch das „Extended Vehicle"-Konzept.[171] Insofern ist das bisherige Hauptargument der Autohersteller, dass nur durch das „Extended Vehicle"-Konzept eine ausreichend hohe Sicherheit erreichbar ist und dieses deshalb trotz der Wettbewerbsprobleme den anderen Lösungen vorzuziehen sei, nicht richtig.[172]

Die Notwendigkeit einer Lösung der durch das „Extended Vehicle"-Konzept entstehenden Probleme hat die EU-Kommission seit Jahren anerkannt und bereits mehrfach Lösungen angekündigt. In ihrer europäischen Datenstrategie im Februar 2020 betont die Kommission die Bedeutung des Teilens der großen Mengen von In-Vehicle-Data für innovative mobilitätsbezogene Dienstleistungen und kündigt eine Reform der Kfz-Typenzulassungsverordnung als sektorspezifische Regulierungslösung an, bei der auch „the rights and interests of the car-owners generating

the data are respected and compliance with data protection rules is ensured"[173]. Angesichts des geplanten Data Acts könnten Lösungen auch in einem solchen legislatorischen Rahmen angedacht werden.[174]

In Bezug auf die Art der Lösung scheint zurzeit primär eine regulatorische FRAND-Lösung („fair, reasonable and non-discriminatory") bezüglich des Zugangs zu den „In-Vehicle Data and Resources" oder die Einführung der „On-Board Application Platform" diskutiert zu werden. In dieser Studie stellen wir zusätzlich (basierend auf der Shared-Server-Idee) die weitere Option einer Datentreuhandlösung vor und diskutieren diese. Da die Anforderungen an eine geeignete Lösung am einfachsten mit der Regulierungslösung mit FRAND-Zugang erklärt werden kann, werden wir zunächst diese vorstellen, bevor wir anschließend zur Datentreuhandlösung und „On-Board Application"-Lösung übergehen.[175]

Abbildung 3: Lösungsoptionen für Zugang zu Daten im vernetzten Auto



5.3.3.2 Lösungsoption I: Reguliertes Zugangsregime mit FRAND-Lösungen

Angesichts eines in der EU bereits existierenden (FRAND-ähnlichen) sektorspezifischen regulatorischen Zugangsregimes für Informationen und Daten in der Kfz-Typenzulassungsverordnung, das den Wettbewerb im Bereich Reparatur- und Wartungsdienstleistungen sichern soll, ist es naheliegend, ein solches Regulierungsregime auch in Bezug auf das Problem des Zugangs zu „In-Vehicle Data and Resources" für das neue viel umfassendere Ökosystem vernetzten und automatisierten Fahrens zu entwickeln. Dies könnte als eine sehr weitgehende Reform innerhalb der Kfz-Typenzulassungsverordnung implementiert werden, wobei eine umfassende Anpassung an die neuen technischen und ökonomischen Bedingungen des vernetzten Autos notwendig wäre.[176] Im einfachsten Fall würden die Autohersteller weiterhin das „Extended Vehicle"-Konzept anwenden mit der Übertragung der Daten auf externe Server, die unter ihrer Kontrolle stehen. Das regulatorische Zugangsregime aber würde ihnen umfassende Verpflichtungen auferlegen, anderen Stakeholdern zu FRAND-Bedingungen Zugang zu den im Fahrzeug generierten Daten zu gewähren. Dies würde sich nicht nur auf die klassischen Reparatur- und Wartungsdienstleistungsanbieter beziehen, sondern auch auf viele andere Anbieter von Dienstleistungen im Bereich des Ökosystems vernetzten Fahrens, um unverzerrten Wettbewerb und freie Innovationsaktivitäten auf den Sekundärmärkten zu ermöglichen und zu sichern.

Zunächst ist dabei wichtig, dass die Autohersteller keine Möglichkeiten haben dürfen, sich selbst (oder ihre Vertragswerkstätten et cetera) im Vergleich zu anderen Unternehmen zu bevorzugen.[177] Eine entsprechend ausgestaltete FRAND-Lösung könnte dies im Prinzip sichern helfen. Von entscheidender Bedeutung ist aber, insbesondere im Hinblick auf Innovation, dass diskriminierungsfreie Datenzugangsansprüche sich nicht nur auf bereits existierende Dienstleistungen beziehen dürfen oder solche die die Autohersteller selbst anbieten, sondern dass die Serviceanbieter auch Zugang zu anderen Daten erhalten können, um neue Dienstleistungen innovativ entwickeln und anbieten zu können. Insofern dürfen nicht die Autohersteller (nach ihren eigenen Gewinninteressen) über das Set von Daten entscheiden, das durch FRAND-Lösungen zugänglich gemacht wird. Dies muss vielmehr eine regulatorische Entscheidung sein, die nach objektiven (an Wettbewerb und Innovation) orientierten Kriterien durch eine Regulierungsbehörde zu treffen ist.[178] Andernfalls wären keine freien Innovationsaktivitäten der unabhängigen Serviceanbieter in diesem Ökosystem möglich, zumindest insoweit für diese ein Zugang zu solchen Daten notwendig ist.

Weiterhin ist nach der obigen Analyse des Gatekeeper-Problems klar, dass die Regulierung nicht nur das Datenzugangsproblem, sondern auch das Interoperabilitätsproblem lösen muss, das heißt unabhängige Serviceanbieter müssen auch die Möglichkeit haben, unter FRAND-Bedingungen einen diskriminierungsfreien technischen Zugang zum Fahrzeug zu bekommen, um den Autonutzerinnen und -nutzern auch Remote Services anbieten zu können. Gleiches gilt für den Zugang zum Dashboard des Fahrzeugs, um gleiche Bedingungen für die Kommunikation mit den Kundinnen und Kunden zu sichern. Insofern sind auch bei dieser Lösung standardisierte interoperable technische Schnittstellen (für Datenaustausch und Interoperabilität) sowie ein standardisiertes Sicherheitskonzept (mit Zertifizierungslösungen für Serviceanbieter) erforderlich. Auch bezüglich der Interoperabilität muss nach objektiven Kriterien durch den Regulator darüber entschieden werden, welcher Zugang unter welchen Bedingungen gewährt werden sollte.[179] Auch diese Entscheidungen sollten nicht vom Gewinninteresse der Autohersteller bestimmt sein, sondern vom Ziel der Sicherung von Wettbewerb und Innovation und den Interessen der Konsumentinnen und Konsumenten. Dies schließt auch eine klare Gebührenregelung für den Zugang zu Daten und dem technischen Zugang zum Fahrzeug ein.

Da es bisher bereits in der Kfz-Typenzulassungsverordnung Regulierungen bezüglich des fairen und diskriminierungsfreien Zugangs zu Informationen und Daten, standardisierten technischen Schnittstellen, Sicherheitsstandards (inklusive sicherheitsbezogene Zertifizierungen) sowie eine Gebührenregelung gibt, sind die wichtigsten regulatorischen Bausteine bereits vorhanden. Allerdings ist es immer noch ein sehr großer Schritt, dieses Regulierungsregime an die neuen technologischen und ökonomischen Bedingungen des Ökosystems vernetzten Fahrens anzupassen, weil es nicht nur um eng begrenzte Reparatur- und Wartungsdienstleistungen geht, sondern um vielfältige und oft noch unbekannte

Services und Nutzungsmöglichkeiten dieser Daten. Deshalb spielt auch die bereits diskutierte Offenheit für Innovationen hier eine völlig andere und viel wichtigere Rolle als in den traditionellen Aftermärkten.[180] Das Hauptproblem der FRAND-Regulierungslösung ist, dass die Gefahr besteht, dass zu eng definiert wird, bezüglich welcher Daten ein FRAND-Zugang gewährt werden soll, oder dass gar der Autohersteller selbst entscheiden kann, zu welchen Daten er einen Zugang nach FRAND-Bedingungen gewährt. Gleiches gilt für die Interoperabilität. Die Autohersteller haben unter den Bedingungen des „Extended Vehicle"-Konzepts immer ein starkes Interesse, die Einschränkungen ihrer exklusiven Kontrolle über die Daten und die Interoperabilität möglichst gering zu halten. Insofern bedarf es auch einer starken regulatorischen Lösung, um die aus dieser Gatekeeper-Position folgenden negativen Wirkungen auf Wettbewerb, Innovation und die Auswahlfreiheit von Konsumentinnen und Konsumenten soweit wie möglich zu reduzieren.[181] Deshalb sind in dieser wettbewerbspolitischen Auseinandersetzung bereits früh die viel grundlegenderen Alternativlösungen „Shared Server" und „On-Board Application"-Platform in die Diskussion gebracht worden, da diese die Chance bieten, eine solche Gatekeeper-Position der Autohersteller erst gar nicht entstehen zu lassen. Dies führt uns direkt zur folgenden Diskussion einer Datentreuhandlösung.

5.3.3.3 Lösungsoption II: Datentreuhand

Bei der (auf der ursprünglichen Shared-Server-Idee) aufbauenden Datentreuhandlösung besteht zunächst die gleiche technische Lösung wie beim „Extended Vehicle"-Konzept, nämlich dass die im Fahrzeug generierten Daten auf einen externen Server außerhalb des Fahrzeugs übertragen werden, über den ein Datenzugang stattfinden kann. Allerdings steht dieser Server nicht unter der Kontrolle der Autohersteller, sondern einer neutralen Instanz, die diese Daten verwaltet und nach bestimmten Prinzipien zugänglich machen kann.[182]

Datentreuhand als obligatorischer Data Host

Die Grundidee besteht darin, dass im Prinzip alle im Auto generierten Daten in eine solche Datentreuhand eingebracht werden, das heißt dass der Backend-Server unter der Governance der Datentreuhand steht und nicht mehr unter der Kontrolle der Autohersteller.[183] Auch diese Datentreuhandlösung kann nur im Rahmen einer Regulierung verwirklicht werden, die den Autoherstellern die Implementierung einer solchen technischen Lösung auferlegt.[184] Es ist Aufgabe des Gesetzgebers (oder einer damit beauftragten Regulierungsbehörde), ausgehend von den damit zu verfolgenden Zielen über die Prinzipien und die Bedingungen zu entscheiden, nach denen diese Daten anderen Unternehmen und Institutionen zugänglich gemacht werden sollen. Institutionell kann es sich bei dieser Datentreuhand um eine staatliche Instanz handeln oder auch eine privatrechtlich organisierte Institution, die mit dieser datentreuhänderischen Aufgabe betraut wird. Diese Institution sollte nicht gewinnorientiert sein und sich aus kostendeckenden Gebühren finanzieren.

Entscheidend für die von der Datentreuhand zu fällenden Entscheidungen sind die vom Gesetzgeber festzulegenden Ziele und Prinzipien. Wichtige Ziele neben der Sicherung des Wettbewerbs könnten die Förderung von Innovation, der Schutz von Verbraucherinnen und Verbrauchern, insbesondere auch bezüglich des Datenschutzes, die Sicherheit und Umweltverträglichkeit im Mobilitätssektor sowie die wissenschaftliche Forschung sein. Der große Vorteil einer Datentreuhandlösung ist, dass damit auch Gemeinwohlziele, die im Mobilitätssektor eine wichtige Rolle spielen, wie Verkehrssicherheit und Verkehrsregelung et cetera von vornherein mitintegriert werden können, sodass zusätzliche spezielle gesetzliche Regelungen für den Zugang zu dafür notwendigen Daten nicht mehr notwendig wären.[185] Gleichzeitig würde eine solche Datentreuhand auch die Möglichkeiten erleichtern, diese im Auto generierten Daten mit Mobilitätsdaten aus anderen Bereichen zu verknüpfen, was neue Perspektiven für den angestrebten europäischen Mobilitätsdatenraum eröffnet, beispielsweise auch dem GAIA-X-Projekt.[186] Dies soll an dieser Stelle nicht weiter diskutiert werden. Wichtig ist aber, dass eine solche Datentreuhandlösung wesentlich mehr Aufgaben erfüllen und Probleme lösen könnte als nur die Wettbewerbs- und Innovationsprobleme in Bezug auf Sekundärmärkte im Ökosystem des vernetzten Fahrens.

