

Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive



Institutionen und Autoren, die an der Studie mitgewirkt haben:

Partnerschaft Deutschland: Philipp Denker; Dr. Dirk Graudenz (extern); Laura Schiff; Dr. Sönke E. Schulz

Lorenz-von-Stein-Institut für Verwaltungswissenschaften an der Christian-Albrechts-Universität zu Kiel:
Dr. Christian Hoffmann; Johanna Jöns; Dr. Florian Jotzo (extern)

Universität Kassel: Thilo Goeble; Prof. Dr. Gerrit Hornung, LL.M.

Fraunhofer FOKUS: Florian Friederici; Rafael Grote; Dr. Ilja Radusch



Management Summary

Digitalisierung ist die zentrale Kraft, die im wirtschaftlichen, politischen und gesellschaftlichen Bereich für Umbrüche sorgt und auch die Zukunft wesentlich prägen wird. Diese Entwicklung erfasst mittlerweile auch den Mobilitätsbereich. Die durch die Digitalisierung des Automobils und den hohen Grad der Vernetzung anfallenden Datenmengen ermöglichen neue Formen der Mobilität und leisten einen wesentlichen Beitrag zur Wertschöpfung. So wird der deutsche Markt für Mobilitätsdaten derzeit auf einen zweistelligen Milliarden-Euro-Betrag geschätzt¹. Obwohl es nicht an Ideen für die Entwicklung neuer Geschäftsmodelle mangelt, wird die Erschließung dieses Potenzials momentan dadurch erschwert, dass eine „Eigentumsordnung“ hinsichtlich der im Kontext von Mobilitätsanwendungen erstellten, übermittelten und genutzten Daten fehlt.

Kennzeichnend für den Status quo sind stattdessen die Heterogenität und Fragmentierung datenbezogener Regelungen – vor allem im Verfassungs-, Datenschutz-, Urheber-, Straf- und Lauterkeitsrecht. Datennutzung und -verwertung werden nicht durch entsprechende rechtlich verankerte Befugnisse, sondern vor allem durch faktische Zugriffsmöglichkeiten bestimmt. Gleichzeitig herrscht ein Mangel an Transparenz hinsichtlich der Erhebung und Verarbeitung von Daten. Kennzeichnend sind Rechtsunsicherheit bezüglich der Datennutzung und starke Abhängigkeiten der Nutzer von Mobilitätsdienstleistungen mit „Alles-oder-Nichts-Regelungen“ im Rahmen der Allgemeinen Geschäftsbedingungen. Die Nutzer können somit de facto oft weder an der Nutzung ihrer Daten wirtschaftlich partizipieren noch die Datenfreigabe granular steuern. Obwohl die Frage nach Möglichkeiten der wirtschaftlichen Nutzung zunehmend an Relevanz gewinnt, gibt es *de lege lata* keine Zuweisung eines eigentumsähnlichen Ausschließlichkeitsrechts, welches es dem „Eigentümer“ erlaubt, „seine Daten“ wirtschaftlich souverän zu nutzen und andere von einer solchen Nutzung auszuschließen.

Das ökonomische Potenzial von Mobilitätsdaten kann vor diesem Hintergrund nicht optimal im besten Interesse aller Beteiligten ausgeschöpft werden. In Anbetracht der fortschreitenden Nutzung vor allem personenbezogener Daten für datenbasierte Geschäftsmodelle mehrten sich auf Verbraucherseite zudem Bedenken über den adäquaten Schutz von Privatheit. Da der Erfolg datenbasierter Geschäftsmodelle auf dem Vertrauen der Nutzer und deren Bereitschaft,

ihre Daten bereitzustellen, basiert, sind beide Aspekte eng miteinander verbunden.

In Anbetracht dieser mit der Digitalisierung im Mobilitätsbereich verbundenen Entwicklungen soll die Studie „Eigentumsordnung für Mobilitätsdaten?“ einen mobilitäts- und industriepolitischen Diskussionsbeitrag zur Klärung der Frage nach einem „Eigentum“ an Mobilitätsdaten als Basis für die Erschließung neuer Geschäftsmodelle leisten. Ziel soll dabei sein, eine Balance zwischen adäquatem Schutz von Privatheit und informationeller Selbstbestimmung auf der einen Seite sowie Innovations- und Investitionsförderung von datenbasierten Geschäftsmodellen auf der anderen Seite zu gewährleisten.

Aus ökonomischer Sicht sind die Realisierung von Datensouveränität im Sinne einer individuellen, aufgeklärten und damit souveränen Entscheidungsmöglichkeit sowie die Schaffung von Voraussetzungen für einen Markt für Daten die zentralen Elemente für die Etablierung von Daten als Wirtschaftsgut. Zur rechtlichen Sicherung einer solchen Datensouveränität kommen sowohl die Schaffung eines eigentumsähnlichen Ausschließlichkeitsrechts als auch andere Handlungsalternativen in Betracht. Letztere können bereichsspezifische Anpassungen, eine ausschließliche Fokussierung auf das Datenschutzrecht, die Etablierung spezifischer Nutzungsrechte und Nutzungslizenzen, die Stärkung des Integritätsschutzes und die Schaffung eines Open-Data-Systems betreffen. Sie können teilweise ergänzend oder zum Teil auch unabhängig von der Schaffung eines Ausschließlichkeitsrechts umgesetzt werden. Da ein eigentumsähnliches Ausschließlichkeitsrecht mit besonderen Herausforderungen – z. B. im Hinblick auf die zahlreichen Abhängigkeiten zu bereichsspezifischen Rechtsgebieten und die zum Schutz der Persönlichkeitsrechte notwendigen Belastungen – verbunden ist, steigen die Anforderungen, wenn dieser Weg beschritten wird.

Ohne damit eine endgültige Entscheidung für die Schaffung eines Ausschließlichkeitsrechts zu treffen, gilt es zu klären, wie ein solches Recht konkret umgesetzt werden könnte. Durch die Entwicklung eines eigenen Zuordnungsansatzes und eines Vorschlags, wie sich dieser gesetzlich abbilden ließe, leistet diese Untersuchung hierfür einen substanziellen Beitrag.

Der entwickelte Ansatz ordnet die Daten auf Basis von konkreten Indizien dem wirtschaftlich Berechtigten, d. h.

1 Eine im Rahmen der hier vorgelegten Studie durchgeführte sehr grobe Abschätzung hat ergeben, dass der Wert der Mobilitätsdaten eines privaten Fahrzeugnutzers in Deutschland (Positionsdaten sowie Fahrzeugdaten) in der Größenordnung von ca. 350 EUR/Jahr liegen könnte. Multipliziert mit der Anzahl der privaten Kraftfahrzeuge in Deutschland zeigt dies, dass es sich um einen Markt von der Größe eines zwei-stelligen Milliarden-Euro-Betrags handelt.

demjenigen, der die wesentliche Investition in die Datenerstellung vornimmt, zu. Er ermöglicht damit nicht nur Rechtssicherheit, sondern korrespondiert auch mit den Ergebnissen der ökonomischen Analyse. Die Zuordnung erfolgt somit an denjenigen, als dessen „Verdienst“ die Erstellung des Datums anzusehen ist, da er unmittelbar oder mittelbar via Zahlung die Kosten für die Entwicklung, Produktion oder Unterhaltung der datengenerierenden Gegenstände trägt oder als Skribent die Datenerstellung bewirkt.

Vor dem Hintergrund der oben beschriebenen Herausforderungen bei der Schaffung eines Ausschließlichkeitsrechts an Daten sind grundsätzlich zwei Vorgehensweisen vorstellbar, um die rechtlichen Voraussetzungen für die Etablierung von Daten als Wirtschaftsgut voranzubringen:

Die erste Option wäre, dass in Gänze ein neues Datengesetz, welches die oben beschriebenen Fragen umfassend löst, angestoßen wird. Hierfür spricht, dass ein ambitionierter Erstaufschlag mehr politischen Impetus bewirken könnte, als ein sukzessives Projekt. Zu beachten ist jedoch, dass sich die Herausforderungen einer umfassenden Lösung als wesentlich komplexer darstellen als bei einem sukzessiven Vorgehen.

Alternativ wäre die zweite Option ein schrittweises Vorgehen, das aus einer Reihe verschiedener Maßnahmen besteht, an deren Ende dann ein Datengesetz stünde. Mit den Maßnahmen würden Schritt für Schritt die Erschließung weitergehender ökonomischer Potenziale und die Konsolidierung des Rechtsrahmens auf Basis einer Zuordnung zum wirtschaftlich Berechtigten verfolgt. Unabhängig von dem gewählten Umsetzungsansatz werden folgende Maßnahmen empfohlen:

- (1) **Gezielte Schließung bestehender Schutzlücken:** Durch die Schließung bestehender Schutzlücken können kurzfristig wichtige Verbesserungen erzielt werden. So erscheint insbesondere die Einführung einer Haftungsnorm zur Verbesserung des Integritätsschutzes von Daten, die nicht auf eigenen Datenträgern gespeichert sind, zielführend, um solche Daten vor fahrlässigen Beeinträchtigungen durch Dritte zu schützen. Da eine solche Maßnahme außerdem das Vertrauen von Unternehmen, künftig noch mehr Datenverarbeitungsvorgänge in die Cloud auszulagern, stärken würde, könnten weitergehende ökonomische Potenziale durch eine verstärkte Nachfrage nach und Investitionen in Cloud-Lösungen erschlossen werden.
- (2) **Förderung eines einheitlichen Marktes für Daten durch Standardisierung:** Um die Bereitschaft zur Datenweitergabe und damit einhergehende wirtschaftli-

che Nutzung zu fördern, ist die Schaffung von Transparenz im Markt zentral. Zu diesem Zweck sollte die Entwicklung eines einheitlichen „Daten-Ausweises“ vorangetrieben werden. Ein solcher „Daten-Ausweis“ sollte die Nutzer diverser Mobilitätsdienstleistungen z. B. über die Art der erhobenen Daten, die Häufigkeit bzw. den Anlass der Datenweitergabe und den bestehenden oder nicht bestehenden Personenbezug informieren. Konkrete Ausgestaltungs- und Umsetzungsmöglichkeiten sind dabei gemeinsam mit der Wirtschaft zu diskutieren. Ergänzend dazu sollten Standardlizenzen für bestimmte Datenkategorien entwickelt werden, um den Austausch von Daten und die Markterschließung zu vereinfachen. Die kooperative Erarbeitung von standardisierten Nutzungslizenzen stellt dabei einen wichtigen ersten Schritt dar.

- (3) **Abbau von Schranken für *Data-Mining* und *Big-Data-Anwendungen*:** Um das wissenschaftliche und ökonomische Potenzial von *Data-Mining* und *Big-Data-Anwendungen* besser auszuschöpfen, sollten politische Initiativen unterstützt werden, die die Spielräume solcher Anwendungen erhöhen und mit berechtigten Schutzrechten Dritter zum Ausgleich bringen. Anknüpfungspunkte bieten derzeitige politische Initiativen auf EU-Ebene im Urheberrecht, die hinsichtlich ihrer Wirkungen und Zielsetzungen näher untersucht werden sollten.
- (4) **Förderung von *Open Data*:** Die öffentliche Bereitstellung von Daten durch staatliche Stellen, insbesondere aus dem *Car-2-Infrastructure*-Bereich, sollte vorangetrieben werden, um eine bessere Zweitverwertung zu ermöglichen. Konkrete Maßnahmen umfassen neben der Identifikation geeigneter Daten insbesondere die Schaffung der rechtlichen, technischen und organisatorischen Voraussetzungen für deren Bereitstellung, z. B. die Vereinheitlichung von Schnittstellen und die Schaffung eines Datenmarktplatzes. Bestehende Standards und Initiativen, wie bspw. die *mCloud* des Bundesministeriums für Verkehr und digitale Infrastruktur oder der Mobilitätsdatenmarktplatz der Bundesanstalt für Straßenwesen im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur, bieten Anknüpfungspunkte, auf denen aufgebaut werden kann. Im Bereich von *Private Open Data* hingegen ist ein Anreiz- und Förderungssystem anzustreben. Durch einheitliche Standards und rechtliche Marktbedingungen können die Voraussetzungen und Bedingungen für die freiwillige Zurverfügungstellung und Nutzung der Daten geschaffen werden. Damit sollte eine unentgeltliche Nutzung und insbesondere die Verarbeitung und Aggregation der Daten sichergestellt werden. Hierbei sind Lizenzierungsmodelle für *Private Open Data* denkbar,

wie diese heute schon bei *Open Source*, z. B. in Form der sog. Linux-Klausel, vorhanden sind.

- (5) **Förderung des Bewusstseins, dass Daten ein marktfähiges Gut sind:** Damit insbesondere Nutzer von Onlinediensten wirklich privatautonom über die Freigabe und Preisgabe ihrer Daten entscheiden können, muss ihnen der ökonomische Wert ihrer Daten als wirtschaftlich handelbares Gut stärker bewusst werden. Die EU-Datenschutz-Grundverordnung leistet – insbesondere durch das darin verankerte Koppelungsverbot – einen wertvollen Beitrag für die Entwicklung konkreter Maßnahmen. So könnten Anreizsysteme geschaffen werden, die Unternehmen dazu bewegen, alternative Bezahlungsmöglichkeiten anstelle von Daten für ihre Dienste anzubieten. Ergänzend könnten schulische und andere Bildungs- und Aufklärungsinitiativen einen wichtigen Beitrag dazu leisten, Daten als Wirtschaftsgut im Bewusstsein der Nutzer zu verankern.
- (6) **Konsolidierung bestehender datenbezogener Regelungen und Zusammenführung in einem Datengesetz:** Um Rechtssicherheit zu gewährleisten und die Ausschöpfung des ökonomischen Potenzials von Mobilitätsdaten, aber auch aller sonstigen Daten, im Sinne aller Marktteilnehmer zu ermöglichen, sollte eine Fragmentierung möglichst minimiert werden. In einem ersten Schritt erscheint ein Normenscreening zur Identifikation betroffener Regelungsbereiche und bestehender Konflikte zielführend. Ausgehend von den Ergebnissen des Normenscreenings könnte dann langfristig ein konsistenterer, rechtsgebietsübergreifender Rahmen für eine funktionierende Datenökonomie geschaffen werden (Datengesetz). Dieser Rahmen könnte die bereits erzielten Verbesserungen der verschiedenen rechtlichen Maßnahmen implementieren. Kernelemente eines solchen Datengesetzes wären die Verständigung auf einen einheitlichen Zuordnungsansatz – wie z. B. der neu entwickelte und dargestellte Zuordnungsansatz zum wirtschaftlich Berechtigten – sowie die Definition notwendiger Schrankenbedingungen, die Verbesserung des Integritätsschutzes und die Anpassung der schuldrechtlichen Regeln an die digitale Welt.

Inhaltsverzeichnis

Management Summary	3
Inhaltsverzeichnis	7
1 Einführung: Ausgangssituation und Grundlagen	11
1.1 Die Automobilbranche im Wandel zum Mobilitätsdienstleister	12
1.2 Dateneigentum als Grundlage für mobilitätsdatenbasierte Geschäftsmodelle	14
1.3 Ziele und Aufbau der Studie	14
2 Fallstudien „digitale Mobilität“	17
2.1 Fallstudie 1: Kfz-Instandhaltung und -Wartung	21
2.1.1 Technische Betrachtung	22
2.1.2 Ökonomische Betrachtung	23
2.2 Fallstudie 2: <i>Carsharing</i>	25
2.2.1 Technische Betrachtung	27
2.2.2 Ökonomische Betrachtung	28
2.3 Fallstudie 3: Mobilitätsdienstplattform	29
2.3.1 Technische Betrachtung	31
2.3.2 Ökonomische Betrachtung	32
2.4 Fallstudie 4: Mobilitätsdienste	32
2.4.1 Technische Betrachtung	33
2.4.2 Ökonomische Betrachtung	35
2.5 Fallstudie 5: <i>Car-2-Infrastructure</i> -Kommunikation	35
2.5.1 Technische Betrachtung	37
2.5.2 Ökonomische Betrachtung	38
2.6 Ergebnis: Fallstudien „digitale Mobilität“	39
3 Rechtliche Erfassung des „Dateneigentums“ im geltenden Recht (<i>de lege lata</i>)	41
3.1 Hintergrund: Verfassungsrechtlicher Schutz von Daten	43
3.2 Bereichsspezifische Zuordnung von Daten im (einfachen) geltenden Recht	46
3.2.1 Datenschutzrecht	46
3.2.2 Urheberrecht	50
3.2.2.1 Überblick	50
3.2.2.2 Anwendung auf die Fallstudien	51
3.2.2.3 Zwischenfazit zum Urheberrecht	54
3.2.3 Strafrecht	54
3.2.4 (Lauterkeitsrechtlicher) Schutz von Betriebs- und Geschäftsgeheimnissen	57
3.2.5 Allgemeines Zivilrecht	58
3.2.5.1 Daten als Eigentum i. S. d. § 903 BGB	58
3.2.5.2 Eigentumsschutz durch § 823 BGB	59
3.2.5.3 Sachgenerierte Daten als Früchte	59
3.2.5.4 Sachgenerierte Daten als Nutzungen	59
3.2.5.5 Zwischenfazit zum allgemeinen Zivilrecht	60
3.2.6 Fazit: Kein „Dateneigentum“ <i>de lege lata</i>	60
3.3 Faktische Herrschaft als Äquivalent zum rechtlichen Eigentum	61

4	Ökonomische Analyse: Etablierung von Daten als Wirtschaftsgut als Voraussetzung für eine hohe wirtschaftliche Gesamtwertschöpfung	65
4.1	Veränderte Kundenanforderungen als Treiber der Digitalisierung im Mobilitätsbereich	66
4.2	Implikationen für Fahrzeugnutzer, Automobilindustrie und den Staat	70
4.2.1	Konfliktfeld Convenience vs. Privatheit	70
4.2.2	Traditionelle Automobilindustrie im Wandel	71
4.2.3	Regulierung im ökonomischen Kontext	72
4.3	Daten als Wirtschaftsgut: Datensouveränität und Markt als Erfolgsfaktoren	73
4.3.1	Wünschenswerte Eigenschaften des Wirtschaftsguts Daten	78
4.3.2	Mechanismen für einen hohen Grad der Nachnutzung	79
4.3.3	Akteure mit Verfügungsgewalt	79
4.3.4	Trends und Entwicklungen bei datenbasierten Geschäftsmodellen	81
4.3.5	Public und Private Open Data	82
4.4	Ergebnis: Hohe wirtschaftliche Gesamtwertschöpfung durch Datensouveränität und Schaffung eines Marktes für Daten	83
5	Optionen zur Realisierung von Datensouveränität	85
5.1	Explizite – übergreifende – Zuordnung von Daten zu einem „Dateneigentümer“	86
5.1.1	Bestimmung des Dateneigentümers durch analoge Anwendung des geltenden Rechts	87
5.1.1.1	Analoge Anwendung des § 903 BGB	87
5.1.1.2	Anerkennung eines Rechts am eigenen Datenbestand	87
5.1.1.3	Anerkennung von Daten als Früchte der datengenerierenden Sache	88
5.1.1.4	Sachgenerierte Daten als Nutzungen	88
5.1.1.5	Zwischenergebnis	88
5.1.2	Neuentwicklung eines Ausschließlichkeitsrechts an Daten/eines Dateneigentums (de lege ferenda)	88
5.1.2.1	Merkmale eines Ausschließlichkeitsrechts	89
5.1.2.2	Historische Gründe für die Schaffung von Immaterialgüterrechten	89
5.1.2.3	Denkbare Ansätze für eine Zuordnung von „Dateneigentum“	90
5.1.2.3.1	Datenspezifische Ansätze	91
5.1.2.3.2	Gegenständliche (sachenrechtliche) Ansätze	96
5.1.2.3.3	Handlungsbezogene Ansätze	98
5.1.2.4	Abschließende Bewertung: Zuordnung zum wirtschaftlich Berechtigten als überzeugendste Handlungsoption	104
5.1.2.4.1	Anwendung des kombinierten Ansatzes auf die Fallstudien	105
5.1.2.4.2	Überführung des neuentwickelten Ansatzes in einen Normtext	107
5.1.3	Gründe für und gegen ein Ausschließlichkeitsrecht an Daten	109
5.2	Handlungsalternativen	110
5.2.1	Vollständiger Verzicht auf gesetzliche Änderungen	110
5.2.2	Bereichsspezifische Anpassungen, insbesondere Schaffung eines effektiven Vertragskontrollrechts	111
5.2.3	Ausschließliche Fokussierung auf das Datenschutzrecht	112
5.2.4	Spezifische Nutzungsrechte und Nutzungslizenzen	113
5.2.5	Schaffung eines verbesserten Integritätsschutzes von Daten	114
5.2.6	Schaffung eines Open-Data-Systems	116
5.2.7	Zwischenergebnis	118
6	Exkurs: Übertragbarkeit auf andere Gebiete: Beispiel Gesundheitsdaten	119