Zur Ausgestaltung der Regelungen des Datenzugangs

Anhand dieser Ziele kann sich der Gesetzgeber orientieren, wenn er die Governance der Datentreuhand festlegt, das heißt die Vorgaben für die Entscheidungen, wem die Datentreuhand zu welchen Bedingungen

Daten zur Verfügung stellt. Es ist naheliegend, dass die Datentreuhand diese Daten primär nach FRAND-Bedingungen zugänglich macht. Allerdings werden aufgrund der Unterschiedlichkeit der zur Verfügung stehenden Daten starke Differenzierungen notwendig sein, welche Unternehmen Zugang zu welchen Daten bekommen sollen. Hierbei wird zwischen verschiedenen Stakeholdern mit ihren unterschiedlichen Verwendungszwecken zu differenzieren sein. Die dabei zur Verfügung zu stellenden Daten sollten aber nicht zu eng definiert werden, um auch breite Innovationsaktivitäten bezüglich neuer Dienstleistungen zu unterstützen. Bezüglich technischer Fahrzeugdaten werden die Autohersteller (und auch ihre Zulieferer) zweifellos eine Sonderstellung einnehmen, insbesondere bezüglich der Daten, die unmittelbar für den Betrieb des Fahrzeugs notwendig sind, aber auch Daten, die (ausnahmsweise zum Beispiel über Datenbankwerke) dem Schutz von Immaterialgüterrechten oder dem Geschäftsgeheimnisschutz zugänglich sind. Jenseits des Datenzugangs für private Firmen, die neue Produkte und Services auf komplementären Sekundärmärkten anbieten wollen, sollten anonymisierte Mobilitätsdaten auch als Input für die Entstehung von freien Datenmarktplätzen für die weitere Analyse und Verwertung solcher Daten zur Verfügung stehen. Weiterhin sind ausgehend von den Gemeinwohlzielen auch Daten über Straßenzustand, Verkehrsverhältnisse, umweltschutzrelevante Daten, Daten für die Unfallforschung oder zur Aufklärung von Haftungsfragen bei Unfällen beziehungsweise für die hoheitliche Aufgabe der periodischen technischen Überwachung der Fahrzeugsicherheit über die Datentreuhand den entsprechenden öffentlichen Institutionen zugänglich zu machen. Solche Datenzugänge sollten – wo möglich und sinnvoll – auch in Realzeit möglich sein. Besonders wichtig wäre ein breiter Zugang zu diesen Daten für Forschungszwecke. Die jeweiligen Datenzugangsregelungen sind genau zu definieren.[187]

Aus diesen Überlegungen wird deutlich, dass je nach den Zielen ein erheblicher Spielraum für die konkrete Ausgestaltung einer solchen Datentreuhandlösung für die im vernetzten Auto generierten Mobilitätsdaten besteht. Datenzugang und Datentreuhand sind insofern zwingend zusammen zu denken. Insofern ist es mit der Einrichtung einer Datentreuhand nicht getan, vielmehr bedarf es umfassender gesetzgeberischer Entscheidungen darüber, welche Daten wem für

welche Zweck und unter welchen Bedingungen zur Verfügung gestellt werden sollen.

Gewährleistung von Verbraucher- und Datenschutz

Wie ist das Verhältnis zwischen einer solchen Datentreuhand und den Verbraucherinnen und Verbrauchern, die als Autonutzerinnen und -nutzer beim Fahren diese Daten generieren? Interessanterweise spielen in der wirtschaftspolitischen Auseinandersetzung über den „Zugang zu In-Vehicle Data and Resources“ die Verbraucherinnen und Verbraucher bisher nur eine sehr untergeordnete Rolle. Dies ist teilweise dem vorherrschenden wettbewerbspolitischen Blickwinkel geschuldet, bei dem davon ausgegangen wird, dass, wenn der Wettbewerb auf den Sekundärmärkten gesichert ist, die Verbraucherinnen und Verbraucher in Form von geringeren Preisen, mehr Innovation und Auswahlfreiheit profitieren.[188] Tatsächlich stellen sich aber durch den Übergang zum vernetzten Fahrzeug auch hier neue grundsätzliche Fragen, die bei der bisherigen Informations- und Datenzugangsregulierung der Kfz-Typenzulassungsverordnung keine Rolle spielten. Zentral ist in jedem Fall die Einhaltung der datenschutzrechtlichen Vorgaben der DSGVO. Im Falle des zurzeit angewendeten „Extended Vehicle“-Konzepts müssen die Autohersteller für die Verarbeitung der personenbezogenen Daten die datenschutzrechtliche Einwilligung der Autonutzerinnen und -nutzer einholen. Da aber ohne eine solche Einwilligung das vernetzte Fahrzeug (oder bestimmte Funktionen) nicht genutzt werden können, stellt sich die Frage, inwieweit die Autonutzerinnen und -nutzer die Möglichkeit haben, auch granulare Entscheidungen darüber zu treffen, wann und welche Daten sie den Autoherstellern für welche Zwecke zur weiteren Verarbeitung und Nutzung überlassen oder ob ihnen nur die Möglichkeit einer pauschalen Einwilligung angeboten wird. Datenschutzrechtlich stellt sich dabei die Frage, ob eine Einwilligung in die Datenerhebung ohne eine solche granulare Einwilligungsmöglichkeit (jedenfalls für nicht für den Betrieb erforderliche Daten) überhaupt wirksam ist.[189] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat das an anderer Stelle für nicht granulare Einwilligungen gerade verneint.[190] Bei der hier diskutierten Datentreuhandlösung wäre es möglich, dass die Datentreuhand einen höheren Standard für den Datenschutz für Autonutzerinnen und -nutzer

setzt als sie nach den bisherigen (und konkret oft unklaren) Vorgaben der DSGVO bestehen. Dies bedeutet, dass sie über den Minimumstandard der DSGVO hinausgehen können (einschließlich einer besseren Umsetzung von „Privacy by Design"- und „Privacy by Default"-Prinzipien). Damit könnte eine solche Datentreuhandlösung auch den Daten- und Verbraucherschutz bei der Nutzung von vernetzten Fahrzeugen stärken.

Interoperabilitätsvorgaben
Zunächst können durch eine solche Datentreuhand aber nur die Wettbewerbs- und Innovationsprobleme gelöst werden, die durch die beim „Extended Vehicle"-Konzept bestehende exklusive Kontrolle der Daten durch die Autohersteller entstehen. Das Problem der exklusiven Kontrolle der Autohersteller in Bezug auf den technischen Zugang zum Fahrzeug (sowie das Dashboard im Fahrzeug) wird hierdurch nicht gelöst. Dies bedeutet, dass es auch bei der Datentreuhandlösung nötig ist, das Problem der Interoperabilität für die Erbringung von komplementären Serviceleistungen im Fahrzeug durch einen regulatorischen Ansatz zu lösen. Insofern sind auch bei dieser Lösung standardisierte interoperable technische Schnittstellen (für Datenaustausch und Interoperabilität) sowie ein standardisiertes Sicherheitskonzept (mit Zertifizierungslösungen für Serviceanbieter) erforderlich. Es handelt sich dabei im Prinzip um die gleichen Aufgaben, die auch in einer Regulierungslösung bezüglich eines FRAND-Datenzugangs notwendig sind (vgl. die obige Lösungsoption I). Das muss hier nicht nochmals tiefer ausgeführt werden. Es bedeutet allerdings, dass einer solchen Datentreuhand eine wesentlich größere regulatorische Aufgabe zukommt als „nur" Entscheidungen über den Zugang zu diesen Daten zu treffen. Sie muss sich auch direkt mit Interoperabiliäts- und Standardisierungsfragen beschäftigen sowie mit Sicherheitskonzepten (einschließlich Sicherheitszertifizierungen), wie dies auch eine Regulierungsbehörde bei Lösungsoption I zu tun hätte.[191] Dies ist deshalb nicht überraschend, weil in vielen Kontexten wirksame Datenzugangslösungen auch regulatorische Entscheidungen in Bezug auf Interoperabilität, Sicherheit (und oft auch Datenschutz) erfordern.[192]

Ausgestaltungsoptionen
Es ist nicht möglich, an dieser Stelle auf die konkreten Ausgestaltungsoptionen einer Datentreuhand im Einzelnen näher einzugehen. Es ist zweifellos von zentraler Bedeutung, dass die weitere Konkretisierung der Datenzugangsregelungen nur mithilfe von Expertinnen und Experten der Stakeholder in diesem Ökosystem des vernetzten und automatisierten Fahrens (Autohersteller, unabhängige Serviceanbieter et cetera) und der öffentlichen Institutionen möglich ist, die bestimmte Daten zur Erfüllung ihrer Aufgabe im öffentlichen Interesse benötigen, sowie von Wirtschafts- und Verbraucherverbänden. Insofern ist auch eine enge Zusammenarbeit zwischen der Datentreuhand und diesen Stakeholdern von zentraler Bedeutung, insbesondere in Bezug auf die Autohersteller. Hierbei ergeben sich viele spezifische Fragen der institutionellen Ausgestaltung, die hier nicht erörtert werden sollen.

5.3.3.4 Lösungsoption III: „On-Board Application"-Plattform

Bisher sind wir von der technischen Lösung ausgegangen, wie sie zurzeit im Konzept des „Extended Vehicle" praktiziert wird, nämlich dass die Daten direkt auf einen externen Server übertragen werden. Dies verschafft entweder dem Autohersteller oder der Datentreuhand eine exklusive Kontrolle über die Daten, sodass diese nur mit deren Einwilligung anderen zugänglich gemacht werden können. Mit der technischen Lösung von offenen und interoperablen „On-Board Application"-Plattformen, auf denen die Daten direkt gespeichert und verarbeitet werden könnten und Software für spezifische Anwendungen installiert werden könnte, wären technisch aber auch ganz andere und viel weitergehende Lösungen möglich, weil jetzt die Kontrolle über diese Daten und auch den Zugang zum Fahrzeug von den Autonutzerinnen und -nutzern (beziehungsweise Kfz-Halterinnen und -Haltern) selbst ausgeübt werden könnte. Damit wäre der technische Bottleneck, der den Autoherstellern die exklusive Kontrolle über die Daten beziehungsweise den Zugang zum Fahrzeug verschafft, beseitigt. Das würde die vollständige Eliminierung der Gatekeeper-Position der Autohersteller ermöglichen. Diese offenen interoperablen Telematikplattformen benötigen umfangreiche industrieweite technische Standardisierungen und Regulierungen bezüglich der Sicherheit (einschließlich eines Zertifizierungssystems).