7 Handlungsempfehlungen	121
7.1 Gezielte Schließung von Schutzlücken	122
7.2 Förderung eines einheitlichen Markts für Daten durch Standardisierung	123
7.3 Abbau von Schranken für Data-Mining- und Big Data-Anwendungen	124
7.4 Public Open Data als Standard definieren und Private Open Data fördern	124
7.5 Förderung des Bewusstseins für die Einordnung von Daten als marktfähiges Gut	125
7.6 Konsolidierung datenbezogener Regelungen und Zusammenführung in einem „Datengesetz“	126
7.6.1 Festlegung eines Zuordnungsansatzes	126
7.6.2 Schaffung der nötigen Schrankenbestimmungen	127
7.6.3 Anpassung der schuldrechtlichen Regeln an die digitale Welt	127
7.6.4 Konkretisierung von AGB-Vorgaben (§§ 305 ff. BGB)	128
7.6.5 Anpassung der Verbraucherschutzvorschriften (§§ 312 ff. BGB: Informationspflichten, Widerrufsrechte)	128
7.6.6 Verbesserung des Integritätsschutzes von Daten durch Schaffung einer eigenen Rechtsgrundlage	129
7.7 Fazit und Auswirkungen der Handlungsempfehlungen auf die Fallstudien	129
Anhang	131
I. Tabellarische Übersicht der Fallstudienanalyse aus technischer Sicht	132
i. Fallstudie 1: Kfz-Instandhaltung und -Wartung	132
ii. Fallstudie 2: Carsharing	133
iii. Fallstudie 3: Mobilitätsdienstplattform	134
iv. Fallstudie 4: Mobilitätsdienste	135
v. Fallstudie 5: Car-2-Infrastructure-Kommunikation	136
II. Bereichsspezifische Zuordnung von Daten im geltenden Recht	137
i. Verfassungsrecht	137
ii. Datenschutzrecht	142
iii. Urheberrecht	147
iv. Strafrecht	152
v. (Lauterkeitsrechtlicher) Schutz von Betriebs- und Geschäftsgeheimnissen	157
vi. Allgemeines Zivilrecht	162
Abbildungsverzeichnis	167
Abkürzungsverzeichnis	168

1 Einführung: Ausgangssituation und Grundlagen

1.1 Die Automobilbranche im Wandel zum Mobilitätsdienstleister

Deutschland gilt als Land des Automobils. Deutsche Ingenieure haben das Auto erfunden, es immer wieder weiterentwickelt und maßgeblich zu dem beigetragen, was es heute ist. Dementsprechend bedeutend ist die **Automobilindustrie** für die deutsche Wirtschaft – nicht nur isoliert betrachtet, sondern vor allem aufgrund ihrer Verflechtungen mit anderen Branchen. Trotz mehrerer wirtschaftlicher Krisen im letzten Jahrhundert und einem allgemeinen Rückgang der verarbeitenden Industrie hat sie stetes Wachstum verzeichnet und trägt mit einem Jahresumsatz von 367,9 Mrd. EUR (2014) erheblich zur **Gesamtwertschöpfung** in Deutschland bei (ca. 12 % des BIP)². Auch zum Innovations- und Technologiestandort Deutschland leistet die deutsche Automobilindustrie einen bedeutenden Beitrag. Sie war maßgeblich an der raschen Abfolge technischer Innovationen, die die Geschichte des Automobils seit Ende des 19. Jahrhunderts prägten, beteiligt und ist auch heute noch die **forschungsstärkste Branche** des Landes sowie international in der **Weltspitze** angesiedelt³.

Ungeachtet der traditionell sehr starken Stellung der deutschen Automobilindustrie gibt es einige **Trends**, die die **Mobilitätsbranche** und deren Zukunft bereits heute entscheidend beeinflussen werden. Neben demografischen

Veränderungen, die zu veränderten Mobilitätsgewohnheiten führen, und dem Klimawandel, der eine Notwendigkeit von Effizienzsteigerungen, alternativen Antrieben und smarten Mobilitätslösungen bedingt, ist die **Digitalisierung** ein zentraler Trend, der **tiefgreifende Veränderungen** in der gesamten Branche und insbesondere in der Automobilindustrie herbeiführt (siehe Kapitel 4.1). Wo früher Neuerungen im klassischen Fahrzeugbau standen, wird **Innovation** in der Branche heute hauptsächlich durch **Entwicklungen im Softwarebereich** angetrieben.

Obwohl diese Entwicklung häufig als relativ neues Phänomen der letzten beiden Dekaden betrachtet wird, zeigt ein detaillierter Blick auf die Geschichte des Automobils, dass die Digitalisierung die Entwicklung des Automobils bereits **seit den späten 1960er Jahren** prägt und seitdem eine immer bedeutendere Rolle einnimmt. Ausgehend von der Motorkutsche und dem Patent-Motorwagen aus dem Jahre 1886, die als Vorläufer der Fahrzeuge von heute betrachtet werden können, fanden **sukzessive Datenverarbeitung und Vernetzung Einzug ins Automobil**. Mit Blick auf die Digitalisierung des Automobils wurden **mehrere Evolutionsstufen** identifiziert. Diese erstrecken sich von der erstmaligen Erstellung von Daten im Fahrzeug über die Vernetzung mittels Kabel und dem mobilen Internetzugang bis hin zur Vollvernetzung aller Fahrzeuge in der Zukunft (Abbildung 1).

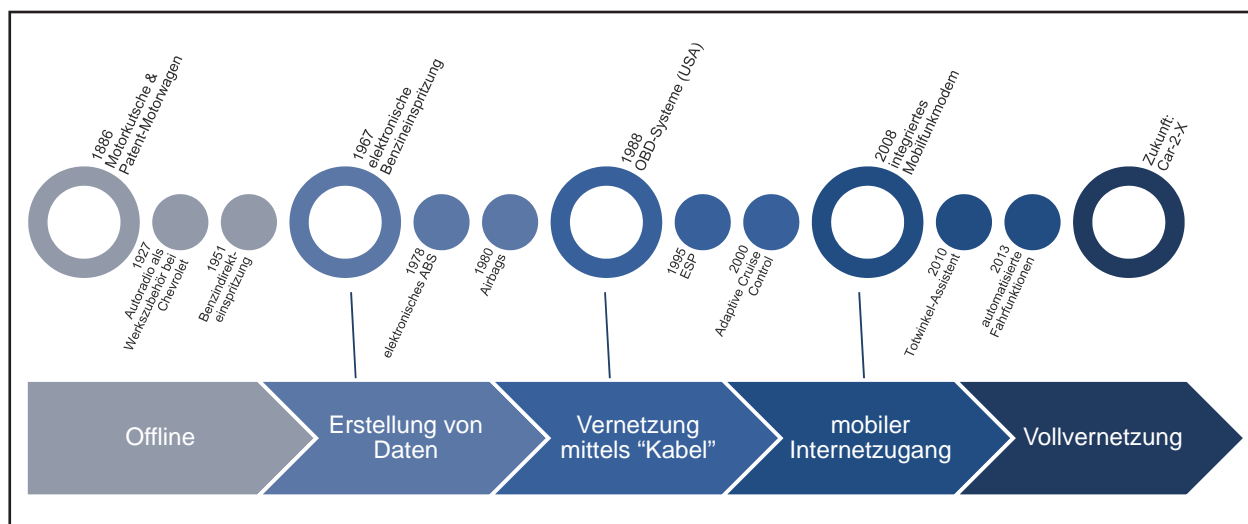


Abbildung 1: Historie der Digitalisierung im Fahrzeugbau

- 2 Statistisches Bundesamt, Fachserie 18, Reihe 1.4, Volkswirtschaftliche Gesamtrechnungen 2015; Statista, Bruttoinlandsprodukt in Deutschland in den Jahren 1960 bis 2016 (Bestand in 1.000), vgl. <http://de.statista.com/statistik/daten/studie/1251/umfrage/entwicklung-des-bruttoinlandsprodukts-seit-dem-jahr-1991>; VDA, 2015, Zahlen und Fakten, vgl. <https://www.vda.de/de/services/zahlen-und-daten/zahlen-und-daten-uebersicht.html>; Statista, Bruttoinlandsprodukt in Deutschland in den Jahren 1960 bis 2016 (Bestand in 1.000), vgl. <http://de.statista.com/statistik/daten/studie/1251/umfrage/entwicklung-des-bruttoinlandsprodukts-seit-dem-jahr-1991>.
- 3 VDA, 2015, Zahlen und Fakten, vgl. <https://www.vda.de/de/services/zahlen-und-daten/zahlen-und-daten-uebersicht.html>.

Bei der Erfindung des Automobils im Jahre 1886 handelte es sich noch um ein **nichtdigitales „Offline-Fahrzeug“**, bei dem keine Daten auf elektronischem Wege erstellt wurden. Bereits seit der Einführung von Autoradios zur Unterhaltung, jedoch im besonderen Maße in Verbindung mit der elektronischen Regelung und Steuerung, bildet **Elektronik** die Grundlage für viele Innovationen im Automobilbereich. Ein erstes Beispiel ist die seit 1967 eingeführte elektronische Benzineinspritzung, die einen Meilenstein der **Erstellung von Daten** im Fahrzeug kennzeichnet. Dabei wurden Daten zunächst nur lokal erstellt und – im Gegensatz zu heute – nicht außerhalb des Fahrzeuges genutzt⁴.

Nach der Einführung des elektronischen Antiblockiersystems (ABS) 1978 und von Airbags im Jahre 1980 stellte die Etablierung von On-Board-Diagnose-Systemen (OBD) 1988 in den USA einen wesentlichen Meilenstein dar⁵. Die **Vernetzung mittels „Kabel“** am genormten OBD-Stecker im Fahrzeug ermöglichte erstmals eine Datenübertragung (über die OBD-Schnittstelle) aus dem Fahrzeug hinaus, um Fehlercodes und Daten aus den verbauten Steuergeräten zu erhalten (z. B. zwecks Servicedurchführung in Werkstätten). Mittlerweile sind viele Geräte für die Schnittstelle nicht nur für Werkstätten, sondern für jedermann erhältlich. Die Daten können auf Smartphones visualisiert oder ins Internet übertragen werden und künftig die Basis für neue Geschäftsmodelle bilden.

Zur **Zugangs- und Nutzungskontrolle** entwickelte sich der Fahrzeugschlüssel vom rein mechanischen Schlüssel über die Integration von elektronischen Komponenten (Wegfahrsperre, Funköffner) bis hin zu Zugangskarten bzw. Zugang per Handy in Carsharing-Fahrzeugen. Während bei den rein mechanischen Schlüsseln keine Daten bei der Nutzung anfallen, so erfordern elektronische Komponenten wie Wegfahrsperren oder Funköffner bereits Datenkommunikation zwischen dem Schlüssel und dem Fahrzeugsystem (Fallstudie 2).

Im Bereich **Telekommunikationstechnik** ist die Entwicklung vom – zu Beginn analogen – Autotelefon über die mobile Datenübertragung mittels integrierten Mobilfunkmodems hin zur Vollvernetzung mit *Car-2-X*- bzw. *Car-2-Infrastructure*-Kommunikation in der Zukunft zu sehen. Dadurch stehen im Fahrzeug verschiedene Kommunikationswege zur Verfügung. Internetverbindungen über Mobilfunk ermöglichen Kommunikation mit entfernten Diensten wie z. B. Online-Wartungsdiensten des Fahrzeug-

herstellers (Fallstudie 1), Vermittlungsservern von *Carsharing*-Anbietern (Fallstudie 2) sowie beliebigen weiteren Mobilitätsdiensten (Fallstudien 3 und 4) und Verkehrsinformationsdiensten (Fallstudie 5). Unabhängig von Telekommunikationsinfrastruktur ermöglicht Ad-hoc-Kommunikation über WLAN (*Car-2-X*) den direkten Datenaustausch zwischen Fahrzeugen aber auch zu entsprechender Verkehrsinfrastruktur an der Straße (*Car-2-Infrastructure*, Fallstudie 5).

Die Digitalisierung im Bereich **Informationen und Unterhaltung** begann mit den ersten Autoradios und führte über Navigationssysteme hin zu Mobilitätsdienstplattformen (MDP, Fallstudie 3 und 4). Die im Vergleich zur Fahrzeugindustrie hohe Innovationsgeschwindigkeit der Informations- und Kommunikationstechnik führte lange Zeit dazu, dass Autoradios im Fahrzeug ausgetauscht bzw. aufgerüstet wurden oder dass Navigationsgeräte per Saugnapf an die Windschutzscheibe geheftet wurden. Die Möglichkeiten von MDP ermöglichen schon heute den Zugang für Anwendungen von Drittanbietern zu Fahrzeugsystemen – ein Trend, der sich in Zukunft verstärken wird.

Bezüglich der Einflüsse der Digitalisierung im Fahrzeugbau unterscheiden sich die Entwicklungen im letzten Jahrzehnt entscheidend von den technologischen Neuerungen, die bereits seit Mitte des 20. Jahrhunderts ein Treiber von Innovationen im Fahrzeugbau sind. Zentrale Merkmale sind neben der abnehmenden Bedeutung des Individualverkehrs insbesondere die **zunehmende Vernetzung unterschiedlicher Verkehrsträger und -mittel sowie die Vernetzung von Mobilitätsangeboten mit Mehrwertdiensten anderer Branchen**. Das Auto von heute ist nicht mehr nur Mittel zur Fortbewegung, sondern zugleich Quelle für Unterhaltung, Information und Mittel zur Kommunikation. Es kontrolliert sich selbst in Echtzeit, kommuniziert mit anderen Fahrzeugen und Infrastruktur und bietet eine Vielzahl von Dienstleistungen an. Diese reichen von Telefonie und Musik über Parkassistenten und Navigationshilfen bis hin zu autonomen Fahrfunktionalitäten. Diese Dienste und Funktionalitäten nehmen heute einen weitaus größeren Stellenwert ein als noch vor wenigen Jahren und werden **immer bedeutender im Vergleich zu traditionellen Qualitätsmerkmalen** (siehe Kapitel 4.1).

Der zentrale Unterschied zwischen den Fahrzeugen und Mobilitätsanwendungen von „gestern“ und „heute“ ist vor allem der **hohe Grad der Vernetzung**. Beim Betrieb des

4 Verband der Automobilindustrie, Zeitstrahl – Innovationen der letzten 130 Jahre, 2016: <https://www.vda.de/de/themen/innovation-und-technik/zeitstrahl/zeitstrahl-innovationen.html>.

5 Verband der Automobilindustrie, Zeitstrahl – Innovationen der letzten 130 Jahre, 2016: <https://www.vda.de/de/themen/innovation-und-technik/zeitstrahl/zeitstrahl-innovationen.html>.

Fahrzeugs entstehen **riesige Datenmengen**, die nicht mehr nur lokal verfügbar sind, sondern über moderne Kommunikationstechnik **für Dritte zugänglich** werden. Datengetriebene und insbesondere personendatengetriebene Anwendungen und Geschäftsmodelle sind auch im Mobilitätssektor von immer größerer Bedeutung.

Vor dem Hintergrund dieser Entwicklung stehen deutsche Unternehmen vor der Frage, wie sie sich angesichts der fortschreitenden Digitalisierung in der Mobilitätsbranche positionieren. Bereits heute zeichnet sich eine Entwicklung von reiner Fahrzeugproduktion hin zur Entwicklung von **integrierten Mobilitätslösungen** ab. Ein Großteil dieser Mobilitätslösungen basiert auf der **Sammlung, Analyse und Auswertung riesiger Datenmengen**.

1.2 Dateneigentum als Grundlage für mobilitätsdatenbasierte Geschäftsmodelle

Die Historie technologiegetriebener Innovationen im Fahrzeugbau zeigt, dass die Digitalisierung einen wesentlichen Beitrag zum Wachstum der Wertschöpfung bei der Fahrzeugentwicklung und -produktion ermöglicht hat. Heute sind es vor allem datenbasierte Mobilitätsanwendungen und -systeme, durch die **signifikante ökonomische Potenziale** erschlossen werden können. So gehen manche Schätzungen davon aus, dass sich das Marktpotenzial von vernetzten Diensten in und um das Automobil von ca. 32 Mrd. EUR in 2015 auf 115 Mrd. EUR in 2020 erhöhen wird (Weltmarkt)⁶. Viele der neuen Geschäftsmodelle basieren auf der Erstellung, Übermittlung und Nutzung von Daten, die einen Personenbezug aufweisen können, aber zum Teil auch anonymisiert einen Mehrwert bieten (siehe Kapitel 2 und 4).

Obwohl es nicht an Ideen für die Entwicklung neuer Geschäftsmodelle mangelt, wird die Erschließung des ökonomischen Potenzials von Mobilitätsdaten momentan dadurch erschwert, dass eine „**Eigentumsordnung**“ hinsichtlich der im Kontext von Mobilitätsanwendungen erstellten, übermittelten und genutzten Daten fehlt (siehe Kapitel 3). Gleichzeitig herrscht ein **Mangel an Transpa-**

renz bezüglich der Erhebung und Verarbeitung von Daten. Kennzeichnend sind **Rechtsunsicherheit** bezüglich der Verwertung von Mobilitätsdaten und starke Abhängigkeiten der Nutzer von Mobilitätsdienstleistungen mit „**Alles-oder-Nichts-Regelungen**“ im Rahmen der Allgemeinen Geschäftsbedingungen diverser Dienste. Das ökonomische Potenzial der Nutzung von Mobilitätsdaten kann vor diesem Hintergrund nicht optimal ausgeschöpft werden (siehe Kapitel 3.3).

Aufgrund des signifikanten ökonomischen Potenzials von technologiegestützten Mobilitätsanwendungen und -systemen eröffnet die Digitalisierung auf der einen Seite einen Zukunftsmarkt, auf dem Deutschland und deutsche Unternehmen angesichts ihrer langen Erfahrung und starken Stellung im Automobilsektor eine relevante Position einnehmen können. Auf der anderen Seite kann sie zu einer ebenso großen Herausforderung für all jene werden, die mit dem Tempo dieses Wandels nicht mithalten können. Diese Entwicklung ist insbesondere vor dem Hintergrund des **Eintretens neuer Marktspieler** zu sehen (siehe Kapitel 4.2). In Anbetracht der großen Bedeutung der Automobilindustrie für Wohlstand, Beschäftigung und Innovation in Deutschland hätte ein Bedeutungsverlust immense Auswirkungen auf der wirtschaftlichen Ebene.

1.3 Ziele und Aufbau der Studie

Vor diesem Hintergrund ist das Ziel dieser Studie, einen industriepolitischen Diskussionsbeitrag zur Klärung der Frage nach einem **Eigentum an Mobilitätsdaten** als Basis für die **Erschließung neuer technologiegetriebener Geschäftsmodelle** zu erbringen. Dieser Beitrag leitet sich von abstrakten Überlegungen ab, die auf Basis von konkreten Anwendungsbeispielen entwickelt wurden, und orientiert sich folglich am technologischen Möglichkeitenraum. Darüber hinaus spielt insbesondere die Integration von rechtlichen Betrachtungen sowie wirtschaftlichen Konsequenzen und Möglichkeiten eine zentrale Rolle.

Im Rahmen dieser Studie werden in **Kapitel 2** zunächst anhand von **fünf Fallstudien** verschiedene Einsatzmöglichkeiten und Anwendungsszenarien für Datenerstellung im Mobilitätskontext beschrieben. Neben einer detaillierten

6 PwC, Racing Ahead. The Connected c@r 2014 study, 2014; Die Schätzung beruht auf einer im Jahr 2014 durchgeführten Studie von Strategy&, PwC und dem Center of Automotive Management. Die Studie basiert auf einer Analyse der Produktportfolios führender Automobilhersteller und Zulieferer sowie Entwicklungen im Bereich Forschung und Entwicklung. Die Schätzung umfasst mehrere Bereiche wie u. a. Entertainment, sicherheitsrelevante Anwendungen, autonomes Fahren oder Mobilitätsmanagement. Basierend auf den Berechnungen wird erwartet, dass der Löwenanteil des geschätzten Marktes auf sicherheitsrelevante Anwendungen (ca. 47 %) und autonome Fahrfunktionalitäten (ca. 36 %) anfällt (PWC, 2014). Das Thema Quantifizierung und Schwierigkeiten diesbezüglich wird in Kapitel 4.3 aufgegriffen.

Analyse der verschiedenen Datenerstellungs-, Datenübermittlungs- und Datennutzungsvorgänge und technischen Zugriffsmöglichkeiten verschiedener Akteure werden auch ökonomische Interessen und Wertschöpfungspotenziale untersucht.

Anhand der skizzierten datenbezogenen Vorgänge werden in **Kapitel 3** die **rechtlichen Rahmenbedingungen** (*de lege lata*) für die Erstellung, Übermittlung und Nutzung von Daten im Mobilitätskontext erfasst. Analysiert wird dabei zunächst, in welchen Rechtsgebieten bereits bereichsspezifische Zuordnungen von Daten zu finden sind. Der Begriff „**Dateneigentum**“ wird im Rahmen dieser Studie zunächst beschreibend für eine rechtliche Zuordnung zu einem Verfügungsberechtigten verwendet. Dies kann gerade auch eine bereichsspezifische Zuordnung sein, die weit hinter der Vorstellung von „Eigentum“ zurückbleibt. Der Begriff wird zudem angesichts seiner Verwendung im Rahmen des öffentlichen Diskurses und der Analysen in der juristischen Fachöffentlichkeit ebenfalls zur Problembeschreibung verwendet. Ob eine Verfügungsberechtigung im Sinne eines Ausschließlichkeitsrechts existiert oder in Anlehnung an das Sacheigentum, an das Urheberrecht oder andere Immaterialgüterrechte, oder als Leistungsschutzrecht, ausgestaltet ist bzw. werden sollte, ist davon zunächst zu trennen. Abschließend erfolgt eine Analyse der faktischen Herrschaft über Daten in der bestehenden Praxis.

In **Kapitel 4** folgt eine **ökonomische Betrachtung** der notwendigen Voraussetzungen für eine möglichst hohe Gesamtwertschöpfung durch die wirtschaftliche Nutzung von Mobilitätsdaten. Grundlage ist eine Analyse der Auswirkungen der Digitalisierung im Mobilitätssektor und ein Austarieren berechtigter Interessen verschiedener Akteurs-

gruppen. Die in diesem Kapitel vorgelegte Analyse hat zum Ziel, Anforderungen aus ökonomischer Sicht zu formulieren, um aus rechtlicher Sicht Lösungsoptionen für eine Regelung von Dateneigentum entwickeln und bewerten zu können. Bei der Erarbeitung eines möglichen Lösungsansatzes aus ökonomischer Perspektive stehen die Schaffung eines Marktes für Mobilitätsdaten sowie die Datensouveränität im Sinne einer Verfügungsgewalt des wirtschaftlich verantwortlichen Akteurs im Vordergrund. Diese Strukturelemente bilden die Basis für eine weitergehende rechtliche Betrachtung.

Ausgehend von den vorangegangenen Ausführungen werden in **Kapitel 5** mögliche **rechtliche Optionen** für die Realisierung von Datensouveränität betrachtet. Im Mittelpunkt stehen die Schaffung und konkrete Ausgestaltung eines eigentumsähnlichen Ausschließlichkeitsrechts für Daten, insbesondere die Entwicklung eines möglichen Zuordnungsansatzes unter Berücksichtigung rechtlicher und ökonomischer Aspekte. Darüber hinaus werden mögliche Handlungsalternativen zur Schaffung eines Ausschließlichkeitsrechts detailliert.

In **Kapitel 6** erfolgt ein Exkurs, in dem die **Übertragbarkeit** des am Beispiel „Mobilitätsdaten“ entwickelten Ansatzes für die Zuordnung eines eigentumsähnlichen Rechts am Datum für andere Bereiche geprüft wird. Exemplarisch dient hierzu das Beispiel „Gesundheitsdaten“.

Die aus den rechtlichen und ökonomischen Analysen gewonnenen Erkenntnisse legen die Basis für die **politisch-strategischen Handlungsempfehlungen** zur Verbesserung bzw. Klärung der Rahmenbedingungen für digitale Mobilitätsdienstleistungen in **Kapitel 7**.

2 Fallstudien „digitale Mobilität“

Die Geschichte der Digitalisierung im Mobilitätssektor und die damit verbundenen sozioökonomischen Entwicklungen unterstreichen die Bedeutung der Frage nach dem Eigentum der generierten Daten. Die Klärung dieser Frage unter Berücksichtigung sowohl rechtlicher als auch ökonomischer Gesichtspunkte bedarf einer Betrachtung von typischen Anwendungsfällen des Einsatzes von Informations- und Kommunikationstechnik im Mobilitätssektor aus technischer Perspektive.

Anhand von fünf Fallstudien in den Bereichen

- **Kfz-Instandhaltung und -Wartung** (Fallstudie 1),
- **Carsharing** (Fallstudie 2),
- **Mobilitätsdienstplattform** (Fallstudie 3),
- **Mobilitätsdienste** (Fallstudie 4) und
- **Car-2-Infrastructure-Kommunikation** (Fallstudie 5)

werden typische Anwendungsfälle beschrieben und die relevanten Datenerhebungs-, Datenübermittlungs- und Datennutzungsvorgänge herausgearbeitet. Die Fallstudienbeschreibung folgt einem einheitlichen Muster. Jede Fallstudie wird durch eine Beschreibung des Kontexts des jeweiligen Anwendungsfalles eingeleitet. In einem ersten Schritt werden die relevanten technischen datenbezogenen Vorgänge anhand eines lebensnahen Sachverhaltes beschrieben. Dabei werden sowohl die anfallenden Daten identifiziert und kategorisiert als auch die beteiligten Akteure unter Berücksichtigung technischer Zugriffsmöglichkeiten herausgearbeitet⁷. Während verschiedene Implementierungsformen der jeweiligen Fallstudie in der Beschreibung adressiert werden, erfolgt die Herausarbeitung der datenbezogenen Vorgänge auf Basis der von den Autoren als wahrscheinlich angenommenen Implementierung.

Um die Entwicklung mobilitätsdatengetriebener Geschäftsmodelle in verschiedenen Mobilitätskontexten zu illustrieren, wird in einem zweiten Schritt für jede Fallstudie ein Wertschöpfungsnetzwerk skizziert. Dabei werden Interessen und Nutzen bzw. Wertschöpfungspotenziale der einzelnen Akteure herausgearbeitet. An geeigneten Stellen wird die Story in einzelnen Fallstudien um einen Akteur erweitert, um den Möglichkeitenraum potenzieller Geschäftsmodelle aufzuzeigen⁸.

Bei der Beschreibung der Fallstudien wurde die Grundannahme getroffen, nur den Positiv-Fall zu betrachten. Das bedeutet, dass für alle Betrachtungen davon ausgegangen wird, dass die Sicherheits- und Schutzmaßnahmen, die gegen missbräuchliche Nutzung getroffen wurden, intakt sind.

Akteure und Datenkategorien

Die Komplexität der Fallstudien im Hinblick auf die beteiligten Akteure und deren Datenzugriffsmöglichkeiten steigert sich von Fallstudie zu Fallstudie (Abbildung 2). Der Fahrer als Hauptnutzer eines Fahrzeugs ist zentraler Akteur in allen Fallstudien. Ihm gegenüber steht jeweils ein weiterer Hauptakteur, der für die Fallstudie besonders relevant ist. Zusätzlich gibt es weitere Akteure, deren Datenzugriff für die Fallstudie nachrangig von Bedeutung ist.

Fallstudie 1 stellt im Hinblick auf die Anzahl der beteiligten Akteure folglich den einfachsten Fall dar. In Fallstudie 2 wird die Komplexität gesteigert, indem die Rollen Fahrer und Eigentümer getrennt werden. In den Fallstudien 3 bis 5 treten analog zum Carsharing-Anbieter der Mobilitätsdienstplattformanbieter, der Mobilitätsdiensteanbieter sowie der Infrastrukturbetreiber als zusätzliche Akteure auf.

⁷ Eine tabellarische Übersicht aller fünf Fallstudien ist Anhang I zu entnehmen.

⁸ Zu beachten ist, dass sich die Analyse der Nutzen- und Wertschöpfungspotenziale auf solche konzentrieren, die durch die Verwertung von Mobilitätsdaten entstehen, nicht auf sonstige, ggf. dem eigentlichen Geschäftsmodell entstammenden Einnahmequellen der jeweiligen Akteure.

Fallstudien	Akteure ⁹						
	Fahrer	Hersteller	Carsharing-Anbieter	Mobilitätsdienste-plattform	Mobilitätsdienst	Infrastruktur-betreiber	Weitere Akteure ¹⁰
1. Kfz-Instandhaltung und -Wartung	X	X					Werkstatt, Zulieferer
2. Carsharing	X	X	X				Vertragstankstelle
3. Mobilitätsdienste-plattform	X	X		X			Wetterdienst
4. Mobilitätsdienste	X	X		X	X		Parkplatz-Vermittlungsportal
5. Car-2-Infrastructure Kommunikation	X	X				X	Verkehrszentrale, Open Data Plattform

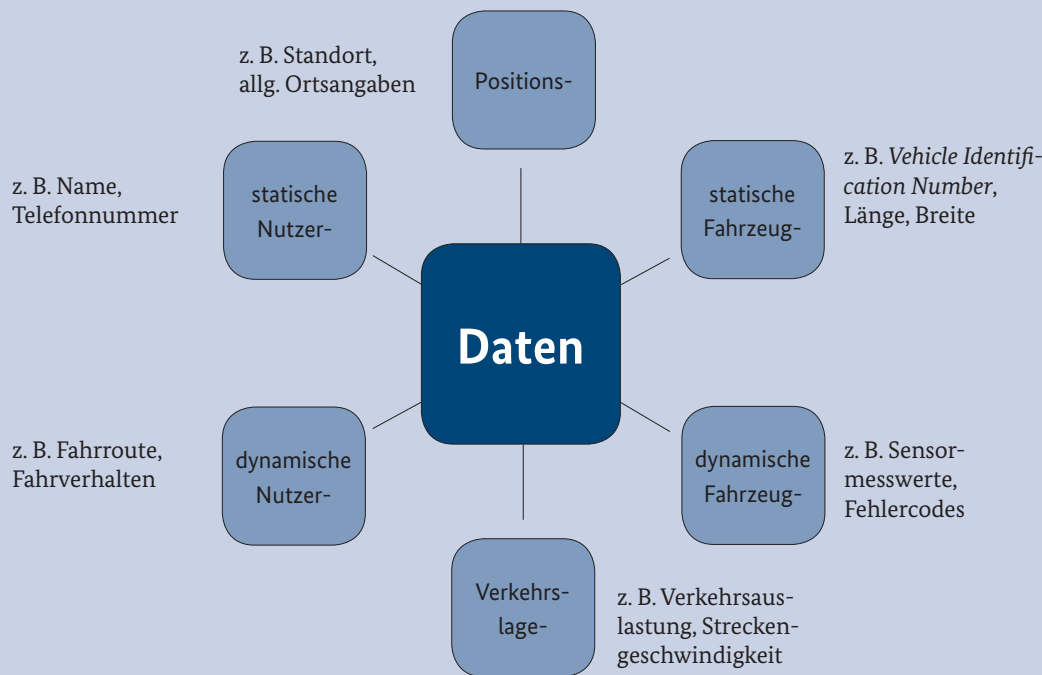
Abbildung 2: Akteursübersicht der fünf Fallstudien

Die in den verschiedenen Mobilitätskontexten anfallenden Daten selbst wurden für diese Studie in sechs Kategorien untergegliedert. Obwohl in jeder Fallstudie Daten verschiedener Kategorien anfallen, steht in jeder Fallstudie

eine Kategorie besonders im Vordergrund:¹¹ **Statische wie dynamische Fahrzeugdaten, Verkehrslagedaten, statische wie dynamische Nutzerdaten und Positionsdaten** (Abbildung 3):

-
- 9 In allen Fallstudien tritt auf technischer Ebene der Telekommunikationsanbieter hinzu, welcher die Datenübertragung abwickelt. Aufgrund dessen mangelnder Relevanz für die Frage der Klärung des Dateneigentums findet dieser in der Betrachtung keine explizite Erwähnung.
- 10 Weitere Akteure sind sowohl solche, deren Datenzugriff nicht im Fokus der Fallstudie steht, als auch solche, die in einem möglichen Erweiterungsszenario Teil des Wertschöpfungsnetzwerks der jeweiligen Fallstudie sind.
- 11 Es handelt sich hierbei um eine technische Klassifizierung, welche ausdrücklich von einer Einteilung in personenbezogene bzw. -beziehbare Daten im juristischen Sinne zu unterscheiden ist.

Kategorisierung von Mobilitätsdaten¹²:



Statische Fahrzeugdaten sind nichtveränderliche Informationen zum Fahrzeug, wie z. B. die *Vehicle Identification Number* (VIN) oder die Fahrzeugabmessungen. Diese treten oft in Verbindung mit dynamischen Fahrzeugdaten auf und sind Hauptbestandteil der übertragenen Nachrichten in Fallstudie 5.

Dynamische Fahrzeugdaten sind die im Fahrzeug anfallenden Sensor- und Diagnoseergebnisdaten, z. B. Messwerte und Fehlercodes. Diese Gruppe von Daten steht im Fokus von Fallstudie 1.

Verkehrslagedaten sind eine Ansammlung von Daten über die Verkehrslage in einem bestimmten Bereich. Diese können je nach Detailgrad aus sehr präzisen Positions- und dynamische Nutzerdaten bestehen, die auf einzelne Fahrzeuge und ggf. deren Fahrer zurückgeführt werden können, oder nur sehr abstrakte Angaben über die Auslastung von Verkehrssegmenten enthalten. In Fallstudie 5 werden Daten gesammelt, um diese zu Verkehrslagedaten zu aggregieren.

Dynamische Nutzerdaten umfassen die konkreten Verhaltensdaten, die sich bei der Nutzung von Fahrzeugen ergeben, z. B. Start- und Zielposition (in Form von Positionsdaten) und Fahrverhalten, aber auch die Daten, die bei der Nutzung von Anwendungen im Automobil entstehen (z. B. im Infotainmentbereich). In Fallstudie 2 werden dynamische Nutzerdaten in Form von Start- und Zielposition erhoben und in Fallstudie 3 und 4 in Form von Anwendungsdaten von Mobilitätsdiensten.

Statische Nutzerdaten sind Daten, die einer bestimmten Person direkt zugeordnet werden können. Fallstudie 3 thematisiert statische Nutzerdaten in Form einer Kontaktliste, in Fallstudie 4 sind es die Zugangsdaten des Benutzers. Diese Einordnung entspricht nicht der Klassifizierung als „personenbezogene Daten“ im rechtlichen Sinne. Es ist zu beachten, dass auch andere der hier genannten Kategorien einen Personenbezug aufweisen können.

Positionsdaten sind Ortsangaben, wie z. B. der Standort eines Parkplatzes oder des Fahrzeuges. Positionsdaten werden hier wie folgt von dynamischen Nutzerdaten unterschieden: Dynamische Nutzerdaten sind die Daten, die durch das Verhalten bedingt entstehen und auch Ortsangaben enthalten können. In Fallstudie 4 werden für ortsbasierte Dienste Positionsdaten verwendet.

Abbildung 3: Kategorisierung von Mobilitätsdaten

¹² Die hier verwendete Kategorisierung hat keinen Alleinheitsanspruch und koexistiert mit anderen gängigen Kategorisierungen von Mobilitätsdaten in der Literatur.

Die Klassifizierung der Daten in die zuvor beschriebenen Kategorien ist unabhängig von der Einstufung ihres Personenbezugs im rechtlichen Sinne. Ein Personenbezug entsteht – abgesehen von statischen Nutzerdaten, welche *per se* einen Personenbezug aufweisen – erst durch die Verknüpfung der Daten zu anderen, personenbezogenen Daten oder durch die direkte Zuordnung zu einer Person. Umgekehrt können Daten anonymisiert oder pseudonymisiert werden, indem der Personenbezug entfernt oder durch die Verwendung eines Pseudonyms erschwert wird (z. B. Ersetzen des Namens durch eine Buchstaben- oder Zahlenkombination)¹³. Die Frage des Personenbezugs und die Bedeutung von Anonymisierung und Pseudonymisierung werden in Kapitel 3 vertieft.

2.1 Fallstudie 1: Kfz-Instandhaltung und -Wartung

Sensorik, die für die elektronische Regelung von Vorgängen im Fahrzeug erforderlich ist, ist in jedem Fahrzeug verbaut. Beispiele für erfasste Messwerte sind die Luftmenge und -zusammensetzung, Kraftstoffmenge, Temperaturen oder Drehzahlen. Auf Basis dieser Sensorwerte wurde bislang eine Offline-Diagnose im Fahrzeug durchgeführt, um Fehlerzustände durch Warnlampen zu signalisieren oder in einem Fehlerspeicher lokal vorzuhalten. Dieser wurde mithilfe eines Kabels oder Diagnosegeräts über die OBD-Schnittstelle im Fahrzeug von der Werkstatt ausgelesen.

OBD-Schnittstelle: Bei der OBD-Schnittstelle handelt es sich um eine standardisierte, technische Schnittstelle, um Daten von den Steuergeräten im Fahrzeug in der Werkstatt auszuwerten. Elektronische Steuergeräte sind eingebettete Systeme im Fahrzeug mit angeschlossenen Sensoren und Aktoren. Sensoren erfassen Daten, die Elektronik verarbeitet diese, um Steuerungs- oder Regelungsaufgaben zu erfüllen. Damit können z. B. ein geringerer Kraftstoffverbrauch oder eine verbesserte Fahrsicherheit erzielt werden.

Im SAE-Standard J 1979¹⁴ sind die On-Board Diagnostics Parameter-IDs (PID) standardisiert. Darüber hinaus können herstellerspezifische PIDs verwendet werden. Beispiele sind Motorkühlmitteltemperatur, Kraftstoffdruck, Motordrehzahl, Fahrzeuggeschwindigkeit, Lufttemperatur, Tankfüllstand, Kraftstofftyp, Öltemperatur und die *Vehicle Identification Number* (VIN).

Mittlerweile bieten viele Automobilhersteller eine Online-Diagnose des Fahrzeugs als zusätzliche Dienstleistung an. Bei Einwilligung in die Nutzung des Dienstes stimmt der Fahrzeugnutzer im Rahmen der Nutzungsbedingungen der Erhebung der für die Online-Diagnose benötigten Daten und – je nach Gestaltung der Nutzungsbedingungen – deren weiteren Verwertung zu. Die neuen Online-Diagnoseverfahren ermöglichen die zentrale und unmittelbare Auswertung von Sensordaten durch den Hersteller. Möglich wird dies durch das lokale Erfassen von Sensordaten und Diagnoseergebnissen und den anschließenden Transfer per Mobilfunk zum Hersteller. Dem Hersteller ist der Fahrzeugzustand somit jederzeit und ohne Werkstattbesuch bekannt. Damit soll die Fahrzeugwartung, z. B. durch die individuelle Planung von Serviceterminen anhand des Fahrzeugzustandes, optimiert werden. Auch können mögliche Fehlfunktionen, wie z. B. Motorstörungen, frühzeitig erkannt und Werkstattbesuche vorbereitet werden.

Folgende Story veranschaulicht den typischen Ablauf einer Online-Diagnose:

Herr Mustermann ist Eigentümer eines Autos. Während er fährt, meldet sein Auto eine Motorstörung, zeigt sie ihm an und sendet sie zugleich automatisiert an den Hersteller. Seine Werkstatt kontaktiert Herrn Mustermann nach der Fahrt, um einen Service-/Wartungstermin zu vereinbaren¹⁵.

13 Der European Road Transport Research Advisory Council (ERTRAC) klassifiziert Daten in die 4 Kategorien: "Complete Public Data", "Anonymised Data", "Released Data" und "Strictly Private Data", entsprechend ihrer Vertraulichkeit.

14 Der Standard J 1979 der SAE International (vormals: Society of Automotive Engineers (SAE)) beschreibt die Kommunikation zwischen Fahrzeug-OBD-Systemen und Test-Geräten mit Bezug auf Emissionsmessungen.

15 Der Fallstudie liegt die Annahme zugrunde, dass Herr Mustermann (der Fahrzeugnutzer) beim Fahrzeugkauf in die Nutzungsbedingungen des Online-Diagnose-Dienstes des Herstellers eingewilligt hat.