Damit handelt es sich bei dem vernetzten Fahrzeug nicht mehr um ein geschlossenes, sondern ein – aus Sicht der Autonutzerinnen und -nutzer – offenes System. Dies würde im Prinzip einen freien unverzerrten Wettbewerb und freie Innovationsaktivitäten auf den Sekundärmärkten des Ökosystems vernetzten Fahrens ermöglichen, weil die Autonutzerinnen und -nutzer Serviceanbietern direkt die notwendigen Daten zukommen lassen und den technischen Zugang erlauben können. Dies bedeutet aber nicht, dass damit bereits alle Probleme gelöst, der Wettbewerb geschützt und eine ökonomisch und an den Zielen der Gesellschaft orientierte Nutzung der in den vernetzten Autos generierten Mobilitätsdaten gesichert ist. Erstens, müssen eventuell andere neu entstehende Wettbewerbsprobleme verhindert werden. Beispielsweise könnten die Automobilhersteller die vorher technisch herbeigeführte Exklusivität der Kontrolle über die Daten und den technischen Zugang zum Fahrzeug durch eine entsprechende vertragliche Bindung wiederherstellen.[193] Des Weiteren könnten große digitale Plattformen, wie Google und Apple, in diesen neuen Markt mit den Kfz-Halterinnen und -haltern einsteigen, was den Autonutzerinnen und -nutzern auf der einen Seite viele Vorteile verschaffen könnte, auf der anderen Seite aber auch ganz neue Marktmachtprobleme zur Folge haben könnte.

Wichtig für unsere Fragestellung ist aber, ob zweitens, auch unter einem solchen Regime offener interoperabler Plattformen Datentreuhändern eine wichtige Rolle zukommen könnte. Aufgrund der wesentlich größeren Möglichkeiten, wie sich die Märkte unter diesem (offeneren) Regime entwickeln könnten, ist diese Frage nicht leicht zu beantworten. Wenn die Autonutzerinnen und -nutzer selbst über die Verwendung der Daten im vernetzten Fahrzeug entscheiden und hierüber die exklusive Kontrolle haben, kann es sehr schwierig werden für öffentliche Institutionen oder die Wissenschaft, für Zwecke des Gemeinwohls Zugang zu bestimmten in den Fahrzeugen generierten Daten zu bekommen, beispielsweise Verkehrsdaten, Daten über Straßenzustand, Umweltdaten oder Daten für Verkehrssicherheitszwecke und Unfallforschung oder für die wissenschaftliche Forschung. Für diese Zwecke ist es oftmals notwendig, sehr viele und aktuelle (Realzeit-)Daten zu haben, um sie entsprechend auswerten zu können. Insofern kann es notwendig sein, dass die Kfz-Halterinnen und -Halter gesetzlichen Verpflichtungen unterliegen sollten,

solche Daten den entsprechenden öffentlichen Institutionen zugänglich zu machen. Eine vom Gesetzgeber beauftragte Datentreuhand, die ähnlich organisiert sein könnte wie bei Lösungsoption II, könnte die Aufgabe haben, solche Daten direkt von den vernetzten Autos zu sammeln und dann – in geeigneter Form und unter Beachtung des Datenschutzes – diesen öffentlichen Institutionen oder für wissenschaftliche Forschungszwecke nach den gesetzlichen Vorgaben zugänglich zu machen. Ob eine solche Datentreuhand auch große anonymisierte Datensets für Innovationszwecke beziehungsweise für das Trainieren von Algorithmen sammeln und zur Verfügung stellen sollte, beispielsweise auch als Teil eines europäischen Mobilitätsdatenraumes, wäre eine weitere diskutierbare Option. Dies hängt jedoch sicher auch von der Entwicklung privater Märkte für Mobilitätsdaten ab, die durch die Kontrolle der Kfz-Halter über die Daten entstehen könnten.

Zusammenfassend kann festgehalten werden, dass auch bei der Umsetzung der „On-Board Application"-Plattformlösung eine Datentreuhand eine wichtige Rolle spielen könnte, die jedoch vermutlich weniger Aufgaben hätte als bei Lösungsoption II.

5.3.4 Diskussion und Folgerungen

Die diskutierten Lösungsoptionen in Bezug auf die durch das „Extended Vehicle"-Konzept der Autohersteller entstehenden Probleme können zusammenfassend folgendermaßen einander gegenübergestellt werden:

Regulierte FRAND-Zugangslösung

Kurzfristig am leichtesten implementierbar scheint eine Lösung, bei der die Autohersteller weiterhin technisch das „Extended Vehicle"-Konzept anwenden und die Daten auf einen externen Server übertragen, aber dies mit einer umfassenden Regulierung in Bezug auf den Zugang zu diesen Mobilitätsdaten sowie den technischen Zugang zum Fahrzeug (Remote Access) kombiniert wird. Dies würde auch die Implementierung von technologischen Schnittstellen und Sicherheitsstandards erfordern, um Wettbewerb, Innovation und Wahlfreiheiten für Konsumentinnen und Konsumenten auf den komplementären Sekundärmärkten zu sichern. Die Grundidee besteht darin, die im Prinzip weiter bestehende Gatekeeper-Position der Autohersteller durch dieses Zugangsregime

soweit wie möglich regulatorisch zu beschränken. Dies könnte auch durch eine umfassende Reform des jetzigen Zugangsregimes der Kfz-Typenzulassungs-Verordnung erfolgen.

Datentreuhandlösung

Hier würden die Daten des vernetzten Fahrzeugs direkt unter der Kontrolle einer Datentreuhand stehen, die diese Daten nach gesetzlich bestimmten Zielen und Prinzipien anderen Unternehmen und öffentlichen Institutionen zugänglich machte (einschließlich der Autohersteller), sowohl zur Sicherung des Wettbewerbs als auch für Gemeinwohlzwecke. Aufgrund des zusätzlich bestehenden Interoperabilitätsproblems ist auch hier eine FRAND-Regulierung des technischen Zugangs zum Fahrzeug erforderlich. Dies impliziert, dass der Datentreuhand über die reine Gewährung von Zugang zu Daten hinaus auch eine regulatorische Aufgabe in Bezug auf Interoperabilität und Sicherheitsstandards zukommen würde, die derjenigen ähnelt, die auch bei einer regulierten FRAND-Lösung notwendig wäre. Allerdings eröffnet eine Datentreuhandlösung von vornherein mehr Möglichkeiten einer Öffnung dieser Datenbestände für breite innovative Nutzungen und eine systematischere Einbeziehung von Gemeinwohl- und Verbraucherinteressen.

„On-Board Application"-Plattform

Bei dieser Lösung würde im Gesamtsystem des vernetzten und zunehmend automatisierten Fahrens ein einheitlicher Standard für offene interoperable Telematiksysteme sowie ein einheitliches Sicherheitssystem etabliert. Dies würde technisch erlauben, dass die Autonutzerinnen und -nutzer selbst über die Verwendung der in ihren Fahrzeugen generierten Daten und den technischen Zugang zum Fahrzeug entscheiden können. Hiermit könnte die Gatekeeper-Position der Autohersteller, die ursächlich für die Wettbewerbs- und Innovationsprobleme auf den Sekundärmärkten ist, direkt beseitigt werden. Dies bedeutet allerdings nicht, dass nicht neue Wettbewerbsprobleme auftreten können, die zu lösen wären. Eine Datentreuhand könnte auch hier eine wichtige Rolle spielen, insbesondere für die Sammlung und Nutzung von Mobilitätsdaten aus dem vernetzten Auto, die für Gemeinwohlzwecke im Mobilitätssektor notwendig wären.

Es war nicht die Aufgabe dieser Studie, eine umfassende Analyse des Problems der Governance der in vernetzten Fahrzeugen generierten Daten vorzunehmen und daraus Politikempfehlungen abzuleiten. Es ging primär um die Frage einer möglichen Rolle von Datentreuhandlösungen. Dies kann aber nicht losgelöst von den Problemen und alternativen Lösungsvorschlägen beantwortet werden. Insofern folgt eine kurze zusammenfassende Analyse.

Die Wettbewerbsprobleme, die aus dem „Extended Vehicle"-Konzept folgen, sind bekannt und brauchen an dieser Stelle nicht wiederholt zu werden. Dagegen erscheint es wichtig, das Problem nochmals aus einer allgemeineren datenökonomischen und datenpolitischen Perspektive zu betrachten. Daten sind nichtrivale Güter, die gleichzeitig von vielen genutzt werden können. Die Mitteilung der EU-Kommission *Building a European Data Economy* (2017) mit ihrer Diagnose, dass Daten nicht genügend genutzt und wiederverwendet werden und sich dies negativ auf Innovationen und die Datenökonomie auswirkt, war ein großer Fortschritt in der datenpolitischen Diskussion, auf dem die aktuelle europäische Datenstrategie immer noch basiert.[194]

Das Ökosystem des vernetzten und automatisierten Fahrens im Mobilitätssektor ist ein komplexes System, in dem zukünftig viele Millionen Autonutzerinnen und -nutzer mit ihren Fahrzeugen eine riesige Menge von Mobilitätsdaten generieren, die wiederum in vielfältigster Weise von vielen Unternehmen und öffentlichen Institutionen genutzt werden können, teils für neue Dienstleistungen für die Autonutzerinnen und -nutzer selbst, teils für die Datenwirtschaft, aber teils auch für Verbesserungen der Verkehrssicherheit, Verkehrsregelung, Unfallforschung et cetera. Aus einer ökonomischen (und noch mehr aus einer gesellschaftlichen) Perspektive ist es sehr problematisch, wenn sich eine sehr kleine Anzahl von privaten Unternehmen faktisch die exklusive Kontrolle über all diese Daten verschaffen kann und dann ausschließlich nach ihrem eigenen unternehmerischen Gewinninteresse über die Verwendung und den Zugang zu diesen Daten verfügte.[195] Aus ökonomischer Sicht führt diese monopolistische Kontrolle über die Daten der von den Autoherstellern verkauften Fahrzeuge nicht nur zu den viel diskutierten Wettbewerbsproblemen, sondern gleichermaßen zu einer systematischen Unter-

nutzung dieser Daten für vielfältige Innovationsaktivitäten und für die Verbesserung von Politiken staatlicher Institutionen im öffentlichen Interesse.[196]

Die Probleme des Datenzugangs beziehen sich primär auf zwei Ursachen: (1) Unternehmen sammeln viele Daten, aber es gibt zu hohe Transaktionskosten am Markt, um sie auf freiwilliger Basis mit anderen Unternehmen besser zu teilen. Auf die Lösung dieses Problems zielt beispielsweise der Data Governance Act mit dem Ansatz, vertrauenswürdige Datenintermediäre zu schaffen. (2) Das zweite Problem sind Versuche von Unternehmen, sich durch ihre exklusive Kontrolle über bestimmte Arten von Daten beziehungsweise durch Strategien der Datenmonopolisierung dauerhafte Vorteile auf Kosten des Wettbewerbs zu verschaffen, mit den bereits diskutierten vielfältigen negativen Auswirkungen. Die Versuche der Autohersteller, das „Extended Vehicle"-Konzept als zentrales Konzept für die Governance der in den Fahrzeugen von den Autonutzerinnen und -nutzern generierten Daten dauerhaft (!) zu implementieren, ist als eine solche Datenmonopolisierungsstrategie zu verstehen. Dies wird durch die fehlende Interoperabilität aufgrund eines Designs der Fahrzeuge als geschlossene Systeme zusätzlich verstärkt und abgesichert.[197]

Aus dieser breiteren Perspektive folgt, dass das Problem des Zugangs zu „In-Vehicle Data and Resources" nicht nur ein Problem zwischen Autoherstellern und unabhängigen Serviceanbietern im Ökosystem des vernetzten und automatisierten Fahrens ist, wie dies die traditionelle Diskussion nahelegt. Es geht nicht nur um Wettbewerbsverzerrungen auf Sekundärmärkten und die Verdrängung von unabhängigen Serviceanbietern. Der Kreis der Stakeholder ist wesentlich breiter und umfasst auch die Autonutzerinnen und -nutzer, die allgemeine Datenwirtschaft und die öffentlichen Institutionen, die im Bereich des Mobilitätssektors im öffentlichen Interesse tätig sind. Dies ist auch der Blickwinkel des europäischen Datenmobilitätsraumes und seinen Zielen. Aus diesem Blickwinkel erscheint die Idee einer datentreuhänderischen Lösung, wie sie hier als Lösungsoption II nur skizzenhaft angedeutet werden konnte, als eine interessante und spannende Option, die es wert ist, systematisch mit allen ihren Vorteilen und Problemen durchdacht und konzeptionell entwickelt zu werden. Es ist klar, dass eine solche Option nicht kurzfristig umgesetzt werden könnte, aber es geht hier um die mittel- und langfristige Gestaltung der Governance der zukünftigen riesigen Datenmengen, die durch den Betrieb vernetzter Fahrzeuge durch die Autonutzerinnen und -nutzer generiert werden, und der Aufrechterhaltung eines freien Wettbewerbs und freier Innovationsaktivitäten innerhalb des zukünftigen Mobilitätssystems.