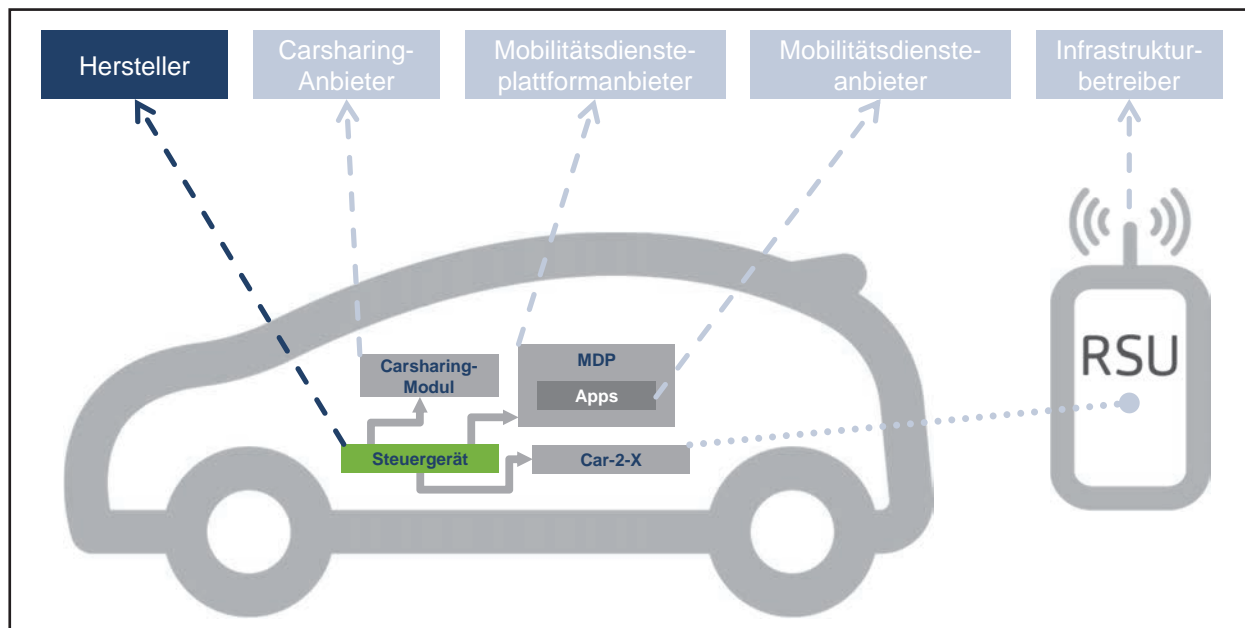


Abbildung 4: Datenflüsse der Fallstudie „Kfz-Instandhaltung und -Wartung“

Die zentralen Akteure dieser Fallstudie sind der Fahrzeughersteller und der Fahrer des Fahrzeugs, der hier – um den Sachverhalt einfach zu halten – auch gleichzeitig Eigentümer und Halter des Fahrzeugs ist. Als weiterer Akteur tritt zudem die Werkstatt in Erscheinung, welche im konkreten Fall eines Reparatur- oder Wartungsauftrages Diagnosedaten (und gespeicherte Kundendaten) vom Hersteller erhält.

Daten der Kategorie „dynamische Fahrzeugdaten“, also Sensor- und Diagnosedaten, stehen im Fokus dieser Fallstudie. Daneben fallen auch statische und dynamische Nutzerdaten an. Mögliche Implementierungen unterscheiden sich vor allem durch die Stelle der Auswertung der Sensordaten – diese kann entweder direkt im Fahrzeug oder beim Hersteller stattfinden. Auf die verschiedenen Varianten wird im Folgenden zusammen mit den datenbezogenen Vorgängen näher eingegangen.

2.1.1 Technische Betrachtung

Lokale Generierung und (Zwischen-)Speicherung von Daten durch und in Fahrzeugsystemen

Grundlage für jede Art der Online-Diagnose ist die Erfassung von Sensordaten unmittelbar im Automobil. Elektronische Steuergeräte sind mit Sensoren verbunden und erfassen ständig Messwerte, wie z. B. Temperaturen (außen, innen, Flüssigkeiten), Drücke (Reifen, Öl), Mengen (Luft, Öl, Kraftstoff) und Drehzahlen (Motor, Räder). Auf Grundlage dieser Messwerte können der aktuelle Betriebszustand des Fahrzeugs bestimmt und Unregelmäßigkeiten erkannt werden.

Eine erste Verarbeitung dieser Daten kann durch elektronische Steuergeräte direkt im Fahrzeug stattfinden. Dabei handelt es sich um kleine eingebettete Systeme, die auf funktionale Sicherheit und extreme Betriebsbedingungen, wie große Temperaturschwankungen, starke Vibrationen und erhöhte Feuchtigkeit, optimiert sind. Daher sind hier Rechenleistung und Speicher zumeist entsprechend limitiert und es ist nur eine rudimentäre Auswertung möglich. Üblich ist ein Abgleich von Soll- und Ist-Werten der einzelnen Sensoren, möglicherweise in Abhängigkeit von bestimmten Randbedingungen wie z. B. der Außentemperatur. Sind die Parameter außerhalb des erwarteten Bereichs, fällt die Diagnose negativ aus. Eine solche negative Diagnose wird üblicherweise in Form eines Fehlercodes zwischengespeichert.

Transfer von Daten aus Fahrzeugsystemen zum Hersteller

Prinzipiell werden bei jeder Form der Online-Diagnose Daten vom Fahrzeug an den Hersteller übertragen. Dies können die Sensordaten, ein Auszug oder Teilauswertung dieser Daten oder auch nur die lokal im Fahrzeug errechneten Diagnoseergebnisse sein.

Eine Online-Datenverbindung zum Hersteller kann, abhängig von der Netzverfügbarkeit und -qualität, jederzeit und überall via Mobilfunk hergestellt werden. Dazu ist entweder ein Mobilfunkrouter im Fahrzeug verbaut oder die Internetverbindung wird über das Smartphone des Fahrers hergestellt. Je nach Implementierung kann die Häufigkeit der Datenübertragungen variieren:

- Im einfachsten Fall werden die erfassten Daten direkt lokal ausgewertet, ohne dass eine Datenübertragung zum Hersteller erforderlich ist. Erst wenn bei der lokalen Diagnose eine Unregelmäßigkeit erkannt wird oder ein anderes vordefiniertes Ereignis eintritt, werden die Daten an den Hersteller übertragen.
- Ergänzend könnten auch auf Initiative des Herstellers aktiv Sensordaten vom Fahrzeug abgerufen werden, um z. B. einen Werkstattbesuch vorzubereiten.
- Eine weitere Option ist das Übertragen von Diagnoseergebnissen und/oder Sensordaten in periodischen Intervallen. So könnte die regelmäßige Übertragung von positiven Diagnoseergebnissen darüber Auskunft geben, ob die Datenerfassung und -übertragung fehlerfrei funktionieren.
- Im Extremfall könnten die erfassten Sensordaten – sofern die Mobilfunkverbindung dies zulässt – ständig an den Hersteller übertragen werden. Ein solcher Transfer könnte beispielsweise zum Zweck einer Auswertung auf den Servern des Herstellers erfolgen. Diese haben eine deutlich höhere Rechenleistung als die Steuergeräte im Fahrzeug. Außerdem ergeben sich durch den Abgleich von Daten verschiedener Fahrzeuge gleichen Typs und Alters erweiterte Diagnosemöglichkeiten.

Zum Fahrzeughersteller übertragene Daten werden dort verarbeitet, d. h. aus Sensordaten werden Diagnosedaten erstellt, abgeglichen und gegebenenfalls Aktionen entsprechend der Diagnoseergebnisse veranlasst. Es ist davon auszugehen, dass die beim Hersteller eingegangenen Daten ganz oder zumindest teilweise in zentralen Datenbanken abgelegt werden, so dass der Hersteller zu einem späteren Zeitpunkt darauf zugreifen kann.

Während lokal gespeicherte Daten keinen Personenbezug aufweisen, wird durch das Übertragen per Mobilfunk und Auslesen der Daten eine Verknüpfung zum individuellen Fahrzeug oder zu dessen Fahrer bzw. Halter hergestellt. Folglich sind sämtliche beim Hersteller eingehenden Daten personenbezogen. Es ist jedoch möglich, dass der Hersteller Daten zur weiteren Verarbeitung (z. B. für statistische Auswertungen) wieder anonymisiert oder pseudonymisiert.

Transfer von Daten vom Hersteller zur Werkstatt

Beim Fahrzeughersteller gespeicherte Daten können unter bestimmten Voraussetzungen an Dritte übermittelt werden. So ist es im Fall einer Reparatur oder Wartung durch einen entsprechenden Wartungsvertrag zwischen Kunden und Hersteller vorgesehen, relevante Daten an die ausführende Werkstatt zu übermitteln. Neben den Kunden- und

Fahrzeugidentifikationsdaten können dies auch aufzeichnete Diagnose- und Sensordaten des Fahrzeugs sein.

Die Übermittlung des Reparatur- oder Wartungsauftrages inklusive der erforderlichen Fahrzeugdaten erfolgt dabei über eine Datenverbindung zwischen den Systemen des Fahrzeugherstellers und der Werkstatt. Dies kann im einfachsten Fall ein klassisches Fax oder im Idealfall eine verschlüsselte Internet-Verbindung sein. Die Werkstatt hat ausschließlich Zugriff auf die im Rahmen des Auftrages übermittelten Daten sowie die während des Werkstatttermins „offline“ vom Fahrzeug (via Diagnoseschnittstelle) und vom Kunden erhobenen Daten. Sie hat keinen Zugriff auf weitere beim Fahrzeughersteller gespeicherte Kunden- oder Fahrzeugdaten.

2.1.2 Ökonomische Betrachtung

Die Wertschöpfungskette dieser Fallstudie erstreckt sich von der Erfassung von Sensordaten im Fahrzeug bis zum Anruf des Kunden zwecks Vereinbarung eines Service-/ Wartungstermins nach Auftreten der Motorstörung. Nutzen entsteht beim Hersteller insbesondere durch Verknüpfung mit Kundendaten, durch die Weiterleitung der Information zur Motorstörung an die Werkstatt und durch die Benachrichtigung des Kunden. Eine über die Fallstudie hinausgehende denkbare weitere Wertschöpfung wäre die Nutzung der entstehenden Daten bei einem Zulieferer des Herstellers nach entsprechender Analyse bzw. einem Datenfluss. Im Einzelnen:

- **Nutzen Hersteller:** Sensordaten werden entweder regelmäßig oder nur in spezifischen Fällen (z. B. einer Motorstörung) an den Hersteller übertragen, der die Daten weiterverarbeitet. Der Nutzen für den Hersteller ist vielfältig. Abhängig vom Umfang der übertragenen Daten erhält er beispielsweise einen guten Überblick über den Verschleiß von Bauteilen, wodurch Optimierungspotenziale im Bereich Forschung und Entwicklung erschlossen werden können. Im Fall einer Störung erhält der Hersteller darüber hinaus wertvolle Hinweise dazu, welche Fahrzeugkomponenten besonders anfällig oder wenig anfällig für Störungen sind, woraus sich Optimierungsmöglichkeiten bei der Produktion ergeben. Durch eine Verknüpfung der Sensor- bzw. Diagnosedaten mit den jeweiligen Kundendaten und die Einbindung einer Werkstatt ergibt sich für den Hersteller zudem die Möglichkeit, eine engere Kunden- bzw. Markenbindung herzustellen.
- **Nutzen Werkstatt:** Eine Werkstatt erhält die Störungsdaten und kann die detaillierten Informationen über die Störung dafür verwenden, auf den Kunden zuzugehen, einen Reparaturauftrag aktiv einzuwerben und ihn

ren Kundenstamm zu erhöhen. Da die Werkstatt frühzeitig Informationen dazu erhält, welche Komponenten genau betroffen sind, können ggf. bereits die Verfügbarkeit von Ersatzteilen geprüft und die Wartungstermine so optimiert werden.

- **Nutzen Fahrzeugeigentümer (= Fahrer)¹⁶:** Die Werkstatt setzt sich direkt mit dem Eigentümer des Fahrzeugs in Verbindung. Aus Sicht des Fahrzeugeigentümers kann ein ggf. auftretendes Problem frühzeitig erkannt werden und so vor dem tatsächlichen Auftreten eines Schadensfalls durch eine kostengünstigere Reparatur beseitigt werden. Dadurch erhöht sich die

Zuverlässigkeit des Fahrzeugs und verbessert sich die Planbarkeit der Reparatur aufgrund detaillierterer Informationen auf Seiten der Werkstatt.

- **Nutzen Zulieferer:** Eine denkbare Erweiterung der Fallstudie besteht darin, dass der Hersteller Störungsdaten aggregiert und an die entsprechenden Zulieferer weiterleitet. Dieser Zulieferer kann die Daten dafür verwenden, seine Komponenten sowohl aus Kosten- als auch aus Qualitätssicht zu optimieren. Dies wiederum verbessert sowohl die Profitabilität des Zulieferers und des Herstellers als auch die Gesamtqualität der hergestellten Fahrzeuge.

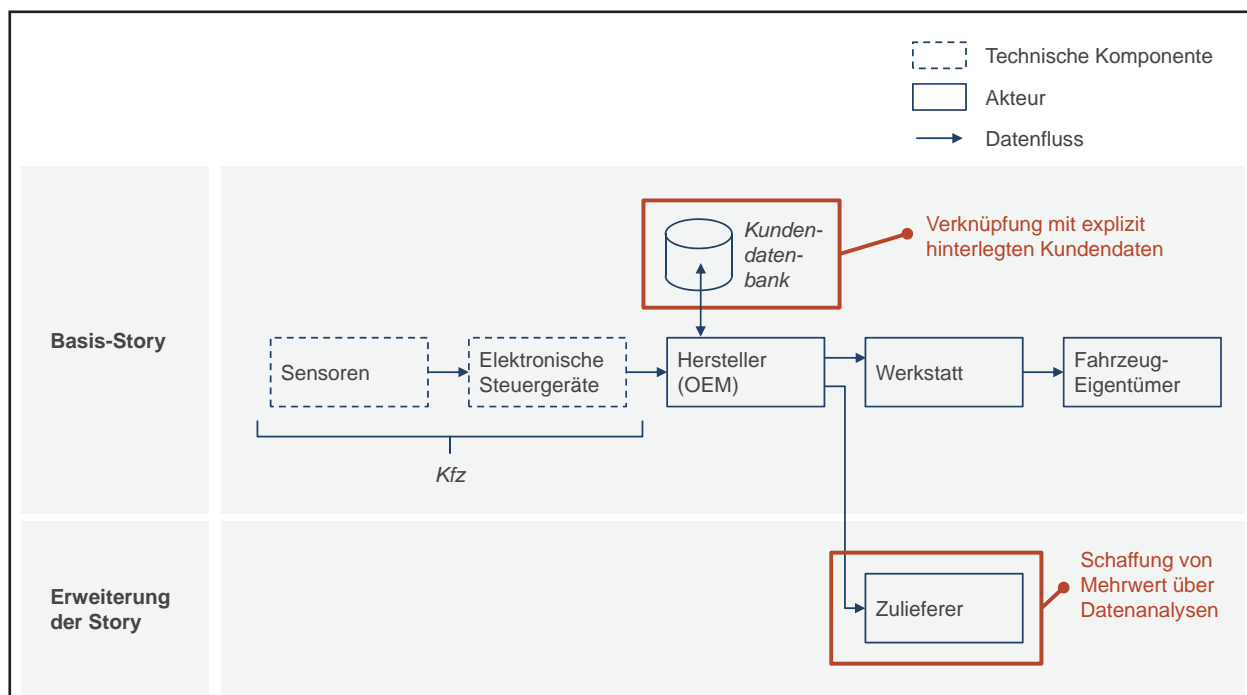


Abbildung 5: Wertschöpfungsnetzwerk der Fallstudie „Kfz-Instandhaltung und -Wartung“

16 Während der Schwerpunkt der Fallstudie auf der Übertragung der Daten zu Vertragswerkstätten (wahrscheinliche Implementierung) liegt, ist dem Fahrzeugnutzer die Möglichkeit offen, die Diagnosedaten durch eine freie Werkstatt auslesen zu lassen. Es besteht die Möglichkeit, Preise zu vergleichen, wodurch sich ein konkreter Nutzen für den Fahrzeugnutzer in Form von Einsparungspotenzialen ergeben kann.

2.2 Fallstudie 2: Carsharing

Carsharing ermöglicht das gemeinsame Nutzen von Fahrzeugen durch mehrere Personen. Anders als bei „klassischen“ Autovermietungen wird das Fahrzeug dabei nur für sehr kurze Zeiträume vermietet oder vermittelt. Dabei haben sich unterschiedliche Ausprägungen – vom stationsgebundenen über das sogenannte *free-floating Carsharing* bis hin zum Vermitteln von fremden, meist privaten Fahrzeugen – entwickelt.

Carsharing-Modelle

Beim klassischen **stationsgebundenen** *Carsharing* muss ein Fahrzeug zunächst reserviert werden, bevor es an einer festgelegten Station abgeholt und nach der Miete am selben Ort wieder abgestellt wird.

Free-floating (nicht-stationsgebundene) *Carsharing*-Fahrzeuge sind über den öffentlichen Raum verteilt und können üblicherweise ohne Reservierung genutzt werden. Anschließend wird das Fahrzeug an einem beliebigen (zulässigen) Parkplatz innerhalb des Nutzungsgebiets abgestellt.

Ein weiteres Modell verzichtet ganz auf eigene Mietfahrzeuge und beschränkt sich lediglich auf die **Vermittlung von fremden, meist privaten Autos** an *Carsharing*-Nutzer.

Interessant für diese Fallstudie ist insbesondere das „*free-floating*“ Modell, da hier eine simple Schlüsselübergabe meist nicht möglich ist und zur Abwicklung der Mietvorgänge der Einsatz spezieller Technologie notwendig ist. Dabei entsteht ein entsprechend hohes Datenaufkommen. Üblicherweise integriert der *Carsharing*-Anbieter zu diesem Zweck eigene Systeme – sogenannte *Carsharing*-Module – mit eigens angepasster Software in die Fahrzeuge.

Carsharing-Modul

Das *Carsharing*-Modul ist ein vom *Carsharing*-Anbieter in das Mietfahrzeug integriertes System. Es enthält Hard- und Software, die das Fahrzeug um die für das *Carsharing* notwendigen Funktionen erweitert. Je nach *Carsharing*-Anbieter können z. B. folgende Funktionen vom *Carsharing*-Modul bereitgestellt werden:

- **Elektronische Zugangskontrolle** über Zugangskarte oder App auf dem Smartphone
- Erfassung der **Mietdaten zur Abrechnung**
- Ermittlung der **Fahrzeugposition** über eigene oder Fahrzeugtechnik
- **Kommunikation** mit dem *Carsharing*-Anbieter über eigene oder Fahrzeugtechnik
- **Personalisierte Fahrzeuganwendungen**, z. B. Navigationssystem
- **Schnittstelle zum Fahrzeug** für Zugriff auf dessen Sensoren (z. B. GPS oder Tankfüllstand), Aktoren (z. B. Öffnen und Schließen des Fahrzeuges) oder weitere Systeme (z. B. Mobilfunkmodem)

Eine besondere Problematik im Zusammenhang mit *Carsharing*-Fahrzeugen stellt die Nutzung durch eine Vielzahl verschiedener Personen dar. Die im Fahrzeug integrierten technischen Systeme bieten Personalisierungsmöglichkeiten (z. B. Sitzposition) und speichern eingegebene Daten und Anfragen (z. B. Ziele im Navigationssystem). Beim eigenen Fahrzeug finden eine Personalisierung und die damit einhergehende Zuordnung von Daten zum jeweiligen Benutzer mithilfe verschiedener Autoschlüssel pro Fahrer oder gar nicht statt. Da im *Carsharing*-Fahrzeug alle Nutzer denselben Autoschlüssel verwenden, besteht hier in der Regel das Problem, dass personalisierte Einstellungen geteilt werden und Daten sowie Anfragen des Vornutzers, wie z. B. die letzten Ziele im Navigationssystem, einsehbar sind.

Dieser Problematik kann vom *Carsharing*-Anbieter nur durch Anpassung der Software im Fahrzeug oder Ersetzen von Teilsystemen durch das integrierte *Carsharing*-Modul entgegengewirkt werden. Gerade die nicht-stationsgebundenen (*free-floating*) *Carsharing*-Anbieter haben – allein wegen der notwendigen elektronischen Zugangskontrolle – üblicherweise ein solches *Carsharing*-Modul in das Fahrzeug integriert. Dieses erlangt je nach Integrations-tiefe Zugriff auf verschiedene Daten im Fahrzeug. Da sich der Nutzer vor der Miete über dieses Modul authentifiziert, ist eine Personalisierung sehr gut möglich. So können einzelne Anwendungen der Fahrzeuge, wie z. B. das Navigationssystem, in personalisierter Form im *Carsharing*-Modul integriert sein und die originären (nicht-personalisierten) Anwendungen des Fahrzeugherstellers ersetzen. Durch die Personalisierung der *Carsharing*-Module ist folglich eine klare Trennung zwischen den Daten der unterschiedlichen Nutzer möglich. Zudem können personalisierte Einstellun-

gen verschiedener Nutzer gespeichert und über mehrere Fahrzeuge hinweg synchronisiert werden, ohne dabei für andere Nutzer sichtbar zu werden. Allerdings gilt dies nur für in das *Carsharing*-Modul integrierte Anwendungen. Werden jedoch einzelne nicht an die Personalisierung des *Carsharing*-Moduls angebundene Anwendungen des Fahrzeugs unverändert genutzt, so besteht für diese weiterhin die Gefahr, dass die betroffenen Daten unbefugt an Nachnutzer gelangen können.

Ein lebensnahes Beispiel für die Datenerstellung bei der Nutzung von *Carsharing*-Fahrzeugen sieht wie folgt aus:

Frau Musterfrau öffnet das Fahrzeug eines Carsharing-Anbieters mit ihrer Zugangskarte und tritt die Fahrt an. Nach Abstellen des Fahrzeugs und Beendigung des Mietvorgangs erhält sie eine Rechnung über die gefahrene Strecke über ihr Kundenkonto.

Im Fokus der Fallstudie 2 stehen die Trennung der zuvor identischen Rollen von Fahrzeughalter und Fahrer sowie die Beziehung beider Akteure beim Zugriff auf statische und dynamische Nutzerdaten. Während der *Carsharing*-Nutzer auch die Rolle des Fahrers einnimmt, ist der *Carsharing*-Anbieter üblicherweise Halter und Eigentümer des Fahrzeugs. Der Hersteller tritt nicht explizit in Erscheinung und hat hier nur noch eine Nebenrolle als „Lieferant“ des Fahrzeugs und eventuell Integrator des *Carsharing*-Moduls (Abbildung 6).

Neben statischen und dynamischen Nutzerdaten fallen zudem Positionsdaten der stehenden Fahrzeuge und dynamische Fahrzeugdaten (z. B. Tankfüllstand) an. Durch die eindeutige Zuordnung der Daten über das *Carsharing*-Modul zu dem jeweiligen *Carsharing*-Nutzer erhalten alle anfallenden Daten einen Personenbezug. Eine detaillierte Beschreibung der wesentlichen datenbezogenen Vorgänge erfolgt in den folgenden Abschnitten.

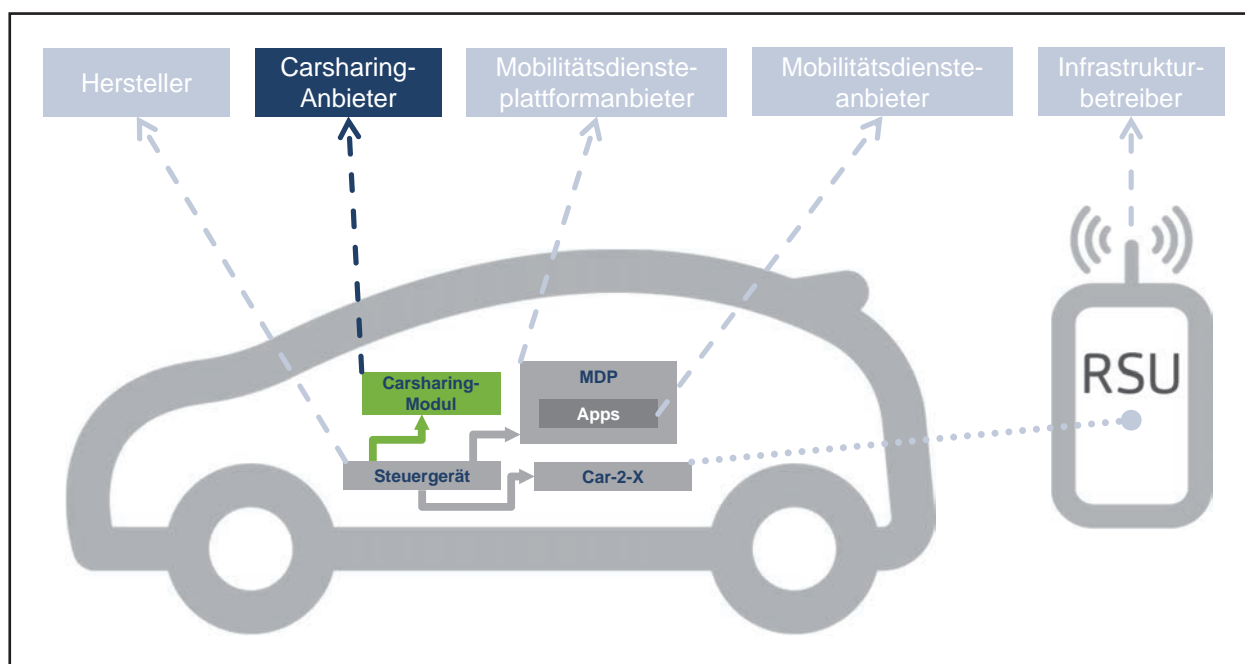


Abbildung 6: Datenflüsse der Fallstudie „Carsharing“

2.2.1 Technische Betrachtung

Transfer von Daten aus dem Carsharing-Modul zum Carsharing-Anbieter zu Mietbeginn und -ende

Da es beim *free-floating* Carsharing keine Möglichkeit gibt, dem Kunden den passenden Fahrzeugschlüssel zum gewünschten Fahrzeug auszuhändigen, wird der Zugang zu den Fahrzeugen durch elektronische Systeme geregelt. Der Carsharing-Nutzer nutzt zum Öffnen des Fahrzeugs üblicherweise seine Kundenkarte (Zugangskarte) oder eine spezielle Smartphone-App des Carsharing-Anbieters.

Das in das Fahrzeug integrierte Carsharing-Modul prüft online die Zugangsberechtigung und verlangt optional zusätzlich die Eingabe einer PIN im Fahrzeug. Der Mietvorgang beginnt bei Öffnung des Fahrzeugs. Gleichzeitig werden neben der Prüfung der Zugangsberechtigung relevante Daten zur Abrechnung per Mobilfunk an den Carsharing-Anbieter übertragen. Diese umfassen mindestens die Kundennummer, den Zeitpunkt sowie die aktuelle Position und den Kilometerstand des Fahrzeugs. Dieselben Daten werden beim Beenden des Mietvorgangs erneut erhoben und an den Carsharing-Anbieter übertragen. Je nach Integrationstiefe kann das Carsharing-Modul auch direkt mit den Sensoren im Fahrzeug interagieren (z. B. Erfassen des Tankfüllstands).

Dort werden die Daten zur Rechnungslegung weiterverarbeitet. Zusätzlich wird die neue Fahrzeugposition zur Prüfung des Abstellortes sowie zur Weitervermittlung des Fahrzeugs verwendet.

Transfer von Statusinformationen vom Carsharing-Modul zum Carsharing-Anbieter während der Miete

Abhängig vom Abrechnungsmodell reicht das einfache Erheben von Daten zu Beginn und Ende des Mietvorgangs nicht aus. Neben den üblichen entfernungs- und zeitbasierten Preismodellen ist auch eine streckenbasierte Abrechnung denkbar. In einem solchen Fall wird auch die genaue Streckenführung während des Mietvorgangs durch durchgängiges Erheben der Fahrzeugposition in Echtzeit erfasst. Auf diese Weise kann sowohl Diebstählen vorgebeugt als auch sichergestellt werden, dass sich das Mietfahrzeug zu jedem Zeitpunkt im zulässigen Nutzungsgebiet befindet.

Neben der Erhebung von Positionsdaten ist – je nach Integrationstiefe des Carsharing-Moduls – auch die Erfassung ausgewählter Sensordaten möglich. Durch das Erfassen des Tankfüllstands, oder Batterieladestandes bei Elektrofahrzeugen, kann so z. B. dem Unterschreiten des minimal zulässigen Tankfüllstandes und den möglichen Folgekosten (z. B. Abschleppen des Fahrzeugs) vorgebeugt werden.

Während ein GPS-Empfänger zur Ermittlung der Positionsdaten sowohl im ursprünglichen Fahrzeug als auch direkt im integrierten System des Carsharing-Anbieters verbaut sein kann, ist der Ursprung der Daten zum Tankfüllstand in jedem Fall eine vom Fahrzeughersteller verbaut Komponente. Üblicherweise wird diese Information von einer Sonde im Tank erfasst und über einen Fahrzeugbus bereitgestellt, welcher über eine Schnittstelle mit dem integrierten Carsharing-Modul verbunden ist und darüber den Tankfüllstand sowie gegebenenfalls weitere Daten weiterreicht.

Fahrzeugbus

In Fahrzeugen kommt nicht ein zentraler Rechner als Steuergerät zum Einsatz, sondern eine Vielzahl von verteilten Steuergeräten, die auf eine oder wenige Aufgaben spezialisiert sind. Dieses verteilte System ist darauf angewiesen, dass Informationen zwischen Steuergeräten geteilt werden können. Zu diesem Zwecke kommen in der Regel mehrere Datenbusse im Fahrzeug zum Einsatz, an welche die jeweiligen beteiligten Steuergeräte angeschlossen sind. Dabei gibt es verschiedene technische Lösungen für die Ausgestaltung des Bussystems.

Der Diagnosebus zur On-Board-Diagnose (OBD) ist ein konkreter Fahrzeugbus, der auch zu Diagnosezwecken nach außen geführt ist (siehe Fallstudie 1).

Die Erhebung von Echtzeitstatusinformationen während des Mietvorgangs ist generell eher als datenintensiv einzustufen, da kontinuierlich Daten gesammelt werden, wobei sowohl die Datenmenge als auch die Frage, ob die Daten auch in Echtzeit an den Carsharing-Anbieter übertragen werden, von der konkreten Implementierung und der Länge der Intervalle zwischen den Erhebungen abhängen.

Datenübertragung des stehenden Fahrzeugs

Auch das stehende Fahrzeug erhebt und sendet regelmäßig Statusinformationen an den Carsharing-Anbieter. Hierfür gibt es mehrere Gründe: Zum einen möchte man auch außerhalb eines Mietvorgangs einen möglichen Diebstahl erkennen – bewegt sich das Auto, wird Alarm ausgelöst. Zum anderen gibt es veränderliche Faktoren – wie z. B. den Akkuladestand bei Elektrofahrzeugen oder die Stromversorgung des Carsharing-Moduls in Verbrennerfahrzeugen, die für die Weitervermittlung relevant sind. Die Datenübertragung an den Carsharing-Anbieter stellt somit unter anderem sicher, dass die elektronische Zugangsprüfung funktioniert und eine Kommunikation zum Carsharing-Anbieter möglich ist. Auf diese Weise wird außerdem die

Notwendigkeit zusätzlicher technischer Wartungen oder das Abschleppen im Falle einer Unterschreitung der kritischen Marke der Energiereserven minimiert.

Sowohl Ladestände als auch Positionen werden periodisch lokal erhoben und können zunächst lokal im Fahrzeug ausgewertet werden. Beim Eintreten von vordefinierten Ereignissen wie einem kritischen Ladestand oder einer unerwarteten Positionsänderung werden die entsprechenden Daten über eine Mobilfunkverbindung an den *Carsharing*-Anbieter übermittelt. Diese datenarme Umsetzung hat jedoch den Nachteil, dass die Fahrzeugstatusinformationen beim *Carsharing*-Anbieter eventuell nicht dem aktuellen Stand entsprechen. Da diese jedoch teilweise zur Weitervermittlung relevant sind (z. B. Akkuladestand), ist zu erwarten, dass der *Carsharing*-Anbieter eine datenintensivere Implementierung bevorzugt, bei der die erhobenen Statusinformationen entweder regelmäßig (z. B. stündlich) oder bei jeder Änderung (z. B. ein Prozentpunkt weniger Akku-ladestand) an ihn übertragen werden.

Obwohl die Datenübertragung technisch gesehen den Übertragungsvorgängen während und zu Beginn der Miete entspricht, ist der fehlende Personenbezug im Fall des nicht vermieteten Fahrzeugs als ein wichtiger Unterschied hervorzuheben.

2.2.2 Ökonomische Betrachtung

Durch das Erfassen und Auslesen von Echtzeitstatusinformationen des Fahrzeugs (z. B. aktuelle Position, Tankfüllstand) sowie von Mietvorgangsdaten und persönlichen Daten des Fahrzeugnutzers ergeben sich für den *Carsharing*-Anbieter verschiedene Möglichkeiten, direkt oder indirekt Gewinn zu erzielen bzw. diesen zu steigern. Der *Carsharing*-Anbieter ist der zentrale Akteur im Wertschöpfungsnetzwerk dieser Fallstudie, aber auch für den *Carsharing*-Kunden und die Tankstelle entstehen konkrete Nutzenpotenziale.

■ Nutzen *Carsharing*-Anbieter:

- Durch die Erhebung der Echtzeitstatusinformationen (z. B. Positionsdaten, Fahrtstrecke) des Fahrzeugs während des Mietvorgangs kann der *Carsharing*-Anbieter den Bedarf an Fahrzeugen sowie viel befahrene Strecken ermitteln und anhand dessen Flotte und Streckennetz verbessern. Somit können die Qualität des Angebots optimiert und Gewinnsteigerungen erzielt werden.
- Durch die Datenübertragung des Tankfüllstandes weiß der *Carsharing*-Anbieter genau, welches seiner Fahrzeuge wann und wie viel von welchem Fahrzeugnutzer/Kunden betankt wurde. Konkret be-

deutet dies, dass er Kunden, die ein Fahrzeug mit leerem Tank abstellen, einen höheren Betrag in Rechnung stellen und seine Fakturierung verbessern kann.

- Die Echtzeit-Kontrolle der gefahrenen Strecke und der genauen Positionsdaten des Mietwagens ermöglicht dem *Carsharing*-Anbieter, genau zu verfolgen, ob der Fahrzeugnutzer das für die Anmietung freigegebene/erlaubte Gebiet verlässt. In einem denkbaren erweiterten Szenario ermöglicht diese Kontrolle eine Form von Compliance-Tracking und die Möglichkeit, Zusatzzahlungen bei Verlassen des erlaubten Fahrgebiets zu erheben.
- Eine mögliche Erweiterung der Fallstudie besteht darin, dass der *Carsharing*-Anbieter die aggregierten Daten der Fahrzeugnutzer aus seiner Kundendatenbank sowie die Mietvorgangsdaten analysieren und die Ergebnisse zur Entwicklung neuer Produkte verwenden kann. Denkbar wäre das Angebot differenzierter Preise in bestimmten Zeitfenstern oder für bestimmte Kundengruppen (z. B. preisliche Anreize zu Rush-Hour-Zeiten). In Kombination mit den Kundendaten wäre dies sogar auf individueller Basis möglich (z. B. höhere Preise für Kunden, bei denen aufgrund ihrer Fahrweise großer Fahrzeugverschleiß oder Unfallschäden drohen).
- Eine Ausgabe von bspw. Tank- oder Freiminutengutscheinen an Kunden, welche zuvor aufgetankt haben, kann einerseits die Kundenbindung verbessern und andererseits für Vermittlungsdienste anteilige Zahlungen generieren. Es ergeben sich kurz- und langfristige Ertragssteigerungspotenziale.

■ **Nutzen Kunde:** Durch die Verbesserung des Produktsortiments (Anpassung Flotte, Streckennetz) sowie den Erhalt von Tankgutscheinen hat der Fahrzeugnutzer sowohl einen qualitativen als auch einen quantitativen Nutzen.

■ **Nutzen Vertragstankstellen:** Durch die Ausgabe von Tank- oder Freiminutengutscheinen durch den *Carsharing*-Anbieter erhält der jeweilige Kunde einen Anreiz, künftig bei den beteiligten Vertragstankstellen aufzutanken. In diesem Erweiterungsfall ergeben sich für die Vertragstankstellen durch Neukundengewinnung und eine verbesserte Kundenbindung Ertragssteigerungspotenziale sowohl in ihrem Kerngeschäft als auch durch den Verkauf ergänzender Produkte und Dienstleistungen im Tankstellenshop (Cross-Selling). Der Nutzen für die Vertragstankstellen entsteht somit in Form von gesteigertem Umsatz, nicht direkt durch die Nutzung von Daten.

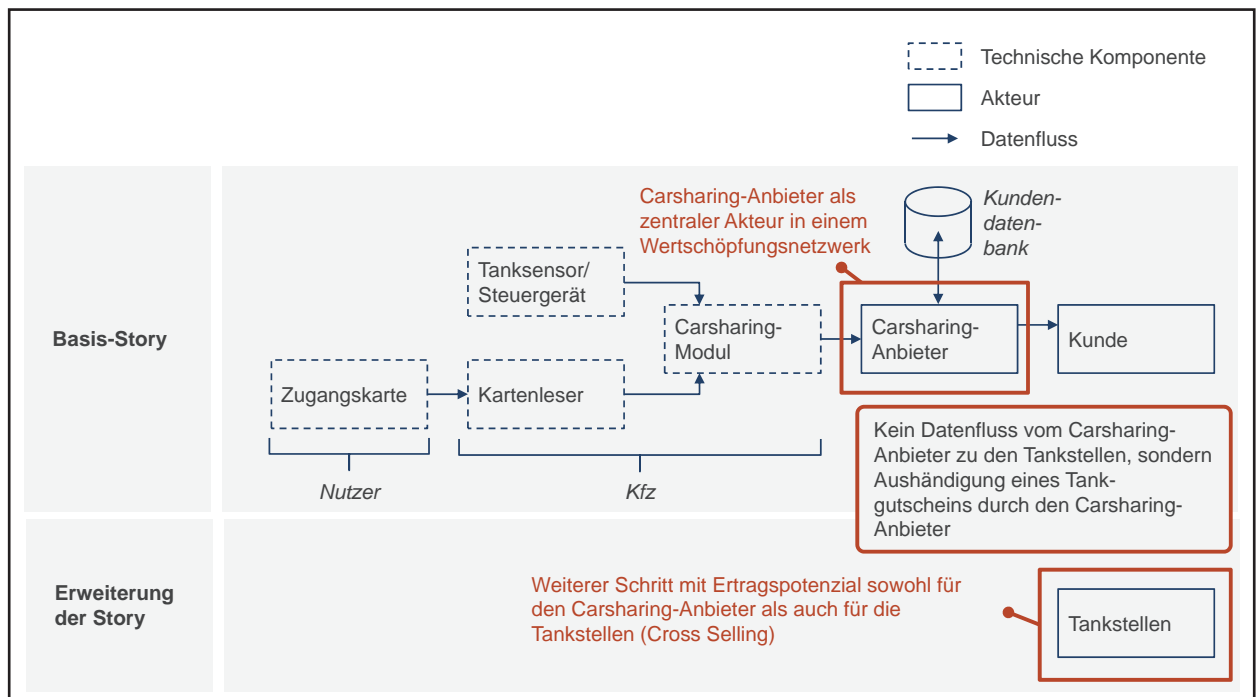


Abbildung 7: Wertschöpfungsnetzwerk der Fallstudie „Carsharing“

2.3 Fallstudie 3: Mobilitätsdienstleistungsplattform

Die „In-Vehicle Infotainment“-Systeme (IVI) aktueller Fahrzeuge bieten bereits mehr als nur Radio und Navigation. Fallstudie 3 wirft einen Blick auf IVI-Systeme, die nicht einem einzelnen, spezifischen Zweck gewidmet sind. Solche sogenannten Mobilitätsdienstleistungsplattformen (MDP) sind die konsequente Weiterentwicklung von Unterhaltungs- und Informationsangeboten im Fahrzeug. Sie sind vollständig in das Look-and-Feel des Fahrzeugdesigns, des Bedienkonzepts sowie der Anzeige- und Bedienelemente integriert. Dabei gibt es viele verschiedene Möglichkeiten der Ausgestaltung von MDP. Gängige Beispiele sind der Anschluss eines Smartphones, voll-integrierte Lösungen und Aftermarket Devices.

Arten von Mobilitätsdienstleistungsplattformen (MDP)

MDP, die eine **Integration eines Smartphones** in die Anzeige- und Bedieneinrichtungen des Fahrzeugs ermöglichen, vermitteln durch Steuerung über Fahrzeugbedienelemente und Anzeige im integrierten Fahrzeugbildschirm den Eindruck einer vollständigen Integration, laufen jedoch auf dem Smartphone. Beispiele sind die Produkte „Android Auto“ (Google), „Apple CarPlay“ und „Mirrorlink“.

Die Hersteller von Mobilbetriebssystemen positionieren ihre Produkte auch bereits als **vollständig integrierte Lösung**, bei der kein Smartphone mehr gekoppelt werden muss, um die gleiche Funktionsvielfalt zu ermöglichen. Beispiele sind die angekündigten Produkte „Windows in the car“ (Microsoft) und „Android in-car“ (Google).

Darüber hinaus gibt es **nachrüstbare Lösungen (Aftermarket Devices)**, wie Autoradios, die Android als Betriebssystem verwenden und daher einen ähnlichen Funktionsumfang wie die vom Hersteller werksseitig integrierten, bereits aufgeführten Systeme ermöglichen.