Folgerungen

Welche Folgerungen können hieraus abgeleitet werden?

1. Zur Sicherung von Wettbewerb und Innovation innerhalb dieses Ökosystems ist die Setzung klarer rechtlicher Rahmenbedingungen notwendig, die entweder die aus der Gatekeeper-Position entstehende Macht der Autohersteller stark beschränkt oder – wesentlich besser – die Entstehung einer solchen Gatekeeper-Position präventiv verhindert.

2. Nachdem das bisherige „Extended Vehicle"-Konzept nicht weiter akzeptiert werden kann, könnte eine vorläufige Lösung des Problems darin bestehen, möglichst schnell eine strikte und weitreichende Regulierung der Anwendung des „Extended Vehicle"-Konzepts unter FRAND-Bedingungen zu implementieren. Dies könnte vermutlich am einfachsten über eine weitere Reform der Kfz-Typenzulassungsverordnung erreicht werden. Aufgrund der speziellen technologischen und ökonomischen Bedingungen ist allerdings in jedem Fall eine sektorspezifische Regulierungslösung erforderlich.[198]

3. Parallel zu einer solchen Lösung sollten dringend Pläne entwickelt werden für die mittel- und langfristige Lösung des Problems einer adäquaten Governance der von vernetzten und automatisierten Fahrzeugen generierten Daten:

   - Dies betrifft zum einen die Governance der in den vernetzten Fahrzeugen von den Autonutzerinnen und -nutzern generierten Daten. Hier sollte die bisher in der Diskussion vernachlässigte Möglich-

keit einer datentreuhänderischen Lösung, wie in der Lösungsoption II angedacht, ernsthaft und umfassend geprüft werden, insbesondere auch in Konnex mit Lösungen für andere Mobilitätsdaten und der Strategie eines europäischen Mobilitätsraums.

› Zum anderen umfasst dies auch die Entwicklung von standardisierten offenen Telematikplattformen für das vernetzte und automatisierte Fahren. Diese könnten nicht nur dabei helfen, die in allen Lösungsoptionen auftretenden Interoperabilitätsprobleme zu lösen, sondern wären auch eine wichtige Voraussetzung für die Integration des vernetzten Fahrzeuges in ein (bereits in Entstehung befindliches) Mobilitätssystem für automatisiertes und letztlich auch autonomes Fahren.[199]

5.3.5 Tauglichkeit des DGA-E zur Problemlösung

Auch außerhalb des Bereichs der Daten des vernetzten Autos sollten Datentreuhandlösungen bei der Frage der Governance von spezifischen Arten von Mobilitätsdaten als eine mögliche Option angesehen werden, die unter bestimmten Bedingungen zweckmäßig sein können. Es wird dabei von der spezifischen Ausgestaltung solcher Treuhandlösungen abhängig sein, ob die Regelungen des geplanten Data Governance Acts relevant sind und, wenn ja, auch tatsächlich helfen könnten. Für die hier diskutierte Datentreuhandlösung für die Daten des vernetzten Autos (Lösungsoption II) kann der DGA keinen Beitrag leisten, aber würde einer solchen Lösung auch nicht im Wege stehen.

28 Specht/Kerber, *Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA*, ABIDA – Assessing Big Data, 2017, S. 119 f.

29 Hoffman/Lutz/Ranzini, *Privacy Cynicism: A New Approach to the Privacy*, online unter: https://cyberpsychology.eu/article/view/6280/5888 (6.3.2018) (zuletzt abgerufen am 18.11.2021); Smith/Dinev/Xu, 35 MIS Quart 2011, 989.

30 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, BVerfGE 65, 1, 43.

31 BVerfG, Beschl. v. 23.10.2006 – 1 BvR 2027/02, MMR 2007, S. 93.

32 Richter, PinG 2016, S. 185 f.; Specht-Riemenschneider/Bienemann, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), *Datenrecht in der Digitalisierung*, 2020, S. 329.

33 Rothmann, *Ungewollte Einwilligung? Die Rechtswirklichkeit der Informierten Zustimmung im Fall von Facebook*, 2.11.2017, S. 7, online unter: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/2017-11-02-Jahrestagung-2017/1.1c_Rothmann_Folien_Vortrag_Forum_Privatheit_Berlin_Uni_Wien_2017.pdf (zuletzt abgerufen am 18.11.2021); nachzulesen bei Rothmann/Buchner, DuD 2018, S. 342 u. 344; darauf Bezug nehmend: Jennessen, *Datenschuldrecht*, im Erscheinen.

34 So zu den Datenschutzbestimmungen von Facebook: LG Berlin, Urt. v. 16.01.2018 – 16 O 341/15, GRUR-RS 2018, 1060 Rn. 40.

35 Arnold, GfK 1990, S. 150 u. 152.

36 Buck-Heeb/Lang, in: BeckOGK BGB, § 675 Rn. 248 ff. (Stand: 1.9.2021); Köndgen, BKR 2011, S. 283 ff.; Eidenmüller, JZ 2005, S. 216 u. 218 ff.; Koch, BKR 2012, S. 485; Koller, in: *Festschrift für Huber*, 2006, S. 821 u. 824 ff.; Spindler, in: Festschrift für Säcker, 2011, S. 469 u. 474 ff.; Sedlmeier, *Rechtsgeschäftliche Selbstbestimmung im Verbrauchervertrag*, 2012, S. 134 ff.; Möllers/Kernchen, ZGR 2011, S. 1 ff.; Arendts, *Die Haftung für fehlerhafte Anlageberatung*, 1998, S. 23; vgl. dazu auch: Specht, Diktat der Technik, 2019, S. 167.

37 Martinek, in: Grundmann, *Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts*, 2000, S. 511, 524; vgl. dazu auch: Specht, Diktat der Technik, 2019, S. 168.

38 Arnold/Hillebrand/Waldburg, DuD 2015, S. 730 ff.; Kühnl, *Persönlichkeitsschutz 2.0*, Diss. Köln 2016, S. 342; Calo, 87 Notre Dame Law Review 1027, 1071 (2012); Heckmann/Paschke, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 12 Rn. 53.

39 Siehe aktuelle Studie: *Rothmann, Ungewollte Einwilligung? Die Rechtswirklichkeit der Informierten Zustimmung im Fall von Facebook*, nachzulesen bei: DuD 2018, S. 342 u. 344.

40 Arnold/Hillebrand/Waldburg, DuD 2015, S. 730 u. 732.

41 Vgl. dazu bereits: Specht-Riemenschneider/Bienemann, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), *Datenrecht in der Digitalisierung*, 2020, S. 330.

42 European Commission, Special Eurobarometer 431 – Data Protection, 2015, S. 85 u. 89; vgl. auch: Spindler/Thorun/Wittmann, Rechtsdurchsetzung im Verbraucherdatenschutz, S. 13

43 Specht-Riemenschneider/Bienemann, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2020, S. 330.

44 Kelley/Bresee/Cranor/Reeder, *A „Nutrition Label" for Privacy*, S. 6, online unter http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf, zuletzt abgerufen am: 6.2.2021.

45 Kelley/Cesca/Bresee/Cranor, *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, S. 8, online unter: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1002&context=cylab (6.2.2018).

46 Art. 13a Abs. 2 des Parlamentsentwurfs zur DSG-VO vom 12.3.2014 (EP-PE_TC1-COD(2012)0011).

47 Kroeber-Riel, *Bildkommunikation*, 2. Aufl. 1996, S. 26 ff. u. 53 ff.; vgl. dazu auch: Maar, in: Maar/Burda, *Iconic Worlds*, 2006, S. 11.

48 Bauer/Fischer/McInturff, ZfbF 51 (9/1999), S. 805 u. 815; Schierl, *Text und Bild in der Werbung*, 2001, S. 228.

49 Kroeber-Riel, a. a. O., S. 53; vgl. zur Geschwindigkeit visueller Kommunikationsaufnahme: Boehme-Neßler, BilderRecht, 2010, S. 64 f.

50 Kroeber-Riel, a. a. O. S. 102.

51 Zu den Gründen vgl. Kroeber-Riel, a. a. O., S. 73 ff. m. w. Nachw.; zur Bilderinnerung vgl. auch: Madigan, in: Yuille, *Imagery, Memory and Cognition*, 1983, S. 65 u. 65 ff.; Specht, *Diktat der Technik, im Erscheinen*; vgl. zum Ganzen auch: Specht-Riemenschneider/Bienemann, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), *Datenrecht in der Digitalisierung*, 2020, S. 334 f.; Geminn/Francis/Herder, ZD-Aktuell, 2021; Gerpott, MMR 2020, S. 739;

52 Krämer, *Journal of Competition Law & Economics 2021*, S. 263; Wendehorst/Schwamberger/Grinzinger, in: Pertot (Hrsg.), *Rechte an Daten*, 2020, S. 104 f.

53 Zur Analyse des sog. Erwartungskalküls i. R. d. Rechtsmittel vgl. Brandes/Weise, *German Working Papers in Law and Economics*, 2009, Paper 7; vgl. auch Kaesling/Knapp, MMR 2020, S. 816 u. 820.

54 Urban/Karaganis/Schofield, *UC Berkley Public Law Research Paper No. 2755628*, 2017, S. 45; vgl. auch Kaesling/Knapp, MMR 2020, S. 816 u. 820.

55 Akester, *Technological Accommodation of Conflicts Between Freedom of Expression and DRM: The First Empirical Assessment*, 2009, S. 104 f.; Penney, *Stanford Technology Law Review*, 2019, S. 412.

56 Kerber, WuW 2021, S. 400.

57 Ebd.

58 Europäischer Datenschutzbeauftragter (EDSB), *Stellungnahme zu Systemen für das Personal Information Management (PIM), Stellungnahme 9/2016* (201), S. 6.

59 Janssen/Cobbe et al., *Internet Policy Review 2020*, Volume 9, Issue 4, 1 (2), online unter https://doi.org/10.14763/2020.4.1536 (zuletzt abgerufen am 18.11.2021).

60 Definition in Anlehnung an: Weinzierl, NVwZ 2020, S. 1087.

61 Engeler, *Stellungnahme zum Entwurf eines TTDSG, BT-Ausschussdrucksache* 19(9)1056, 20.4.2021, S. 4 ff., online unter: https://www.bundestag.de/resource/blob/836166/e95c01bdb37ed9f6c08ef027cd902e47/19-9-1056_Stellungnahme_SV_Dr-_Engeler_oeATTDSG_21-04-2021-data.pdf (zuletzt abgerufen am 18.11.2021); Janssen/Cobbe et al., *Internet Policy Review 2020*, Volume 9, Issue 4, 1, S. 13 ff., online unter: https://doi.org/10.14763/2020.4.1536 (zuletzt abgerufen am 18.11.2021).

62 *Datentreuhänder gesetzlich regeln – Stellungnahme des VZVB*, S. 6, online unter: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zuletzt abgerufen am 18.11.2021).

63 Freiherr von Ulmenstein, DuD 2020, S. 528 f.

64 Vgl. Zur Vertragsgestaltung zwischen Betroffenem und Datentreuhänder Pinsent Masons et al., *Data Trusts: Legal and Governance Considerations,* 2019, S. 26 f., online unter: https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf (zuletzt abgerufen am 18.11.2021).

65 Specht-Riemenschneider/Blankertz et. al., MMR-Beil, 2021, S. 25 u. 40 f.

66 *Datentreuhänder gesetzlich regeln – Stellungnahme des VZVB*, online unter: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zuletzt abgerufen am 18.11.2021).

67 Auch die Datenethikkommission sieht beide Perspektiven auf PIMS, vgl. Gutachten Datenethikkommission, Oktober 2019, S. 135, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4D-BFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am 18.11.2021).

68 *Gutachten Datenethikkommission*, Oktober 2019, S. 134, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4D-BFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am 18.11.2021).

69 Schwartmann/Benedikt/Reif, MMR 2021, S. 99 u. 101; Schwartmann/Hanloser/Weiß, *PIMS im TTDSG – Vorschlag zur Regelung von Diensten zur Einwilligungsverwaltung im Telekommunikation-Telemedien-Datenschutzgesetz, Kurzgutachten*, März 2021, S. 10, online unter: https://enid.foundation/wp-content/uploads/2021/03/Schwartmann_Hanloser_Weiss-Kurzgutachten_Dienste_zur_Einwilligungsverwaltung_20210302.pdf (zuletzt abgerufen am 18.11.2021); a. A. Assion, Stellungnahme als Sachverständiger zu BT-Drs. 19/27441, Ausschuss-Drs. 19(9)1039 v. 19.04.2021, S. 12, online unter: https://www.bundestag.de/resource/blob/835498/3fc24ea374301c2ba608c9509cc64ec1/19-9-1039_Stellungnahme_SV_Assion_oeA_TTDSG_21-04-2021-data.pdf (zuletzt abgerufen am 18.11.2021).

70 Ein Überblick über die Marktversagensprobleme beim Standard-setting geben Farrell/Simcoe, *Four Paths to Compatibility*, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, S. 34–58.

71 Im Anwendungsbereich der Art. 13, 14 DSGVO ist dies nur dann möglich, wenn zusätzlich textbasierte Informationen erteilt werden, vgl. Specht-Riemenschneider/Bienemann, in: Specht-Riemenschneider/Werry/Werry (Hrsg.), *Datenrecht in der Digitalisierung*, 2020, S. 324 f.

72 Ebd., S. 339; *SVRV – Gutachten zur Lage der Verbraucherinnen und Verbraucher 2021*, S. 392, online unter: https://www.svr-verbraucherfragen.de/wp-content/uploads/SVRV_Gutachten_2020.pdf (zuletzt abgerufen am 18.11.2021).

73 Kroeber-Riehl, *Bildkommunikation*, 1996, S. 53, S. 73 ff.

74 Am Weizenbaum-Institut werden z. B. derartige Lösungen entwickelt, vgl. MMR-Aktuell 2019.

75 Ablehnend: Ernst, ZD 2017, S. 110 f.; Klement, in: *NK-DatenschutzR*, 1. Aufl. 2019, Art. 7 DSGVO Rn. 37; Taeger, in: Taeger/Gabel, DSGVO/BDSG, 3. Aufl. 2019, Art. 7 DSGVO Rn. 10; Schulz, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DSGVO Rn. 9; Heckmann/Paschke, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 7 DSGVO Rn. 34; Helfrich, in: Hoeren/Sieber/Holznagel, *MultimediaR*, Oktober 2020, Teil 16.1.D. I. Rn. 51; dafür aber: Janicki, DSRITB 2019, 313, 323; Hoffmann, NZS 2017, 807, 808; Specht, in: Specht/Mantz, *Hdb. Europäisches und deutsches DatenschutzR*, 1. Aufl. 2019, § 9 Rn. 42; Ingold, in: Sydow,

EU DSGVO, 2. Aufl. 2018, Art. 7 DSGVO Rn. 19; Buchner/Kühling, in: Kühling/Buchner, DSGVO/BDSG, 3. Aufl. 2020, Art. 7 DSGVO Rn. 31; Gierschmann/Schlender/Stentzel/Veil-Gierschmann, Art. 7 DSGVO Rn. 47.

76 Zur Einwilligung insgesamt vgl. grundlegen: Ohly, *„Volenti non fit iniuria" – Die Einwilligung im Privatrecht*, 2002.

77 Specht-Riemenschneider, in: Specht/Mantz, *Hdb. Europäisches und deutsches DatenschutzR*, 1. Aufl. 2019, § 9 Rn. 42; Ingold, in: Sydow, EU DSGVO, 2. Aufl. 2018, Art. 7 DSGVO, Rn. 19; Buchner/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 7 DS-GVO, Rn. 31.

78 Specht-Riemenschneider, in: Specht/Mantz, *Hdb. Europäisches und deutsches DatenschutzR*, 1. Aufl. 2019, § 9, Rn. 42; Ingold, in: Sydow, EU DSGVO, 2. Aufl. 2018, Art. 7 DSGVO, Rn. 19; Buchner/Kühling, n: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 7 DS-GVO, Rn. 31; Kühling, ZfDR 2021, 1, 8.

79 So zutreffend Kühling, ZfDR 2021, 1, 8.

80 Riesenhuber, in: Riesenhuber, *Europäische Methodenlehre*, 3. Aufl. 2015, § 10 Rn. 4–7.

81 MMR-Beitrag zitieren.

82 MüKo BGB-Schubert, 8. Auflage 2018, § 164 Rn. 72.

83 Lang, TTDSG – *Neuregelung des Datenschutzes in den Bereichen Telekommunikation und Telemedien geplant*, K&R 2020, S. 714 u. 716; Richter, *Stellungnahme zur öffentlichen Anhörung des Wirtschaftsausschusses am 24.02.2021 zum Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien*, 2021, S. 3, online unter: https://www.bundestag.de/resource/blob/835918/ed8f50751361504905bfa51b4ee6f738/19-9-1045_Stellungnahme_SV_Richter_Stiftung_Datenschutz_oeA_TTDSG_21-04-2021-data.pdf (zuletzt abgerufen am 18.11.2021).

84 Art.-29-Datenschutzgruppe, WP 259, S. 13; WP 187, S. 20 f.; WP 131, S. 9.

85 Verbraucherzentrale Bundesverband, *Personal Information Management Systems (PIMS)*, 2020, S. 7, online unter: https://www.vzbv.de/sites/default/files/downloads/2020/04/06/20-02-19_vzbv-positionspapier_pims.pdf (zuletzt abgerufen am 16.07.2021).

86 Online unter: https://www.medizin-informatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf (zuletzt abgerufen am 18.11.2021).

87 Gutachten Datenethikkommission, Oktober 2019, S. 127, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am 18.11.2021).

88 Ebd.

89 Ebd., S. 126 f.

90 Specht/Blankertz et al., MMR-Beil, 2021, S. 25 u. 42 f.

91 Gutachten Datenethikkommission, Oktober 2019, Empfehlung 23, S. 140, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am 18.11.2021).

92 Vgl. zu dieser Wahlmöglichkeit nur Golland, MMR 2018, 130 (134); Golland, *Datenschutzregulierung als Eingriff in Wertschöpfungsmodelle*, in: Ochs/Friedewald/Hess/Lamla (Hrsg.), *Die Zukunft der Datenökonomie*, 2019, S. 45 u. S. 54.

93 S. hierzu oben IV.

94 Vgl. Blankertz/Specht-Riemenschneider, *What Regulation for Data Trusts Should Look Like*, S. 28 ff., online unter https://www.stiftung-nv.de/sites/default/files/regulation_for_data_trusts_0.pdf (zuletzt abgerufen am 18.11.2021).

95 Vgl. VZBV, *Neue Datenintermediäre*, 15.9.2020, S. 7, online unter: https://www.vzbv.de/publikationen/datenintermediaere-gesetzlich-regeln (zuletzt abgerufen am 18.11.2021).

96 Krämer, *Journal of Competition Law & Economics*, 2020, 1 (38).

97 Vgl. Schwartmann/Hentsch, PinG 2016, S. 117 ff.; dagegen aber: Bisges, MMR 2017, S. 301; Specht, in: *Stiftung Datenschutz, Datendebatten, Rechte an Daten – Regulierungsbedarf aus Sicht des Verbraucherschutzes*.

98 Gutachten Datenethikkommission, Oktober 2019, S. 134, online unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=92AD72B05F123D4DBFCC72D56297DE96.2_cid295?__blob=publicationFile&v=6 (zuletzt abgerufen am 18.11.2021).

99 BT-Drs. 19/29839, S. 78.

100 Ebd.

101 So auch: Golland, NJW 2021, S. 2238 u. 2241.

102 Zutreffend: Ebd.

103 In Finnland existiert zu diesem Zweck Findata, s. https://findata.fi/en/ (zuletzt abgerufen am 18.11.2021). In Australien werden Gesundheitsdaten, die über ‚My Health Record' gespeichert sind, durch ein Data Governance Board verwaltet, vgl. Australian Department of Health, *Framework to Guide the Secondary use of My Health Record System Data*, S. 15, online unter https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf (zuletzt abgerufen am 18.11.2021); s. zu beiden Institutionen den folgenden Abschnitt.

104 Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, online unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/REG-GUT-2021_Registergutachten_BQS-TMF-Gutachtenteam_2021-10-29.pdf, S. 255 f. (zuletzt abgerufen am 18.11.2021).

105 Ob Findata oder der Datenhalter selbst für die Erteilung der Erlaubnis zuständig sind, richtet sich nach Sect. 44 des Secondary Use Acts.

106 Siehe Specht-Riemenschneider, Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität, August 2021, S. 102 ff., online unter https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (zuletzt abgerufen am 18.11.2021).

107 Australian Government – Department of Health, *Framework to Guide the Secondary Use of My Health Record System Data*, S. 31, online unter: https://www1.health.gov.au/internet/main/publishing.nsf/content/F98C37D22E65A79BCA2582820006F1CF/$File/MHR_2nd_Use_Framework_2018_ACC_AW3.pdf (zuletzt abgerufen am 18.11.2021).

108 ebd S. 47.