Alle Varianten ermöglichen die Bündelung von fahrzeug- und nutzerspezifischen Daten in der MDP, um darauf aufbauend Dienste anzubieten. MDPs werden häufig von Drittanbietern angeboten und in das Fahrzeug integriert. Doch inzwischen haben auch viele Hersteller eigene MDPs entwickelt (siehe Kapitel 4.2.2).

Gegenstand dieser Fallstudie ist die Nutzung von vorinstallierten Basisdiensten/-anwendungen des MDP-Anbieters auf der Plattform eines Drittanbieters:

Im Fahrzeug von Herrn Mustermann ist eine Mobilitätsdienstplattform eines Drittanbieters integriert. Auf dem wird das aktuelle Wetter an der Fahrzeugposition angezeigt. Herr Mustermann ist mit seinem persönlichen Account am System angemeldet und tätigt einen Telefonanruf aus der synchronisierten Kontaktliste.

Im Vergleich zu den vorherigen Fallstudien kommt in Fallstudie 3 der MDP-Anbieter als zusätzlicher, zentraler Akteur hinzu. Im Mittelpunkt der Betrachtung stehen seine Beziehungen zum Fahrer und zum Fahrzeughersteller.

Unabhängig von der konkreten Ausgestaltung der MDP geht es in Fallstudie 3 um die Kombination von statischen Nutzerdaten (in Form des personalisierten Accounts des Nutzers und seiner Kontaktliste) mit Positionsdaten und Daten, die vom Plattformbetreiber bereitgestellt werden (hier das Wetter). Diese Fallstudie mit den resultierenden Datenflüssen ist technisch und funktional betrachtet mit allen genannten MDPs realisierbar.

Integrationstiefe

Die Tiefe der Integration und die Menge der Daten, die zwischen den Fahrzeugsystemen und der lokalen MDP geteilt werden, variieren zwischen den konkreten Implementierungen. Bei ab Werk integrierten Lösungen hat der Fahrzeughersteller vollen Einfluss darauf, wie die Integration erfolgt, welche technischen Zugriffsmöglichkeiten bestehen und welche Daten geteilt werden. Bei Nachrüstlösungen erfolgt die Auswahl durch die ausführende Stelle vergleichbar mit der Integrationstiefe von Carsharing-Modulen in Fallstudie 2. Es lassen sich folgende Integrationstiefen differenzieren:

Vollständig voneinander **isolierte Systeme**, wie z. B. Navigationssysteme, die mittels eines Saugnapfs an der Windschutzscheibe befestigt werden, haben keinen Zugriff auf das Fahrzeug.

Nachgerüstete Autoradios oder andere Geräte mit OBD-II-Anschlussmöglichkeit können über einen **Diagnosebusabgriff** Zugang zu Fahrzeugdaten erhalten.

Vollständig integrierte Lösungen mit direktem Zugriff auf fahrzeuginterne Bussysteme können einen gleichberechtigten Zugang zu allen Informationen haben.

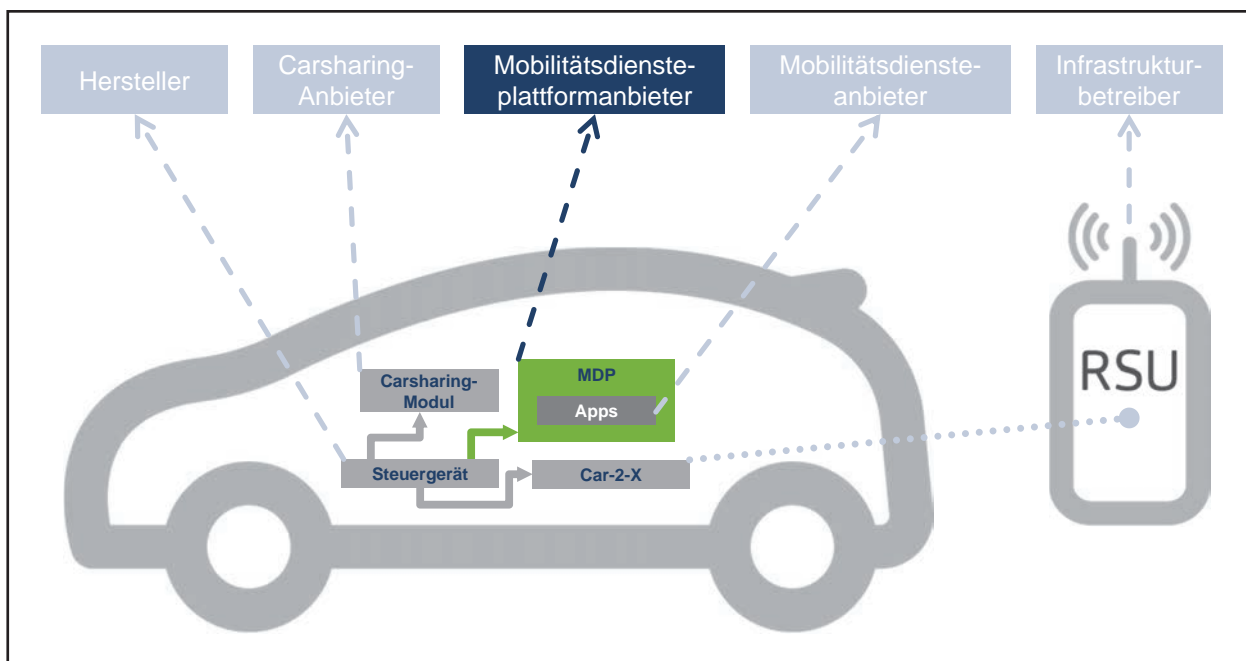


Abbildung 8: Datenflüsse der Fallstudie „Mobilitätsdienstplattform“

2.3.1 Technische Betrachtung

Synchronisierung der Mobilitätsdienstplattform mit der Cloud

Der MDP-Anbieter bietet Nutzern im Allgemeinen ein Benutzerkonto mit mehreren Basisdiensten (z. B. Adressbuch- und E-Mail-Anwendungen sowie Telefonie und Kalenderfunktionen). Nutzer erhalten Speicherplatz für persönliche Daten und können E-Mails, Kalendereinträge, ihre Kontaktliste und vieles mehr in der *Cloud* des MDP-Anbieters speichern. Um die Nutzung der genannten Basisdienste zu ermöglichen, werden die in der *Cloud* gespeicherten Daten synchronisiert. Dabei können Daten sowohl von der *Cloud* in die MDP als auch umgekehrt von der MDP in die *Cloud* fließen. Die dabei eingesetzten Technologien sind die im Fahrzeug befindliche MDP mit ihren Schnittstellen zu Fahrzeugdaten sowie die Serversysteme des MDP-Anbieters. Die Verbindung wird über eine Internetverbindung per Mobilfunk hergestellt.

Welche Daten zwischen der MDP und den *Cloud*-Systemen des MDP-Anbieters synchronisiert werden ebenso wie die Häufigkeit und Strategie der Synchronisierung sind dabei plattformabhängig. Bei Tätigung des Telefonanrufs in der beschriebenen Story wird folglich die Kontaktliste des Fahrzeugnutzers (Personendaten) aus der *Cloud* mit der MDP synchronisiert.

Der MDP-Anbieter hat technische Zugriffsmöglichkeiten auf alle in der *Cloud* synchronisierten Daten. Die Fahrzeugsysteme (z. B. IVI oder die Freisprecheinrichtung des Fahrzeugs) haben keinen Zugriff auf die Daten der MDP, können jedoch bei Bedarf mit benötigten Daten (z. B. Rufnummer bei Anrufinitiierung) versorgt werden.

Datenfluss von der Mobilitätsdienstplattform zum Fahrzeug

Durch die Tätigung des Telefonanrufs aus der synchronisierten Kontaktliste werden Daten, die in der MDP vorliegen, auch für weitere Fahrzeugsysteme nutzbar gemacht. Auch ohne MDP ist es möglich, dem Fahrzeugsystem ganze Kontaktlisten aus via Bluetooth gekoppelten Mobiltelefonen zu übertragen, um Anrufe vom Fahrzeugsystem aus zu initiieren und mit der darin verbauten Freisprecheinrichtung zu führen. Übertragen auf das Szenario der MDP wäre zum einen eine Übertragung der gesamten Kontaktliste in das IVI-System des Fahrzeugs denkbar, um von dort bequem Anrufe initiieren zu können. Zum anderen ist eine Implementierung vorstellbar, bei der benötigte Daten (Telefonnummer und evtl. Kontaktnamen zur Anzeige) erst zur Anrufinitiierung übertragen werden. Dies wäre insbesondere im Fall einer vollständig integrierten MDP notwendig, wenn diese keine eigene Mobilfunkhardware besitzt und stattdessen auf ein im Fahrzeug integriertes

Telefoniesystem zurückgreifen muss. Aber auch bei einer per Smartphone integrierten MDP werden spätestens bei hergestellter Verbindung die Audiodaten des Telefonats an das Fahrzeugsystem weitergereicht, um den Ton über die Lautsprecher des Fahrzeugs auszugeben.

Datenfluss vom Fahrzeug zur Mobilitätsdienstplattform

Neben der Synchronisation von Personendaten entsteht durch die Verwendung der Basisanwendungen auf der MDP ein Datenfluss zwischen Fahrzeug und MDP. In der beschriebenen Story bezieht die Wetteranwendung über einen eigenen oder den im Fahrzeug verbauten GPS-Empfänger (sofern technische Zugriffsmöglichkeiten bestehen) die Positionsdaten des Fahrzeugs, um eine lokalisierte Anzeige des aktuellen Wetters auf dem Bildschirm des IVI-Systems anzeigen zu können. Mit der aktuellen Fahrzeugposition wird eine Anfrage zum Wetterdienstanbieter gestellt, der diese mit der darzustellenden Wetterinformation beantwortet.

Für Fallstudie 3 wird angenommen, dass der Anbieter der MDP auch der Anbieter des Wetterdienstes ist und dieser durch die Anfragen Kenntnis über die Position der anfragenden Fahrzeuge erhält. Die Anfrage muss hierbei nicht notwendigerweise einen Bezug zum Fahrzeug bzw. Nutzer enthalten. Welche weiteren Informationen außer der genauen Position noch enthalten sind, ist von der konkreten Implementierung abhängig.

2.3.2 Ökonomische Betrachtung

Durch das Angebot und die Nutzung der MDP und der darauf vorinstallierten Basisdienste entsteht Nutzen bei allen beteiligten Akteuren. Im Zentrum des Wertschöpfungsnetzwerks steht der MDP-Anbieter selbst, da er die Standortdaten des Fahrzeugs – insbesondere in Kombination mit Nutzerdaten – für das Angebot von Mehrwertleistungen nutzen kann. Eine denkbare Erweiterung der beschriebenen Story ist die Installation zusätzlicher Anwendungen auf der MDP. Dieses Szenario wird in Fallstudie 4 beschrieben (siehe Kapitel 2.4).

- **Nutzen MDP-Betreiber:** Durch Verknüpfung der Standortdaten des Fahrzeugs mit Profilen naheliegender Restaurants, Geschäfte oder Tankstellen ist es dem MDP-Betreiber möglich, diese und ggf. deren Bewertung im Navigationssystem anzuzeigen sowie standortbezogene Werbung auf dem Display des Infotainmentsystems zu schalten. Während Ersteres als Zusatznutzen des Navigationssystems anzusehen ist, kann der MDP-Anbieter durch Letzteres konkreten Nutzen auch für andere Akteure schaffen. Hier sind vielfältige Geschäftsmodelle denkbar: So z. B. der Verkauf von Werbefläche auf der MDP oder der Handel mit Nutzerdaten aus der MDP-*Cloud*.

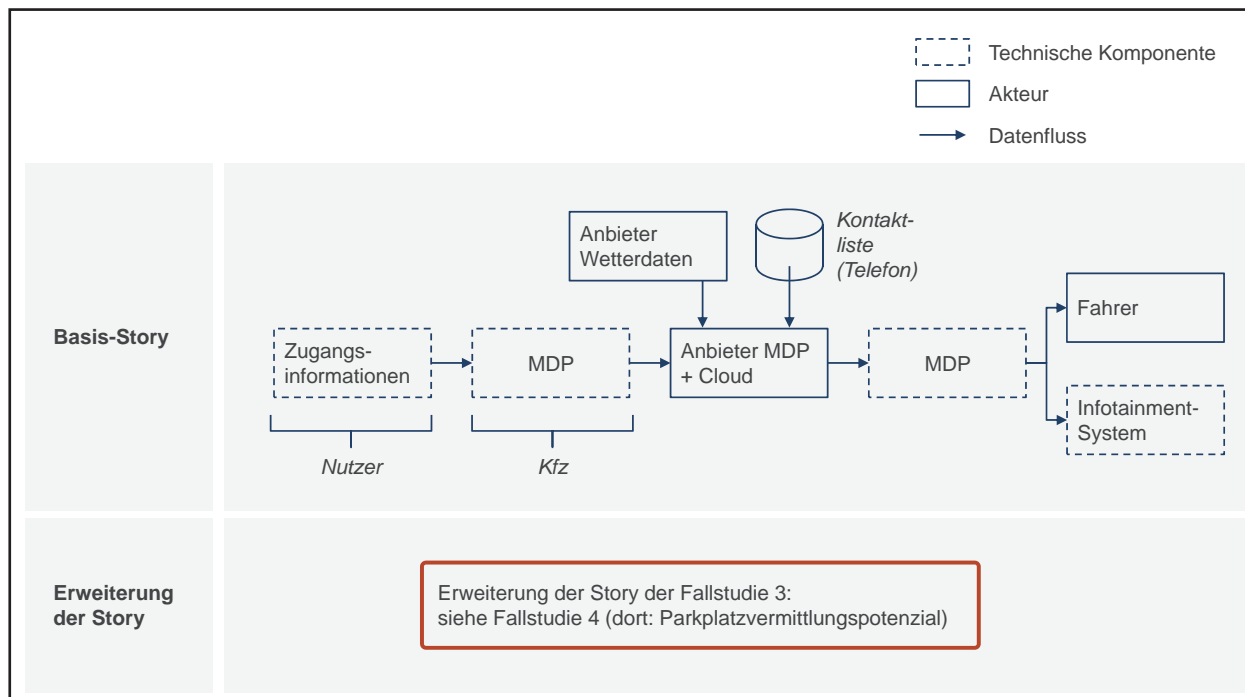


Abbildung 9: Wertschöpfungsnetzwerk der Fallstudie „Mobilitätsdienstesteplattform“

- **Nutzen Fahrzeugnutzer:** Der Fahrzeugnutzer kann über die synchronisierte Kontaktliste bequem Anrufe über die MDP tätigen und die im Fahrzeug integrierte Freisprechanlage zu diesem Zweck nutzen. Ebenso stellt die automatische Anzeige der lokalen Wetterinformationen in Echtzeit – und in einem erweiterten Fall die Anzeige naheliegender Geschäfte, Restaurants oder Tankstellen – eine nützliche Zusatzinformation dar. Insgesamt ergibt sich durch die Bereitstellung vorinstallierter Basisanwendungen durch den MDP-Anbieter ein Komfortgewinn für den Fahrzeugnutzer.

die Komplexität der Akteurskonstellation mit verschiedenen Datenzugriffsmöglichkeiten nochmals gesteigert.

Da es eine Vielzahl von Mobilitätsdiensten mit unterschiedlichen Angeboten gibt, ist eine Verallgemeinerung für diese Fallstudie nicht möglich. Aus diesem Grund wird exemplarisch die Nutzung einer Mobilitätsdienstleistung zur Parkplatzvermittlung betrachtet:

Frau Mustermann sucht über eine Parkplatzreservierungs-App eines unabhängigen Anbieters, die auf der MDP installiert ist, einen freien Stellplatz in einem Parkhaus in ihrer Umgebung.

2.4 Fallstudie 4: Mobilitätsdienste

Über offene MDP haben (vom Fahrzeughersteller und MDP-Anbieter) unabhängige Mobilitätsdiensteanbieter die Gelegenheit, ihre Dienste in das Fahrzeug zu bringen. Jedem Diensteanbieter steht frei, seinen Mobilitätsdienst in Form von Apps über die App-Marktplätze der MDP zu verteilen, so dass der Nutzer sie selbstständig installieren und so das in Fallstudie 3 beschriebene Angebot von Basisanwendungen erweitern kann.

Fallstudie 4 ist somit eng an die vorhergehende Fallstudie angelehnt. Im Fokus stehen hier von Drittanbietern betriebene Mobilitätsdienste, welche auf der zuvor beschriebenen MDP installiert sind bzw. nachinstalliert wurden. Durch das Hinzutreten des Mobilitätsdiensteanbieters, zusätzlich zum MDP-Anbieter und Fahrzeughersteller, wird

Der Datenfluss in dieser Fallstudie führt von Fahrzeug und Fahrzeugnutzer über die MDP und die Reservierungs-App hin zum Mobilitätsdiensteanbieter, hier das Parkplatzvermittlungsportal (Abbildung 10).

Da Mobilitätsdienste – wie in der exemplarischen Story – häufig ortsbasierte Dienste sind, spielen Positionsdaten (wie z. B. der Ort des Parkplatzes) eine zentrale Rolle. Je nach Mobilitätsdienst können auch Daten weiterer Kategorien anfallen – im Fall des Parkplatzvermittlungsdienstes z. B. dynamische Nutzerdaten (u. a. Zeit und Nutzungsverhalten des Fahrers) und statische Nutzerdaten (z. B. Zugangsdaten). Die Datenintensität kann nutzungsabhängig und implementierungsabhängig variieren. Im Folgenden

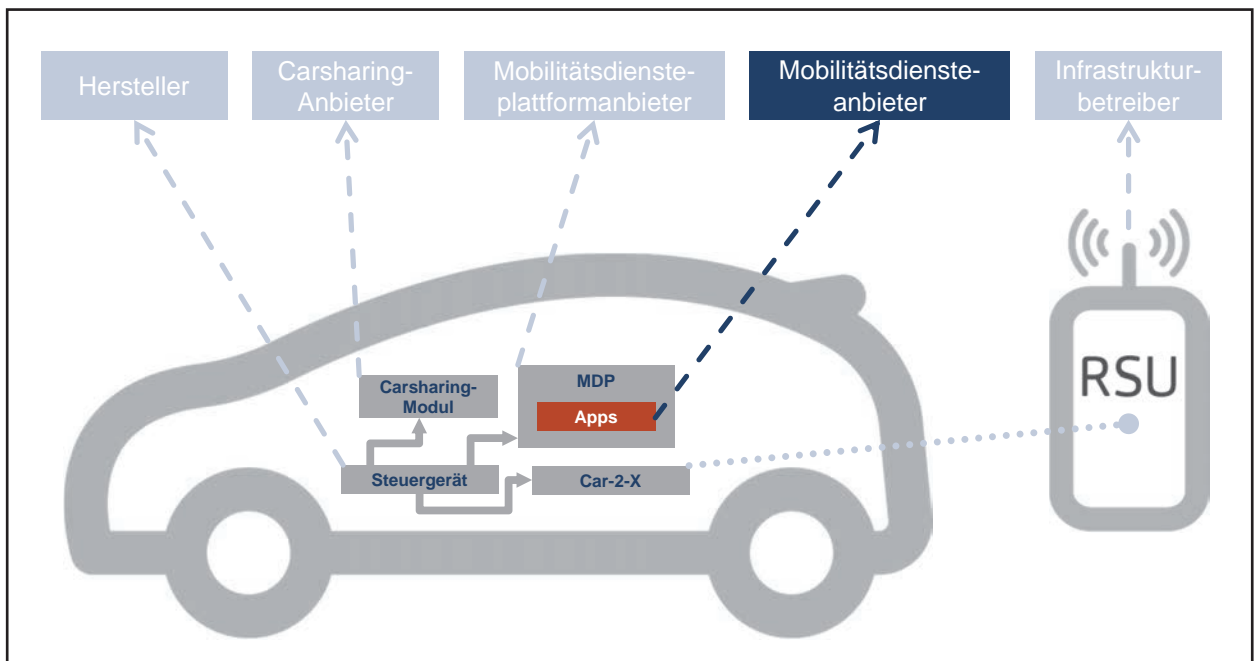


Abbildung 10: Datenflüsse der Fallstudie „Mobilitätsdienste“

werden die datenbezogenen Vorgänge der beschriebenen Story betrachtet.

2.4.1 Technische Betrachtung

Interaktion zwischen Nutzer und App

Jede Mobilitätsdienste-App wird dem Nutzer eine auf den entsprechenden Dienst zugeschnittene Bedienoberfläche anbieten, in der anwendungsbezogene Daten erfasst werden können. Da viele Mobilitätsdienste ortsbasiert sind, ist insbesondere die Erfassung des aktuellen Standortes häufig erforderlich oder kann optional zur Verbesserung des Dienstes – durch Lokalisierung – aktiviert werden.