109 Australian Government – Department of Health, a. a. O., S. 31; s. auch Specht-Riemenschneider, a. a. O. S. 106 ff.

110 Australian Government – Department of Health, a. a. O., S. 51.

111 Zu den genauen Gründen vgl. oben VI. 3.

112 Kircher, GuP 2021, S. 1 u. 5 f.
113 Vgl. auch Strech/von Kielmannsegg/Zenker/Krawczak/Semler, „Datenspende“ – Bedarf für die Forschung, ethische Bewertung, rechtliche, informationstechnologische und organisatorische Rahmenbedingungen, 2020, S. 125 ff., online unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Ministerium/Berichte/Gutachten_Datenspende.pdf (zuletzt abgerufen am 18.11.2021).
114 https://www.tmf-ev.de/zoombild.aspx?img=/Portals/0/TMF_07rz_01.jpg&text= (zuletzt abgerufen am 18.11.2021); https://www.tmf-ev.de/News/articleType/ArticleView/articleId/4456.aspx (zuletzt abgerufen am 18.11.2021); Specht-Riemenschneider, a. a. O., S. 127.
115 Vgl. Dazu auch: Kircher, GuP 2021, S. 1 u. 4.
116 Vgl. §§ 13, 15 Gesundheitstelematikgesetz 2012, Fassung vom 18.11.2021.
117 Samuelson/Zweckhauer, *Journal of Risk and Uncertainty*, S. 7 ff.
118 Vgl. zur datenschutzrechtlichen Kritik an der deutschen Regelung, die nach Auffassung der Datenschutzbehörden eine zu geringe Granularität der Einwilligung vorsieht und daher die Anforderungen an die Freiwilligkeit der Einwilligung nicht erfülle: DSK, Entschließung v. 1.9.2020, online unter: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf (zuletzt abgerufen am 18.11.2021); zur Frage, ob eine Granularität der Einwilligung für ihre Freiwilligkeit tatsächlich erforderlich ist: Kircher, GuP 2021, S. 1 u. 8 f.
119 Specht-Riemenschneider, a. a. O., S. 143.
120 Jarass, in: Ders., EU-Grundrechte-Charta, 4. Auflage, 2021, Art. 13 Rn. 8 m. w. Nachw. 324 Bernsdorff, in: Meyer/Hölscheidt, *Charta der Grundrechte der Europäischen Union*, 5. Auflage, 2019, Art. 13 Rn. 14.
121 Specht-Riemenschneider, a. a. O., S. 148.
122 Vgl. Medizininformatik-Initiative, online unter: https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf (zuletzt abgerufen am 18.11.2021)
123 DSK, Entschließung v. 1.9.2020, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20200901_PDSG_Entschlie%C3%9Fung.pdf (zuletzt abgerufen am 18.11.2021).
124 Kickingereder/Burth et al., Radiology 2016, S. 880 ff.
125 Specht-Riemenschneider, GRUR Int. 2017, S. 1040 u. 1042 ff.
126 Specht-Riemenschneider/Radbruch, *Deutsches Ärzteblatt*, Heft 27/28 2021, online unter: https://www.aerzteblatt.de/archiv/220270/Datennutzung-und-schutz-in-der-Medizin-Forschung-braucht-Daten (zuletzt abgerufen am 18.11.2021).
127 ebd.
128 Specht-Riemenschneider, Studie zum Forschungsdatenzugang im Auftrag des BMBF, S. 142 f.
129 Blankertz, Vertrauliche Datentreuhand – Wie die Datentreuhand effektiv Daten schützen und sichern kann, erscheint in DuD 2021.
130 Ebd.
131 Specht-Riemenschneider, a. a. O., S. 148 f.
132 Ebd., S. 148.
133 Bspw. Apheris oder Decentriq.
134 Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten (NGD), S. 2 ff.
135 Vgl. Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, online unter: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/5_Publikationen/Gesundheit/Berichte/REG-GUT-2021_Registergutachten_BQS-TMF-Gutachtenteam_2021-10-29.pdf (zuletzt abgerufen am 18.11.2021).
136 Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten (NGD), S. 2 ff.
137 Specht-Riemenschneider, a. a. O., S. 140.
138 Zu den einzelnen Verarbeitungsschritten vgl. *Machbarkeitsstudie virtuelles Netzwerk Gesundheitsdaten* (NGD), S. 14 ff.
139 Vgl. Art. 1 DGA-E.
140 In der Ratsfassung vom 24.9.2021.
141 KVs sind in der Regel in der Rechtsform der AG oder der VVAG tätig.
142 In der Ratsfassung vom 7.9.2021.
143 so zutreffend Richter, ZEuP 2021, S. 534 u. 650, mwN.
144 COM (2020) 767 final, S. 9; krit. Veil, *Data Governance Act III: Datenaltruismus*, CR-online.de, 28.10.2021, online unter: https://www.cr-online.de/blog/2021/10/28/data-governance-act-iii-datenaltruismus/ (zuletzt abgerufen am: 18.11.2021).
145 Spindler, CR 2021, S. 98 u. 106.
146 Vgl. grundsätzlich zu vernetzten Fahrzeugen OECD/ITF, Automated and Autonomous Driving. Regulation under Uncertainty. Corporate Partnership Report, 2015; Alonso Raposo/Ciuffo/Makridis/Thiel, The R-Evolution of Driving: From Connected Vehicles to Coordinated Automated Road Transport (C-ART), 2017, online unter: https://op.europa.eu/en/publication-detail/-/publication/7eed7b8e-44e2-11e7-aea8-01aa75ed71a1/language-en (zuletzt abgerufen am 18.11.2021).
147 Vgl. als Überblick Kerber, JIPITEC, 2018, S. 312–315; Specht/Kerber, *Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA*, 2018, S. 169–192; Martens/Mueller-Langer, Journal of Competition Law & Economics 16, 2020, S. 116–141.
148 Vgl. zum ‚Extended Vehicle‘-Konzept der Autohersteller ACEA, *Access to Vehicle Data for Third-party Services*, 2016; ACEA, *Access to In-Vehicle Data* (November 2021). Für die Kritik anderer Serviceanbieter und Verbraucherverbände vgl. FIGIEFA, *Commission Communication on „Free Flow of Data“. Input from the Independent Automotive Aftermarket*, 2016; FIA, *Policy Position on Car Connectivity*, 2016; BEUC, *Protecting European Consumers with Connected and Automated Cars*, 2017.
149 C-ITS Platform, Final Report, 2016, S. 72–90.
150 TRL, Access to In-Vehicle Data and Resources – *Final Report*, 2017, S. 8–16.
151 EU Commission, On the Road to Automated Mobility, COM (2018) 283 fin., S. 13; vgl. auch die Forderung des Europäischen Parlaments für eine Lösung (Report on a European Strategy on Cooperative Intelligent Transport Systems, 2017/2067, INI). Committee on Transport and Tourism (PE610.712v02-00).
152 Vgl. *die Vorschläge des 56. Deutscher Verkehrsgerichtstag, Arbeitskreis II, Empfehlung Nr. 5*, einsehbar bei: Janker, SVR 2018, 78, 79; ähnlich: vzbv, *Rechtssicher fahren mit automatisierten Fahrzeugen*, 2016, S. 14; kritisch: Brockmeyer, ZD 2018, 258, 259 f.; Wagner/Goeble, ZD 2017, 263, 267; sowie: Hoeren, NZV 2018, 153.
153 Zur Unterscheidung/Abgrenzung des § 63a zum § 1g Abs. 5 vgl. Möller, DAR 2021, 608, 610 f.; Steeger, SVR 2021, 128, 134; Wagner, SVR 2021, 287, 289 ff.
154 Regulation (EU) 715/2007 of 20 June 2007 of the European Parliament and of the Council on Type Approval of Motor Vehicles with Respect to Emissions from Light Passenger and Commercial Vehicles (Euro 5 and Euro 6) and on Access to Vehicle Repair and Maintenance Information, *Official Journal of the European Union*, L 171/1, 29.6.2007.
155 Kerber/Gill, JIPITEC, 2019, S. 246 f.

156 Vgl. zur letzten Reform 2018: Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the Approval and Market Surveillance of Motor Vehicles and their Trailers, and of Systems, Components and Separate Technical Units Intended for Such Vehicles, Amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and Repealing Directive 2007/46/EC, *Official Journal of the European Union*, L 151/1, 14.6.2018. Diese Reform der Kfz-Typenzulassungsverordnung hat dieses Problem gerade nicht gelöst (vgl. ausführlich Kerber/Gill, JIPITEC, 2019, S. 250–254).

157 Vgl. zur folgenden Analyse aus einer ökonomischen Perspektive Kerber, JIPITEC, 2018, S. 310–331; Martens/Mueller-Langer, *Access to Digital Car Data and Competition in Aftersales Services*, Digital Economy Working Paper 2018-06, JRC Technical Reports, 2018.

158 Der Zugang zum Dashboard (HMI = Human Machine Interface) ist wichtig für eine direkte Kommunikation zwischen Autonutzerinnen und -nutzern sowie unabhängigen Servicebetreibern.

159 Zu den Vor- und Nachteilen von offenen und geschlossenen Modellen von vernetzten Fahrzeugen vgl. Determann/Perens, *Berkeley Technology Law Journal*, 2017, S. 915.

160 Solche Kombinationen von Datenzugangsproblemen und Interoperabilitätsproblemen sind aus anderen Bereichen der Wettbewerbspolitik inzwischen gut bekannt.

161 Es handelt sich hier um einen etwas anderen Gatekeeper-Begriff als im ‚Digital Markets Act'-Vorschlag der EU-Kommission. Hier geht es um den Zugang zum Ökosystem des vernetzten Fahrens mit seinen vielfältigen Sekundärmärkten, den die Autohersteller durch ihre exklusive Kontrolle über die Daten und den technischen Zugang vollständig kontrollieren können.

162 Für bestimmte Daten, wie bspw. Standortdaten, kann es auch die Alternative des Zugangs über Handydaten geben.

163 Vgl. ausführlich Kerber, JIPITEC, 2018, S. 319–321. Es kann auch nicht erwartet werden, dass dieses Problem durch einen Systemwettbewerb zwischen den Autoherstellern gelöst wird. Vgl. ebd., S. 324.

164 Den Verfassern ist bewusst, dass der sachenrechtliche Begriff der Aneignung für unkörperliche Gegenstände wie Daten nicht passt; er soll hier daher nicht in diesem Sinne verstanden werden, sondern zum Ausdruck bringen, dass die Hersteller faktisch die Kontrolle über die betreffenden Daten erlangen. Diese de facto exklusive Kontrolle über die Daten wirkt jedoch ökonomisch wie eine „eigentumsähnliche" Position.

165 Diese Problematik, dass die Hersteller von smarten Geräten sich die exklusive Kontrolle der (mit ihnen von den Nutzerinnen und Nutzern generierten) Daten „aneignen" und ökonomisch verwerten, tritt auch in anderen Bereichen auf, bspw. smarten landwirtschaftlichen Geräten oder smarten TV-Geräten.

166 Vgl. zu den negativen Wohlfahrtswirkungen monopolistischer Datenpreise, Martens, in: Drexl, *Data Access, Consumer Interests and Public Welfare*, 2021, S. 74.

167 Vgl. zu den verschiedenen alternativen Lösungen C-ITS Platform, Final Report, 2016, S. 78–86; TRL, *Access to In-Vehicle Data and Resources – Final Report*, 2017, S. 32–49; Martens/Mueller-Langer, *Access to Digital Car Data and Competition in Aftersales Services*, JRC Digital Economy Working Paper 2018-06, S. 7–13.

168 Im ‚Extended Vehicle'-Konzept der Automobilhersteller gibt es auch einen neutralen Server, der sich jedoch nur auf diejenigen Daten bezieht, die die Autohersteller selbst anderen Serviceanbietern zur Verfügung stellen wollen.

Dies hat nichts mit der ‚Shared Server'-Lösung und der später noch genauer zu präsentierenden Lösung eines „neutralen" Datentreuhänders zu tun.

169 Vgl. Martens/Mueller-Langer, *Access to Digital Car Data and Competition in Aftersales Services*, JRC Digital Economy Working Paper 2018-06, S. 13; Kerber, JIPITEC, 2018, S. 322, wo auch auf die Möglichkeit eines Marktversagens in Bezug auf die Wahl der optimalen Technologie im Hinblick auf Interoperabilität hingewiesen wird. Standardisierte ‚On-Board Application'-Plattformen sind auch für zukünftige V2I (Vehicle-to-Infrastructure) oder V2V (Vehicle-to-Vehicle) Kommunikation zur Verbesserung der Fahrsicherheit und des Verkehrsflusses von zentraler Bedeutung.

170 TRL, *Access to In-Vehicle Data and Resources – Final Report*, 2017, S. 8–16. TRL betont, dass alle drei Lösungen Vor- und Nachteile haben, kommt dann insgesamt jedoch zu dem obigen eindeutigen Gesamtergebnis. Für eine ausführliche Analyse der Positionen von Stakeholdern in dieser Diskussion vgl. Specht/Kerber, *Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA*, 2018, S. 169–191.

171 TRL, a. a. O., S. 75–79; Martens/Mueller-Langer, a. a. O., S. 12; FIA/TÜVIT, IT Security der On-Board Telematik Plattform, 2020; ADPA et al., *Secure On-Board Telematics Platform Approach*, February 2021.

172 Vgl. auch Kerber, JIPITEC, 2018, S. 318 f.: Hieraus folgt insbesondere auch, dass es kein Trade-off-Problem zwischen Wettbewerb und Sicherheit gibt, d. h. man muss nicht zugunsten von mehr Sicherheit auf Wettbewerb verzichten. Weiterhin kann aus dem Sicherheitsargument nicht die Notwendigkeit der exklusiven Kontrolle über Daten abgeleitet werden (ibid.).

173 Vgl. EU Commission, *A European Strategy for Data*, COM (2020) 66 fin., S. 27 f.; zuletzt war für das vierte Quartal 2021 ein Vorschlag für eine Reform der Kfz-Typenzulassungsverordnung angekündigt, der aber erneut verschoben wurde.

174 Da bisher kein Vorschlag vorliegt, kann dies hier nicht diskutiert werden.

175 Es könnte auch darüber nachgedacht werden, diese Datenzugangsprobleme durch wettbewerbsrechtliche Datenzugangsansprüche oder über das Datenportabilitätsrecht von Art. 20 DSGVO zu lösen. Zu den Schwierigkeiten einer wettbewerbsrechtlichen Lösung vgl. Kerber, *Journal of Competition Law & Economics*, 2019, S. 381–426; zur Problematik einer Lösung über das Datenportabilitätsrecht, vgl. Martens/Mueller-Langer, *Journal of Competition Law and Economics*, 2020, S. 116–141; Gill/Kerber, *Competition Policy International, Antitrust Chronicle*, November 2020, S. 54–59. Vgl. hierzu auch grundsätzlich Picht, *International Review of Intellectual Property and Competition Law* 51, 2020, S. 940–976.

176 Vgl. hierzu Kerber/Gill, JIPITEC, 2019, S. 255 f.

177 Dies ist auch bereits im bisherigen Zugangsregime der Kfz-Typenzulassungsverordnung so geregelt gewesen, auch wenn der aus der Diskussion über digitale Plattformen und dem ‚Digital Markets Act'-Vorschlag jetzt sehr bekannte Begriff der Selbstbevorzugung dort nicht verwendet wird. Wichtig ist dabei auch, dass die Autohersteller kein Monitoring machen dürfen bzgl. der abgerufenen Daten oder sich durch ihre viel breitere Verfügung über Daten Vorteile gegenüber den unabhängigen Serviceanbietern verschaffen dürfen (Kerber/Gill, JIPITEC, 2019, 253 f.).

178 Aus einer wettbewerbspolitischen Perspektive geht es darum, Daten für mehr Wettbewerb und Innovation zu FRAND-Bedingungen zur Verfügung zu stellen, damit auch bisher unbekannte neue Services und neue Märkte entstehen können.

179 In der aktuellen Diskussion wird dabei auch von der Notwendigkeit einer Separation of Duties ausgegangen, d. h. dass diejenigen Entitäten, die für die Zugangsautorisierung und für die Zulassung von Software von Serviceanbietern zuständig sind, unabhängig von den Autoherstellern als Betreiber der vernetzten Fahrzeuge sind.

180 Insofern ist ein Vorgehen nach einer vorgegebenen Liste von existierenden Use Cases nicht geeignet; vielmehr sollte man sich aus Innovationssicht wesentlich stärker an der Idee von Open Data orientieren.

181 Folglich sind auch Ansätze, die auf freiwilliges Data Sharing nach gewissen Prinzipien setzen, ungeeignet, die Probleme für Wettbewerb und Innovation zu lösen.

182 Obwohl die „Shared Server"-Lösung als eine mögliche Lösungsoption bereits auf der C-ITS-Plattform diskutiert und auch von der TRL-Studie empfohlen wurde, ist die Frage der konkreten Ausgestaltung dieser Governance-Lösung wenig diskutiert worden. Ursprünglich war die Idee, dass alle Stakeholder, die am Zugang zu den Daten interessiert sind, diese Daten gemeinsam verwalten, d. h. die Autohersteller und die verschiedenen Typen von Serviceanbietern (vgl. C-ITS Platform, *Final Report*, 2016, S. 81 f.).

183 Die Frage, wo die Daten konkret gespeichert werden, kann sehr unterschiedlich gelöst werden. Entscheidend ist die exklusive Kontrolle durch die Datentreuhand.

184 Die Autohersteller können auch weiterhin für das IT-System des Fahrzeugs und die Sicherheit verantwortlich sein (einschließlich Haftung), hätten dann allerdings die Rolle eines IT-Dienstleisters.

185 Dies würde bspw. auch für die bereits diskutierte spezielle Datentreuhänderregelung bzgl. Daten aus Fahrzeugen mit automatisierten Fahrfunktionen gelten, die derzeit am Forschungsdatenzentrum beim Kraftfahrtbundesamt gespeichert werden.

186 "A Common European mobility data space, to position Europe at the forefront of the development of an intelligent transport system, including connected cars as well as other modes of transport. Such data space will facilitate access, pooling and sharing of data from existing and future transport and mobility databases." (*EU Commission,* A European Strategy for Data, COM(2020) 66 fin., S. 22).

187 Auch wenn es sich hier um keine Public Sector Information handelt, könnte darüber nachgedacht werden, ob nicht auch die dort angewendeten Prinzipien zumindest zum Teil auch bei einer Datentreuhand eine Rolle spielen könnten. Denn auch diese Datentreuhand hat die Aufgabe, Daten für Innovation und die weitere wirtschaftliche Nutzung zugänglich zu machen, soweit nicht die Rechte Dritter tangiert sind (Geschäftsgeheimnisse etc., Datenschutz).

188 Die Automobilclubs und Verbraucherverbände haben sich in dieser Auseinandersetzung über das „Extended Vehicle"-Konzept klar auf die Seite der unabhängigen Serviceanbieter gestellt. Vgl. FIA, Policy Position on Car Connectivity, 2016; BEUC, *Protecting European Consumers with Connected and Automated Cars*, 2017.

189 Auf der erwähnten C-ITS-Plattform haben sich die Stakeholder auf fünf Leitprinzipien geeinigt. Das erste dieser Prinzipien bezieht sich auf die Einwilligung zur Verfügungstellung von Daten: „(a) Data Provision conditions: Consent: The data subject (owner of the vehicle and/or … the user of the vehicle…) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end users and data subjects. This is without prejudice to requirements of regulatory applications." (C-ITS Platform, *Final Report*, 2016, S. 75 f.). Vgl. aus verbraucherpolitischer Sicht FIA, *Policy Position* on *Car Connectivity*, 2016; BEUC, *Protecting European Consumers with Connected and Automated Cars*, 2017, aus datenschutzrechtlicher Sicht Hornung/Goeble, *Computer und Recht*, 2015, S. 265, Hansen, in: *Grundrechtsschutz im Smart Car*, 2019, S. 273, und aus ökonomischer Sicht zu den Problemen der Autonutzerinnen und -nutzer bzgl. der datenschutzrechtlichen „Einwilligungen" Kerber, JIPITEC, 2018, S. 323.

190 BfDI, *Musterbescheid gesetzliche Krankenkassen*, online unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2021/2021_Musterbescheid-Gesetzliche-Krankenkasse.pdf?__blob=publicationFile&v=1 (zuletzt abgerufen am 22.11.2021).

191 Selbstverständlich ließe sich auch darüber nachdenken, dass das Interoperabilitätsproblem in der Kfz-Typenzulassungsverordnung geregelt werden könnte, während sich die Datentreuhand auf die Governance der Daten beschränkt. Aber dies würde eine sehr sorgfältige Koordination erfordern, da die Daten- und Interoperabilitätsprobleme eng miteinander verknüpft sind.

192 Vgl. Kerber, in: Drexl, Data Access, Consumer Interests and Public Welfare, 2021, S. 461–474.

193 Insofern müsste eine solche vertragliche Bindung wettbewerbsrechtlich untersagt werden, zumindest bzgl. solcher Daten, die nicht für den unmittelbaren Betrieb des Fahrzeugs erforderlich sind.

194 Vgl. EU Commission, *Building a European Data Economy*, COM (2017), 9 final; EU Commission, *A European Strategy for Data*, COM (2020), 66 final.

195 Das parallele Problem der Kontrolle großer Mengen von personenbezogenen Daten durch die großen Digitalkonzerne ist wohlbekannt und bisher ungelöst.

196 Gerade in Bezug auf Mobilitätsdaten könnte die Idee, „Daten als Infrastruktur" für Innovationen zu verstehen, besonders gut anwendbar sein. Vgl. OECD, *Data-Driven Innovation*, 2015; vgl. auch die jüngst erschienene Studie über Datenallmende Bertschek/Bonin/Kühling/Thüsing/Wenzel, *Entwicklung eines Konzepts zur Datenallmende* (Expertise im Auftrag des Bundesministeriums für Arbeit und Soziales), 2021 (IZA Research Report No. 119).

197 Das vor kurzem veröffentlichte Positionspapier des europäischen Automobilverbands ACEA (ACEA Position Paper). *Access to In-Vehicle Data*, November 2021) verteidigt erneut das „Extended Vehicle"-Konzept der Autohersteller. In ihm finden sich nur kleine Zugeständnisse, die an dem Kern dieses Konzepts und der hier dargestellten Probleme nichts ändern. Es entspricht insbesondere auch nicht den Anforderungen an eine regulierte FRAND-Lösung wie sie hier als Lösungsoption I beschrieben wurde.

198 Allerdings könnte auch eine wohlabgestimmte Kombination von horizontalen Regeln eines zukünftigen Data Acts und einer sektorspezifischen Regulierung zu wirksamen Lösungen führen.

199 Vor diesem Hintergrund beabsichtigte bereits die ITS Richtline von 2010 eine entsprechende Plattform im Fahrzeug, welche die direkte Vernetzung mit der Transport Infrastruktur ermöglichen soll. (Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, OJEU L 207/1.) Ebenfalls die seit April 2018 verpflichtend einzubauenden eCall-Notrufsysteme basieren auf einer solchen interoperablen, standardisierten, sicheren, und offenen Plattform (Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, OJEU L 123/77).