So ist es auch im konkreten Beispiel der Parkplatzvermittlungs-App. Neben den vom Nutzer einzugebenden Daten zum gesuchten Parkplatz, wie Zeit und Datum, besonderen Merkmalen etc., wird mit der Eingabe des Ortes die Suche lokalisiert. Unterbleibt die Eingabe des Ortes, wird der aktuelle Standort des Fahrzeugs als Zielort angenommen (siehe „Datenübertragung aus Fahrzeugsystemen über die MDP zur App“).

Datenübertragung aus Fahrzeugsystemen über die MDP zur App

Prinzipiell hat keine App direkten Zugriff auf Daten des Fahrzeugs. Hier stellen sowohl die Schnittstelle zwischen

Fahrzeug und MDP als auch zwischen Plattform und App Barrieren mit definierten Zugriffsbeschränkungen dar. Während die erstgenannte Schnittstelle in Fallstudie 3 zur MDP thematisiert wird, kommt hier die Schnittstelle zwischen Plattform und den Apps neu hinzu. Diese ist plattformspezifisch und wird durch sogenannte „Application Programming Interfaces“ (APIs) definiert. APIs sind Programmierschnittstellen, welche den Apps Zugriff auf Ressourcen der Plattform ermöglichen. Dabei müssen nicht alle der Plattform zur Verfügung stehenden Daten auch zwingend den Apps zugänglich sein. Üblicherweise sind die Daten kategorisiert und jede App muss während der Installation oder beim Zugriff die Berechtigung für die jeweilige Kategorie anfordern. Je nach Plattform kann der Nutzer zudem die Zugriffsberechtigung einzeln für jede Kategorie kontrollieren und so die Rechte der App nach seinen Wünschen einschränken. Wie im Fall von Smartphone-Apps ist deren Nutzung ohne die Erteilung umfassender Zugriffsrechte auf Daten jedoch eventuell nicht möglich. Auf der MDP abgelegte Daten einer App sind prinzipiell nur für diese verfügbar. Andere Apps haben darauf keinen Zugriff.

Im Fall der lokalisierten Suchanfrage der Parkplatzvermittlungs-App sieht der Datenfluss der hierfür benötigten Positionsdaten wie folgt aus:

Zugriffsberechtigungen

Alle Computersysteme, die mehr als eine Aufgabe zur gleichen Zeit erfüllen sollen, stehen vor der Herausforderung, dass Ressourcen, die physisch nur einmal vorhanden sind, von allen diesen Aufgaben (z. B. in ihrer technischen Ausgestaltung als Prozess) gemeinsam genutzt werden müssen. Daher werden in aktuellen Computersystemen vom Mobiltelefon bis zum Supercomputer Mechanismen eingesetzt, die den Zugriff auf die Ressourcen (wie zum Beispiel den Arbeitsspeicher) regeln. Im gleichen Zuge wird auch die Trennung von Daten, die zu den jeweiligen Aufgaben (Prozessen) gehören, gewährleistet. Für Daten, die auf Massenspeichern abgelegt werden, kommen Zugriffsschutzmechanismen in Form von Lese- und Schreibberechtigungen zum Einsatz.

- Die aktuelle Fahrzeugposition wird von vielen Apps und Diensten auf der MDP genutzt und daher zentral von dieser bereitgestellt. Die Plattform hat entweder über den Fahrzeugbus Zugriff auf die aktuellen Positionsdaten des im Fahrzeug integrierten GPS-Empfängers und ruft diese regelmäßig ab oder besitzt einen eigenen GPS-Empfänger und nutzt diesen.
- Die Parkplatzvermittlungs-App hat bereits während der Installation die Rechte zur Abfrage der exakten Fahrzeugposition eingefordert und vom Nutzer bestätigt bekommen.
- Nach der Eingabe einer Suchanfrage durch den Nutzer möchte die Parkplatzvermittlungs-App die Anfrage mit der aktuellen Fahrzeugposition um einen Ort ergänzen und fragt die Daten über die plattformspezifische API ab.
- Die MDP prüft, ob die Parkplatzvermittlungs-App tatsächlich über die Rechte zum Zugriff auf Positionsdaten verfügt, und liefert den vorliegenden Wert für die Fahrzeugposition an die Parkplatzvermittlungs-App.

Datenfluss zwischen App und Mobilitätsdiensteanbieter

Mit den Daten, die von Fahrzeugnutzer und Fahrzeug bereitgestellt wurden, wird durch die App eine lokalisierte Suchanfrage an die Systeme eines Diensteanbieters vorgenommen. Technisch äquivalent zu dem Datenfluss, der in Fallstudie 3 zwischen der Wetteranwendung und dem Wetterdienst stattfindet, tritt an dieser Stelle jedoch nicht der MDP-Anbieter auch als Mobilitätsdiensteanbieter auf, sondern ein Dritter, in diesem Fall das Parkplatzvermittlungsportal. Die Anfrage der Parkplatzvermittlungs-App

wird also an die Serversysteme des Parkplatzvermittlungsportals geleitet.

Dort werden die Anfrage verarbeitet, freie Parkplätze am angefragten Standort ermittelt und an die Parkplatzvermittlungs-App zurückgeschickt. Optional können die Anfrage sowie die dabei übermittelten Daten einem Kundenprofil zugeordnet und für die weitere Verarbeitung gespeichert werden. Sollte über das Kundenprofil die Zuordnung zu einer Person möglich sein, erhalten die übermittelten Daten dadurch einen Personenbezug.

2.4.2 Ökonomische Betrachtung

Im Zentrum des Wertschöpfungsnetzwerks der Fallstudie steht der Anbieter des Parkplatzvermittlungsportals (bzw. der zugehörigen Reservierungs-App), welcher Zugriff auf die im Nutzerkonto hinterlegten persönlichen Daten, Positionsdaten des Fahrzeugs und verschiedene anwendungsbezogene Daten hat. Darüber hinaus entstehen auch bei allen anderen beteiligten Akteuren Wertschöpfungspotenziale oder ein konkreter Nutzen:

- **Nutzen MDP-Betreiber:** Die Anbieter diverser Apps wie der Parkplatzreservierungs-App sind meist als offizielle Entwickler beim MDP-Anbieter gelistet und zahlen diesem jährliche Gebühren. Durch diese Einnahmen erzielt der MDP-Betreiber Gewinn bei konstanten Kosten.
- **Nutzen Parkplatzvermittlungsportal (Reservierungs-App):** Der Anbieter des Parkplatzvermittlungsportals (bzw. der Parkplatzreservierungs-App) fungiert als Vermittler zwischen der Nachfrage- (der Parkplatzsuchende/Fahrzeugnutzer) und Angebotsseite (der Parkhaus- bzw. Parkplatzbetreiber). Durch diesen Dienst leistet er nicht nur einen wesentlichen Beitrag dazu, dass ein Geschäftsverhältnis zwischen beiden Parteien zu Stande kommt, sondern kann auch die Transaktion diesbezüglich abwickeln. Während die Nutzung der App für den Fahrzeugnutzer meist kostenfrei ist, zahlt der Parkhaus- bzw. Parkplatzbetreiber einen gewissen Anteil des Transaktionswerts an den App-Anbieter.
- **Nutzen Fahrzeugnutzer:** Durch die Nutzung der Reservierungs-App hat der Fahrzeugnutzer einen geringeren Aufwand, um sein Ziel – einen verfügbaren, kostengünstigen Parkplatz – zu erreichen. Sein Nutzen besteht neben einer größeren „Convenience“ sowohl in einem Ersparnis von Zeit, die er sonst auf die Parkplatzsuche verwendet hätte, als auch von Kosten (bspw. über einen direkten Preisvergleich des Vermittlungsportals).
- **Nutzen Allgemeinheit:** Durch die Nutzung der Reservierungs-App verringert sich die durchschnittliche Su-

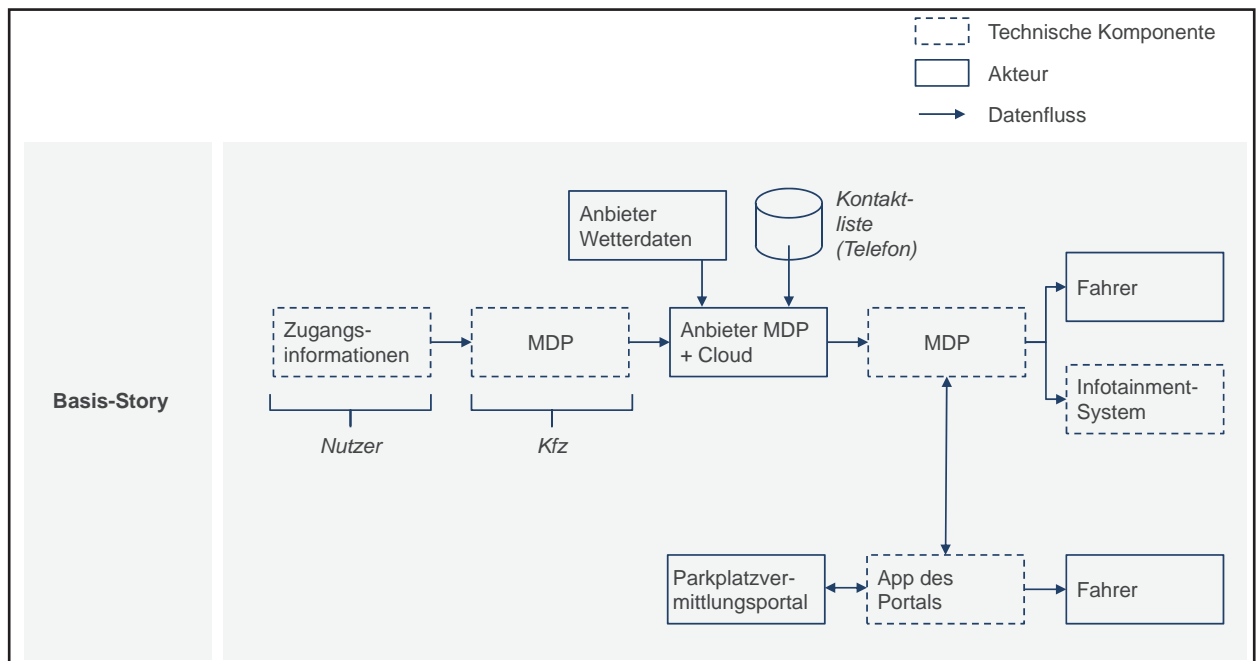


Abbildung 11: Wertschöpfungsnetzwerk der Fallstudie „Mobilitätsdienste“

che der Fahrzeugnutzer nach einem Parkplatz. Infolgedessen verringert sich das Stauaufkommen, der Verkehrsfluss wird verbessert und auch verkehrsbedingte CO₂-Emissionen werden verringert. Insgesamt entsteht ein erheblicher Nutzen für Staat und Gesellschaft im Allgemeinen.

2.5 Fallstudie 5: Car-2-Infrastructure-Kommunikation

Für die Verkehrsplanung und -optimierung ist das Wissen über die aktuellen Verkehrsflüsse relevant. Bereits seit Längerem gibt es datenverarbeitende Elektronik am Straßenrand. Z. B. werden Ampeln elektronisch geregelt, der Verkehr mit Kameras überwacht oder die Anzahl von Fahrzeugen mit Hilfe von in der Fahrbahn eingelassenen Messschleifen erfasst. Durch die Einführung von Car-2-X-Nachrichten¹⁷ können noch genauere Daten aufgezeichnet

und so ein sehr viel präziseres Lagebild als mit der bestehenden Technologie erstellt werden. Car-2-X-Kommunikation beschreibt folglich eine auf Nahbereichsfunk aufgebaute, drahtlose Verbindung zwischen Fahrzeugen sowie zwischen Fahrzeugen und fest bzw. mobil am Straßenrand installierten *Roadside-Units* (RSU), welche diese Nachrichten empfangen und aufzeichnen. Die Kommunikation erfolgt dabei ad-hoc, direkt zwischen den Teilnehmern, welche als gleichberechtigte Netzelemente auftreten. Eine spezielle Kommunikationsinfrastruktur ist nicht notwendig. Dadurch unterscheidet sich diese Fallstudie von allen vorherigen.

Car-2-X-Nachrichten werden verbindungslos an alle im Funkempfangsbereich befindlichen Teilnehmer gesendet. Je nach Nachrichtentyp geschieht dies entweder periodisch oder ereignisbezogen. Car-2-X-Kommunikation erfolgt im Wesentlichen über zwei Nachrichtentypen: *Cooperative Awareness Messages* (CAM) und *Decentralised Environmental Notification Messages* (DENM).

17 Der Oberbegriff Car-2-X-Kommunikation umfasst verschiedene Kommunikationstechniken in der Automotive- und Verkehrstechnik wie beispielsweise Car-2-Infrastructure-Communication (C2I) oder Car-2-Car-Kommunikation (C2C). Dabei geht es um die drahtlose, funkbasierte Kommunikation zwischen verschiedenen Fahrzeugen (C2C) oder zwischen Fahrzeugen und Verkehrsinfrastruktureinrichtungen wie z. B. *Roadside-Units* oder Lichtsignalanlagen.

Cooperative Awareness Messages (CAM)¹⁸ sind Statusnachrichten, durch welche die Erstellung eines aktuellen Umgebungsbildes des Fahrzeugs einschließlich anderer Verkehrsteilnehmer möglich ist. Darin übertragene Daten sind eine Identifikationsnummer (optional pseudonymisiert), der Zeitstempel, der Fahrzeugtyp, die geografische Position und Ausrichtung, Geschwindigkeit und Fahrtrichtung sowie Fahrzeugausmaße. Darüber hinaus werden Informationen bezüglich der Längsbeschleunigung, Krümmung der Fahrzeugtrajektorie und der Winkelgeschwindigkeit der Drehung um die Hochachse übertragen. Die Häufigkeit der Aussendung von CAMs variiert zwischen einer und zehn Nachrichten pro Sekunde.

Im Gegensatz zu CAMs werden **Decentralised Environmental Notification Messages (DENM)**¹⁹ dazu verwendet, gezielt auf kritische Verkehrssituationen aufmerksam zu machen, bspw. bereits geschehene Unfälle und Gefahrenstellen wie Glätte oder Verkehrsstauungen. Anders als für CAMs ist für DENMs auch eine Weiterleitung innerhalb des Car-2-X-Netzes vorgesehen, um die Informationen auch entfernten Teilnehmern zur Verfügung zu stellen.

Mit dem Lagebild der Umgebung und den Warnungen vor Gefahrensituationen lassen sich viele Anwendungsfälle für Car-2-X-Kommunikation implementieren. Diese können der Verbesserung des Verkehrsflusses, der Erhöhung der Verkehrssicherheit oder der Reduktion von Emissionen dienen.

In dieser Studie wird eine Anwendung, bei der Car-2-Infrastructure-Daten von der Verkehrsinfrastruktur gesammelt und weiterverarbeitet werden, exemplarisch betrachtet:

Während der Fahrt mit ihrem LKW fährt Frau Musterfrau über eine Brücke und passiert dabei eine Roadside-Unit des Landesbetriebs Straßenbau, die alle Car-2-X-Nachrichten aufzeichnet und zur Verkehrszentrale des Landesbetriebs überträgt.

Die zentralen Akteure dieser Fallstudie sind der Fahrer (zugleich Fahrzeugeigentümer und Fahrzeughalter) und der Infrastrukturbetreiber, welcher die RSU aufstellt und betreibt, wie hier der zuständige Landesbetrieb Straßenbau. Damit treten hier erstmals staatliche Akteure in den Mittel-

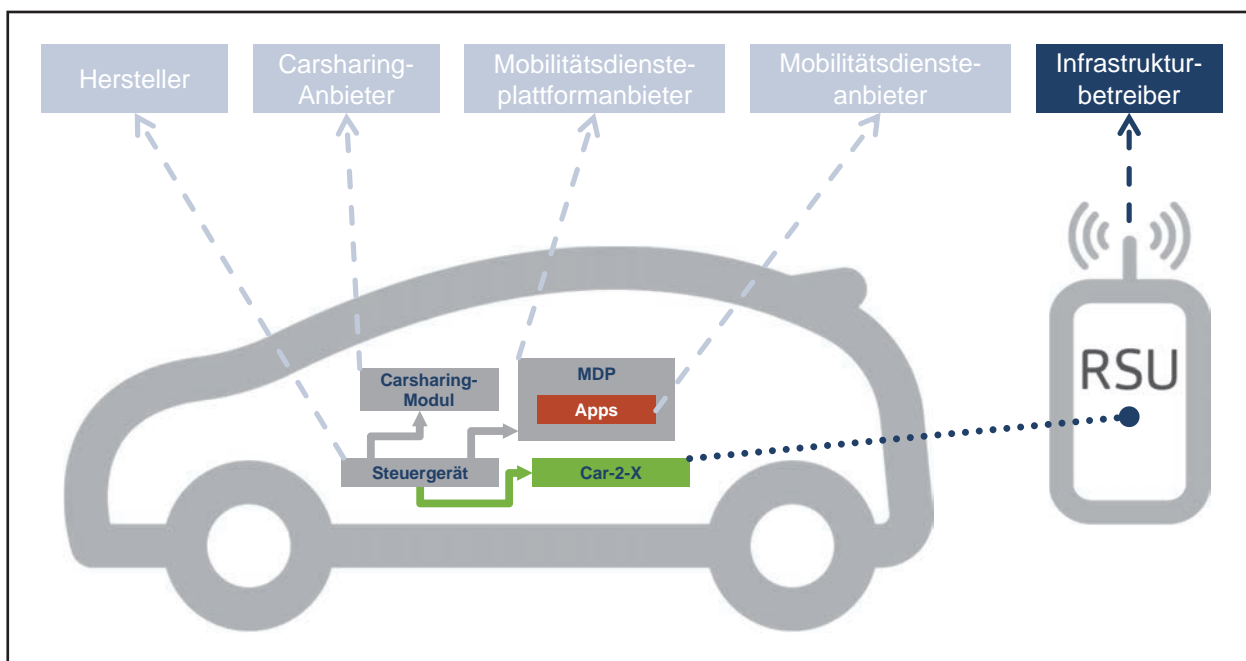


Abbildung 12: Datenflüsse der Fallstudie „Car-2-Infrastructure-Kommunikation“

¹⁸ Spezifiziert in ETSI EN 302 637-2 V1.3.2 (2014-11).

¹⁹ Spezifiziert in ETSI EN 302 637-3 V1.2.2 (2014-11).

punkt. Weitere Akteure sind der Fahrzeughersteller, der das Car-2-X-Kommunikationssystem im Fahrzeug verbaut hat, und die Verkehrszentrale, welche die gesammelten Car-2-X-Nachrichten erhält und weiterverarbeitet.

Im Fokus dieser Fallstudie stehen statische (z. B. Länge und Breite des LKWs) und dynamische Fahrzeugdaten (z. B. Sensormesswerte), welche regelmäßig in Form von Car-2-X-Nachrichten (CAM und DENM) ausgesendet werden, sowie Verkehrslagedaten (z. B. Verkehrsauslastung).

2.5.1 Technische Betrachtung

Aussenden von Car-2-X-Nachrichten durch das Fahrzeug

Das vom Hersteller fest in den LKW verbaute Car-2-X-Kommunikationssystem bezieht während der Fahrt Daten von anderen Steuergeräten im Fahrzeug und sendet regelmäßig Positions- und Statusinformationen des LKWs in unverschlüsselten Car-2-X-Nachrichten (CAM und DENM) im 5,9 GHz-Band (IEEE 802.11) aus.

Um einen Missbrauch durch Aussenden falscher Nachrichten zu verhindern, werden alle Nachrichten digital signiert und mit einem gültigen Zugangszertifikat versehen. Da diese Signaturen eine permanente, eindeutige Zuordnung von Nachrichten mit ihrem Inhalt, wie z. B. der Position, zu einer eindeutigen ID – dem Zertifikat – ermöglichen würden, verfügen die Fahrzeuge über eine große Menge von Zugangszertifikaten, die jeweils nur einen kurzen Gültigkeitszeitraum besitzen und in schneller Folge gewechselt werden können. So ist die nachträgliche Zuordnung von Daten eines Absenders, die mit verschiedenen Zugangszertifikaten signiert wurden, zueinander nicht möglich (Nicht-verkettbarkeit). Da eine Zuordnung der Zertifikate (sowie damit signierter Daten) zum sendenden Fahrzeug (oder gar zum Fahrer oder Fahrzeughalter) nur im Ausnahmefall durch die ausstellenden Behörden möglich ist, ermöglicht die Verwendung dieser Zugangszertifikate eine Pseudonymisierung der betroffenen Daten.