6 Zusammenfassung der Ergebnisse in rechtspolitischen Handlungsempfehlungen

Die Ergebnisse dieses Gutachtens lassen sich in folgenden rechtspolitischen Handlungsempfehlungen zusammenfassen:

Grundsätzliches

1. Mithilfe der Datentreuhand kann zur Lösung vielfältiger Probleme in der Digitalwirtschaft beigetragen werden. Entscheidend für ihren treuhänderischen Charakter ist die Bindung im Innenverhältnis zum Datengeber: Ein Treuhänder hat sein Handeln an den Interessen der anderen Vertragspartei auszurichten. Seine eigenen Interessen hat er nötigenfalls zurückzustellen. Der Datenintermediär ist dagegen im Innenverhältnis nicht derart gebunden. Damit ist der Datenintermediär der Oberbegriff, die Datentreuhand eine Unterform, die wiederum ihrerseits verschiedentlich ausgestaltet werden kann. Neben den zentralen Unterscheidungen zwischen zentraler und dezentraler Datenspeicherung sowie obligatorischer und fakultativer Nutzung können Datentreuhänder vielfältige Funktionen übernehmen, wie etwa die Pseudonymisierung und Anonymisierung oder auch die Auswertung von Daten. Neben PIMS können daher zum Beispiel auch Data Escrows Datentreuhänder sein.

2. Aufgrund der unterschiedlichen Ausgestaltungsmöglichkeiten kommen verschiedene Datentreuhandmodelle zur Lösung verschiedener Probleme in Betracht. Regulierung sollte von diesen bestehenden Problemen ausgehend einen funktionierenden Rechtsrahmen für die jeweils zur Problemlösung erforderlichen Datentreuhänder schaffen.

3. Die Datentreuhand kann dabei aber stets nur ein Element einer solchen Problemlösung sein. Weitere Lösungskomponenten müssen hinzutreten. Erforderlich ist im Mindesten ein Dreiklang aus Datentreuhand, Datenzugang und Interoperabilität.

Datentreuhänder im Onlinesektor

4. Im Onlinesektor existiert ein erhebliches Problem der Übernutzung personenbezogener Daten. Dieses Problem ist auf eine Informationsüberlastung, ein datenschutzrechtliches Durchsetzungsdefizit sowie für die Interaktion mit großen Onlineplattformen auf ein wettbewerbliches Problem zurückzuführen.

5. Zur Lösung des Problems der Übernutzung personenbezogener Daten im Onlinesektor können Personal Information Management Systems (PIMS) erheblich beitragen. Hierfür bedarf es eines funktionierenden Rechtsrahmens, der die Chancen und Risiken der PIMS-Nutzung gleichermaßen in Betracht zieht.

6. Die fehlende Funktionsfähigkeit von PIMS ist nicht auf ein fehlendes Vertrauen zurückzuführen, sondern auf einen ungenügenden Nutzen. Um diesen Nutzen herzustellen, ist eine Regulierung auf Systemebene erforderlich, das heißt es bedarf zwingend der Pflicht zur Berücksichtigung der PIMS-Vorgaben für Datenverarbeiter sowie Interoperabilitätsvorgaben. Darüber hinaus sind Feinjustierungen im Rechtsrahmen sowie Maßnahmen zur Risikominimierung erforderlich.

7. Diese Feinjustierungen betreffen vor allem

- die Möglichkeit, die datenschutzrechtliche Einwilligung für Betroffene erklären zu können;
- die Möglichkeit, datenschutzrechtliche Befugnisse durch Dritte ausüben zu können;
- breitere Einwilligungsmöglichkeiten gegenüber PIMS;
- Interkonnektivitätsverpflichtungen großer Onlineplattformen.

8. Es bedarf einer gesetzgeberischen Entscheidung über Finanzierung und Organisation von PIMS. Sollen PIMS auch durch Private angeboten werden dürfen, müssen sie wirtschaftlich arbeiten können. Um eine falsche Anreizsetzung zu vermeiden, sollten sie aber, erstens, nicht Daten, sondern allein Services monetarisieren. Zweitens, sollten sie nicht von den Datenverarbeitern bezahlt werden dürfen, sondern von den Nutzerinnen und Nutzern finanziert werden müssen. Um zu vermeiden, dass eine Inanspruchnahme von PIMS und damit ein wirksamer Daten- und Verbraucherschutz einkommensabhängig ist, sollte über Subventionsmodelle nachgedacht werden.

9. Der Data Governance Act und auch § 26 TTDSG treffen keine Entscheidungen auf Systemebene, sondern dienen lediglich der Minimierung der Risiken bei der Nutzung von PIMS. Sie tragen daher zur Problemlösung wenig bei.

Datentreuhänder im Gesundheitssektor

10. Im Gesundheitssektor besteht hingegen das Problem einer Unternutzung von Daten für Forschungszwecke. Das ist einerseits auf eine schwierige Auffindbarkeit der erforderlichen Daten zurückzuführen, die in zahlreichen Registern verteilt liegen, und andererseits auf datenschutzrechtliche Unsicherheit bei der Zusammenführung und Auswertung großer Datenbestände.

11. Zur Lösung dieser Probleme bedarf es eines Dreiklangs aus Koordinationsstelle, Datenspendetreuhand und flexiblen Datenteilungstreuhändern.

12. Die Koordinationsstelle, die idealerweise sowohl auf nationaler Ebene für nationale Forschungsprojekte sowie auf europäischer Ebene für grenzüberschreitende Forschungsprojekte etabliert wird, weiß mittels Dokumentenreferenzregistern, in welchen Registern welche Daten liegen und steht dem Forscher als Ansprechpartnerin zur Verfügung.

13. Die Datenspendemöglichkeiten existieren de lege lata bereits über die Strukturen des Forschungsdatenzentrums und die ePA. Diese Möglichkeiten sollten ausgebaut und um Anreize für die Datenspende ergänzt werden, zum Beispiel der Kontaktmöglichkeit der spendenden Patientinnen und Patienten für den Fall neuer Forschungserkenntnisse.

14. In Registern gespeicherte Daten beziehen sich regelmäßig auf nur bestimmte Daten, zum Beispiel Daten der Sozialversicherung oder Daten bestimmter Krankheitsbilder. Es bedarf daher ergänzender flexibler Datentreuhandstrukturen mit höchsten Sicherheitsstandards, in denen Daten rechtssicher zusammengeführt und zu Zwecken der Forschung im Gemeinwohlinteresse ausgewertet werden können. Diese Datentreuhandlösungen könnten sowohl staatlicherseits als auch privatwirtschaftlich angeboten werden.

15. Zur Lösung des Problems der Unternutzung von Daten im Gesundheitssektor könnte der EHDS erheblich beitragen, indem er die horizontalen Regelungen des DGA-E sinnvoll ergänzt.

Datentreuhänder im Mobilitätssektor

16. Datentreuhandlösungen können ein geeignetes Instrument für Datenzugangsprobleme in Bezug auf Mobilitätsdaten sein. Diese Studie konzentriert sich auf die zukünftig stark wachsenden Datenmengen, die in vernetzten Fahrzeugen durch die Autonutzerinnen und -nutzer generiert werden und von vielen Unternehmen und für Zwecke des öffentlichen Interesses (Verkehrssicherheit, Umwelt et cetera) genutzt werden können. Auch für diese Daten besteht die Gefahr einer Unternutzung.

17. Es gibt seit Jahren eine intensive Auseinandersetzung um das sogenannte „Extended Vehicle"-Konzept der Autohersteller, mit dem sie die exklusive Kontrolle über diese Daten und über den technischen Zugang zum Fahrzeug ausüben können und damit den Zugang zu dem Ökosystem vernetzten und automatisierten Fahrens kontrollieren (Gatekeeper-Position). Das daraus zu erwartende massive Wettbewerbsproblem auf den Sekundärmärkten (Reparatur, Wartung, Navigation et cetera) mit negativen Auswirkungen auf Innovation und die Wahlfreiheit von Autonutzerinnen und -nutzern ist von der EU-Kommission als zu lösendes Problem anerkannt worden, allerdings hat sie bisher keinen Lösungsvorschlag vorgelegt.

18. Eine Datentreuhand, die diese in den Fahrzeugen generierten Daten unter ihrer Kontrolle hat und sie als „neutrale Instanz" nach gesetzlichen Vorgaben und Prinzipien den Stakeholdern dieses Ökosystems, der Datenwirtschaft sowie öffentlichen Institutionen und der Wissenschaft für Gemeinwohlzwecke zugänglich macht, wäre eine Lösungsoption, um präventiv die Gatekeeper-Position der Autohersteller nicht entstehen zu lassen und damit Wettbewerb, Innovationen und die Wahlfreiheit der Autonutzerinnen und -nutzer zu sichern. Mit einer Datentreuhand könnte zudem eine wesentlich bessere Nutzung dieser großen Menge von Mobilitätsdaten erreicht werden (Daten als Infrastruktur), als bei einer monopolistischen Kontrolle durch die Autohersteller.

19. Alternative Lösungen im Mobilitätssektor sind die strikte Regulierung eines FRAND-Zugangs in Bezug auf die (unter der Kontrolle der Autohersteller stehenden) Daten des vernetzten Autos. Dies könnte durch eine Weiterentwicklung des bereits bestehenden Zugangsregimes für Reparatur- und Wartungsinformationen in der Kfz-Typenzulassungsverordnung geschehen. Notwendig ist (ebenso wie bei der Datentreuhand) aber auch eine FRAND-Regelung bezüglich des technischen (Remote-)Zugangs zum Fahrzeug, um die Erbringung komplementärer Dienstleistungen zu ermöglichen (Lösung des Interoperabilitätsproblems).

Die Einführung einer „On-Board Application"-Plattform als alternative technische Lösung, die durch eine standardisierte offene und interoperable Telematiklösung die Möglichkeit eröffnet, dass die Autonutzerinnen und -nutzer selbst die Kontrolle über die von ihnen im Fahrzeug generierten Daten ausüben und anderen Serviceanbietern den Zugang zum vernetzten Fahrzeug ermöglichen können. Dies würde die Gatekeeper-Position der Autohersteller beseitigen.

Umfassende Sicherheitsstandards (mit Zertifizierungen) sind notwendig bei allen Lösungsoptionen.

20. Die Lösung dieses Gatekeeper-Problems ist notwendig und überfällig. Mittel- und langfristig sollte in jedem Fall eine Lösung über eine standardisierte „On-Board Application"-Plattform angestrebt werden. Kurzfristig wäre zunächst eine Reform der Kfz-Typenzulassungsverordnung mit einer strikten (auch innovationsorientierten) FRAND-Regulierung für den Zugang zu Daten und die Lösung des Interoperabilitätsproblems zu empfehlen.

21. Die bisher konkret wenig diskutierte Datentreuhandlösung sollte dringend auf ihre Vorteile und Probleme geprüft werden. Wir sind der Meinung, dass eine Datentreuhandlösung über die Lösung dieses Wettbewerbsproblems hinaus weitere spannende Perspektiven für eine effiziente und an Gemeinwohlzielen orientierte Nutzung dieser zukünftig sehr großen Mengen von Mobilitätsdaten eröffnet.

Datentreuhänder und Datenmittler sind wichtige Hilfsmittel einer europäischen Datenwirtschaft, die ihre Potenziale zu unser aller Gunsten nur entfalten können, wenn ihnen rechtlich dazu die Möglichkeit gegeben wird. Die Untersuchung zeigt, dass die jeweils in Betracht kommenden Datentreuhandmodelle modellspezifisch ausgestaltet sein müssen und daher auch jeweils eines völlig unterschiedlichen Rechtsrahmens bedürfen, um tatsächlich zur Problemlösung beitragen zu können.

In der Studie werden verschiedene Probleme in drei Sektoren – Gesundheits-, Online- und Mobilitätssektor analysiert, die unter Einbeziehung von Datentreuhändern gelöst werden können.

Konrad-Adenauer-Stiftung e. V.