Empfang und Speicherung von Car-2-X-Daten durch den Infrastrukturbetreiber und Dritte

Die durch die fest in den LKWs verbauten Car-2-X-Kommunikationssysteme ausgesendeten Car-2-X-Nachrichten aller Verkehrsteilnehmer können von der *Roadside-Unit* des Landesbetriebs Straßenbau (Infrastrukturbetreiber) empfangen und gespeichert werden. Die Daten werden in einer Umfeldtabelle zu einem präzisen Bild des aktuellen

Verkehrsgeschehens in der näheren Umgebung der RSU zusammengeführt. Durch regelmäßiges Eintreffen neuer Nachrichten der umgebenden Fahrzeuge kann die Umfeldtabelle dynamisch angepasst werden und so immer ein aktuelles Verkehrslagebild widerspiegeln²⁰. Die ausgesendeten Nachrichten und die darin enthaltenen Daten (statische und dynamische Fahrzeugdaten) können neben der in der Story beschriebenen RSU von allen erreichbaren Empfängern in der Umgebung empfangen werden. Der Absender hat also keinen Einfluss darauf, wer die ausgesendeten Daten empfängt und verarbeitet. Umgekehrt sind die Daten für jeden Empfänger in Sendereichweite frei zugänglich und nutzbar.

Transfer aufgezeichneter Car-2-X-Daten zur Verkehrszentrale

Eine einzelne RSU kann – entsprechend der Sendereichweite der sendenden Fahrzeuge – nur Daten aus ihrer näheren Umgebung empfangen. Für ein umfassendes Bild eines größeren Gebiets müssen also die Daten mehrerer RSU zusammengeführt werden.

Aus diesem Grund werden die in der RSU aufgezeichneten Daten häufig zur Verkehrszentrale gesendet. Je größer und dichter das RSU-Netzwerk dabei ist, umso besser kann in der Verkehrszentrale ein detailliertes Verkehrslagebild auf Grundlage der gesammelten CAM-Nachrichten erstellt werden. Insgesamt geht es dabei um die Erfassung des Verkehrs vor und auf Brücken, um deren Auslastung und Verwendung durch Schwerlastverkehr zu erfassen.

Das RSU-Netzwerk kann auf verschiedene Art und Weise mit der Verkehrszentrale verbunden sein – z. B. über dedizierte Datenleitungen, eine Anbindung per Richtfunk oder über bestehende Mobilfunknetze. In der Verkehrszentrale können dann alle Daten aggregiert werden.

In der Anfangsphase der Einführung von Car-2-X-Kommunikation werden nur wenige Fahrzeuge Car-2-X-Nachrichten aussenden. Daher ist davon auszugehen, dass in der Übergangszeit eine Anreicherung der empfangenen Daten mit zusätzlicher Sensorik in den RSU, wie z. B. Schleifendaten, sinnvoll ist.

2.5.2 Ökonomische Betrachtung

Wertschöpfungs- und Nutzenpotenziale ergeben sich in dieser Fallstudie vor allem durch die Verarbeitung und weitere Nutzung der Car-2-X-Nachrichten durch die Ver-

20 Neben den passiven Anwendungsfällen können RSUs auch als Sender auftreten, um z. B. Warnungen vor Gefahrenstellen als DENMs oder in Verbindung mit Lichtsignalanlagen, Kreuzungsgeometrien und entsprechende Ampelphasen per Car-2-X zu verbreiten.

kehrszentrale – z. B. zur Steuerung von Wechselverkehrszeichen, die Fahrer informieren bzw. beeinflussen. In einem möglichen Erweiterungsfall ist darüber hinaus die weitere Verwendung der Daten über ein *Open-Data*-Portal denkbar. Im Detail:

- **Nutzen Verkehrszentrale:** Die RSU leiten die pseudonymisierten Daten an die/eine Verkehrszentrale weiter. Letztere kann die erhaltenen Daten bündeln und nach Verarbeitung einen Nutzen daraus ziehen, da ein sehr präzises Bild über die Verkehrssituation im Allgemeinen und auch über spezielle Situationen (z. B. Gefährdung bei starkem Wind durch wenig beladene LKWs auf Brücken) möglich wird. Auf Basis der lokalen Umfeldtabelle, die die RSU aus den empfangenen Daten erstellt, können verschiedene verkehrliche Anwendungsfälle umgesetzt werden. So können z. B. Ampelphasen dynamisch geregelt werden, um dem öffentlichen Nahverkehr oder dem Schwerlastverkehr eine Priorisierung zu erteilen, oder den Fahrzeugen kann eine Geschwindigkeitsempfehlung für die „grüne Welle“ gegeben werden.
- **Nutzen Fahrer/individuelle Verkehrsteilnehmer:** Die Verkehrszentrale kann eingreifen, indem auf Basis der gewonnenen Informationen Verkehrslenkungsmaßnahmen ausgelöst werden, die entweder den Verkehrsfluss im Allgemeinen beeinflussen (z. B. durch eine Geschwindigkeitsreduktion oder individuelle Umleitungen) oder die im Einzelfall den Verkehrsfluss stoppen, um Gefährdungen zu unterbinden (z. B. bei Höhenkontrollen).
- **Nutzen Unternehmen/Zivilgesellschaft:** Eine mögliche Erweiterung der Fallstudie besteht in der Weiterleitung geeigneter anonymisierter oder pseudonymisierter Daten an ein *Open-Data*-Portal, auf dem die Daten für interessierte Parteien kostenfrei bereitgestellt werden. Neben der Nutzung durch die öffentliche Hand könnten somit auch Unternehmen diese Daten nutzen – beispielsweise für die Entwicklung diverser Dienste wie einer Navigations-App für die Routenplanung bei Verkehrsstörungen. In diesem Fall können Verkehrsdaten monetarisiert werden. Auch für interessierte Akteure der Zivilgesellschaft sind Anwendungen denkbar.

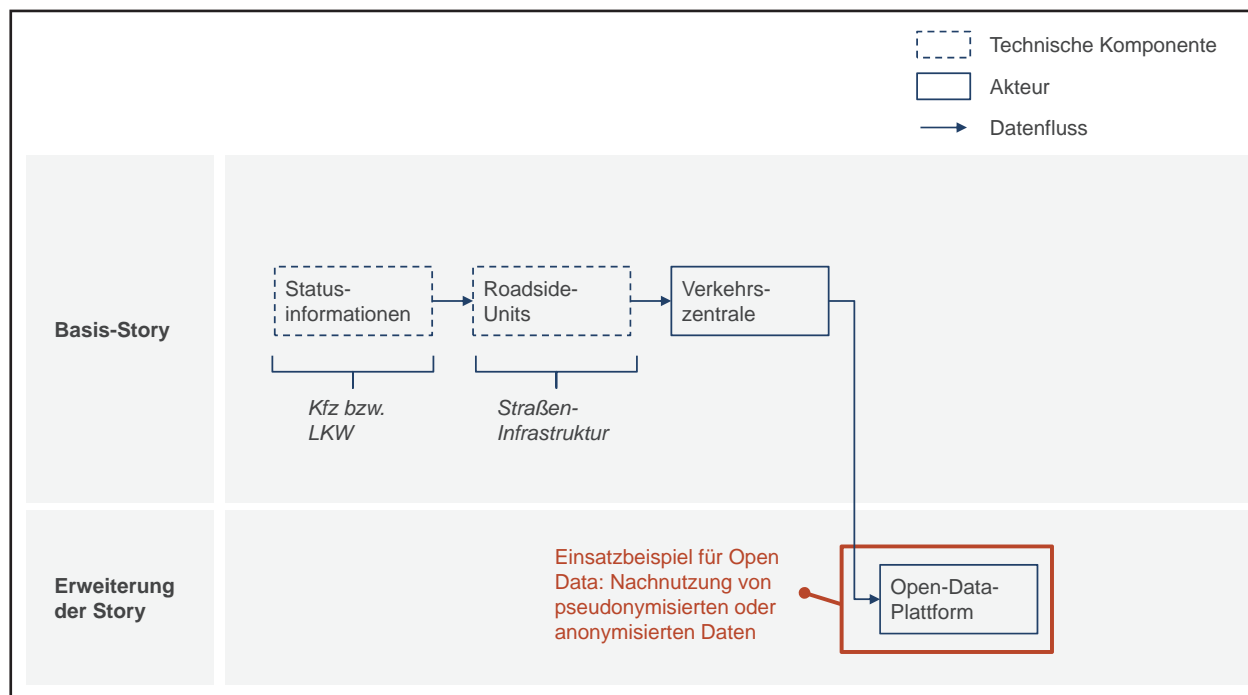


Abbildung 13: Wertschöpfungsnetzwerk der Fallstudie „Car-2-Infrastructure-Kommunikation“

2.6 Ergebnis: Fallstudien „digitale Mobilität“

Die Ausführungen zu den Fallstudien zeigen, dass in jedem der fünf Mobilitätskontexte eine Vielzahl von Datenerstellungs-, Datenübermittlungs- und Datennutzungsvorgängen für die Erbringung des jeweiligen Mobilitätsdienstes notwendig ist. Die Zugriffsmöglichkeiten der beteiligten Akteure sind komplex und meist von der konkreten technischen Ausgestaltung des Dienstes abhängig. Insgesamt zeigt die Betrachtung, dass durch alle skizzierten Datenströme

ein ökonomischer Mehrwert generiert werden kann, wobei die Zugriffsmöglichkeiten der involvierten Akteure von zentraler Bedeutung für die wirtschaftliche Nutzung der erstellten Daten sind. Datennutzungen und -nachnutzungen erfolgen auf unterschiedliche Art und Weise sowohl mit als auch ohne Mobilitätsbezug und eröffnen vielfältige Wertschöpfungspotenziale für die beteiligten Akteure. Um die Frage nach den rechtmäßigen Verfügungsberechtigungen für die Nutzung der erstellten Daten zu beantworten, folgt in Kapitel 3 eine Untersuchung der beschriebenen Szenarien auf Basis bestehender Regelungen in verschiedenen Rechtsgebieten.

3 Rechtliche Erfassung des „Dateneigentums“ im geltenden Recht (*de lege lata*)

Die Klärung der Frage nach einer eigentumsrechtlichen Zuordnung von Daten im geltenden Recht bedarf einer Untersuchung des Rechtsrahmens für die Erstellung, Übermittlung und Nutzung von Daten anhand von konkreten Anwendungsbeispielen. Die Untersuchung im folgenden Kapitel erfolgt daher auf Basis der zuvor detaillierten Fallstudien. Von den beschriebenen technischen und ökonomischen Vorgängen (siehe Kapitel 2) wurden folgende, aus rechtlicher Perspektive relevanten Datenerstellungs-, -übermittlungs-, sowie -nutzungsvorgänge identifiziert und als Basis für die rechtliche Analyse extrahiert (Abbildung 14).

Für diese datenbezogenen Vorgänge gilt es zunächst zu betrachten, ob das geltende Recht (*de lege lata*) **eine dem (Sach-)Eigentum vergleichbare Zuordnung** zu einer indi-

vidualisierbaren natürlichen oder juristischen Person bereithält. Wäre dies der Fall, könnte die rechtliche und ökonomische Bewertung der technischen Möglichkeiten im Mobilitätssektor auf einer solchen eindeutigen Zuordnung aufbauen und helfen, das ökonomische Potenzial weiter zu heben. Sollte das geltende Recht keine solche Zuordnung treffen, rückt die Schaffung eines **Dateneigentums** – zunächst verstanden ohne eine konkrete Aussage über dessen Ausgestaltung und Reichweite²¹ – in den Mittelpunkt der Diskussion. Daher wird bei der folgenden Analyse diese Ebene als Ausgangspunkt aller weiteren Überlegungen zum Dateneigentum betrachtet. Im Rahmen der Zuordnung von Daten zu einem Berechtigten lassen sich drei Ebenen entsprechend der nach Reichweite und Wirkung unterschiedlichen Rechte an Daten differenzieren (Abbildung 15).

Fallstudie 1: Kfz-Instandhaltung und -Wartung
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten
Fallstudie 2: Carsharing
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter
Fallstudie 3: Mobilitätsdienstplattform
3a) Eingabe von Daten in die Mobilitätsdienstplattform und Synchronisierung mit der Cloud des MDP-Anbieters
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstplattform und deren Anbieter
3c) Transfer von Daten aus der Mobilitätsdienstplattform zum Fahrzeugsystem
Fallstudie 4: Mobilitätsdienste
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)
4b) Transfer von Daten aus Fahrzeugsystemen (über die MDP) zum Mobilitätsdienst und dessen Anbieter
Fallstudie 5: Car-2-Infrastructure-Kommunikation
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte

Abbildung 14: Übersicht datenbezogener Vorgänge in Fallstudien 1 bis 5

21 Der Begriff „Dateneigentum“ wird daher zunächst beschreibend für eine rechtliche Zuordnung zu einem Verfügungsberechtigten verwendet. Ob diese Verfügungsberechtigung dem Sacheigentum entspricht, in Anlehnung an das Urheberrecht oder andere Immaterialgüterrechte oder als Leistungsschutzrecht ausgestaltet ist bzw. werden sollte, ist davon zunächst zu trennen; siehe dazu 5.1.

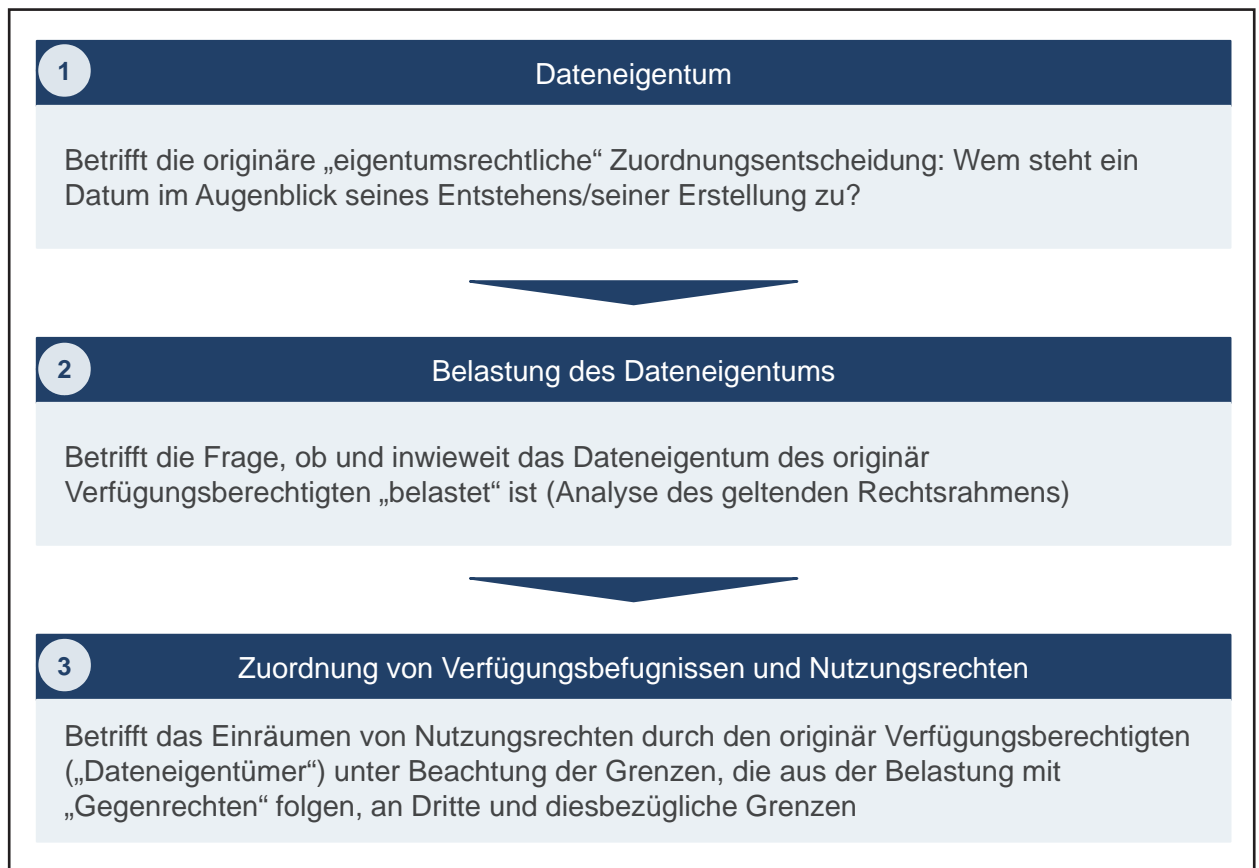


Abbildung 15: Ebenenmodell

Auf der **ersten Ebene** ist eine umfassende Zuordnung eines Datums zu einem Rechtssubjekt mit der Folge umfassender Befugnisse an dem Rechtsobjekt gegenüber jedermann denkbar und zu betrachten. Auf der **zweiten Ebene** existieren zugunsten einzelner Dritter bzw. der Allgemeinheit Einschränkungen, die auch gegenüber einem umfassenden Ausschließlichkeitsrecht Geltung beanspruchen bzw. beanspruchen würden (Beispiel: datenschutzrechtliche Positionen Dritter als „Belastung“). In rechtlicher Hinsicht wäre ggf. ein ausdifferenziertes System an Schrankenbestimmungen zur Absicherung der Nutzung des Datums durch andere Rechtssubjekte zu entwickeln. Neben den gesetzlichen Nutzungsrechten Dritter ist auf der **dritten Ebene** die vertragliche Einräumung von Nutzungsrechten durch den originär Berechtigten und die Reichweite seiner Verfügungsbefugnis zu betrachten.

Gegenstand dieser Studie ist primär die erste Ebene, also die **Frage**, ob ein **umfassendes Ausschließlichkeitsrecht** an Daten bereits existiert (dazu sogleich) und – falls dies nicht der Fall sein sollte – ob die Schaffung eines umfassenden Ausschließlichkeitsrechts an Daten vorteilhaft sein kann und welchem Rechtssubjekt dieses Recht zugewiesen werden sollte (siehe Kapitel 5.1.).

Die **zweite und dritte Ebene** können im Rahmen dieser Studie nur angedeutet werden. Sicher ist, dass dabei die ermittelten bereichsspezifischen Regelungen aufgrund des verfassungsrechtlich gebotenen Schutzes der Persönlichkeit der von Datenverarbeitung Betroffenen weiterhin Geltung beanspruchen müssen. Darüber hinaus sind bei der Normierung eines Ausschließlichkeitsrechts insbesondere datenschutzrechtliche Vorschriften zwingend auf der zweiten Ebene als Belastung des Ausschließlichkeitsrechts zu berücksichtigen. Dabei besteht selbstverständlich weiterhin die Möglichkeit der Anonymisierung personenbezogener Daten, die zu einem Wegfall der Einschränkungen in der Nutzung des Datums durch das Datenschutzrecht führen würde.

3.1 Hintergrund: Verfassungsrechtlicher Schutz von Daten

Bevor untersucht werden soll, inwieweit sich auf einfachgesetzlicher Ebene Hinweise auf ein Dateneigentum finden lassen (dazu unter 3.2), soll zunächst der verfassungsrechtliche Schutz von Daten dargestellt werden.

Festzustellen ist dabei zunächst, dass die Grundrechte selbst keine Zuordnung von Eigentum vornehmen, sondern aufgrund ihres primär abwehrrechtlichen Charakters allenfalls bestehende Rechtspositionen vor (unberechtigten) staatlichen²² Eingriffen schützen. Daher stellt sich die Frage, auf welche Grundrechte sich Grundrechtsträger berufen können, wenn in „ihre“ Daten eingegriffen wird.

Naheliegender erscheint es, die **Eigentumsgarantie aus Art. 14 GG** heranzuziehen. Voraussetzung für die Eröffnung des sachlichen Schutzbereiches wäre, dass Daten eigen-tumsfähig im verfassungsrechtlichen Sinne sind. Zu den schutzfähigen Rechtspositionen von Art. 14 GG gehören alle vermögenswerten Rechte, die das bürgerliche Recht einem privaten Rechtsträger als Eigentum zuordnet²³, die durch privatrechtliche Normen dem Einzelnen so „zugeordnet sind, dass er die damit verbundenen Befugnisse nach eigenverantwortlicher Entscheidung zu seinem privaten Nutzen ausüben darf“²⁴. Geschützt werden von Art. 14 GG damit zunächst physische Datenträger, auf denen die hier in Rede stehenden Daten gespeichert sein können.

Der verfassungsrechtliche Eigentumsbegriff beschränkt sich jedoch nicht auf das Sacheigentum nach bürgerlichem Recht, sondern geht darüber hinaus und erfasst auch andere vermögenswerte Rechte²⁵. Die physische Verkörperung von Daten auf Datenträgern ist daher für den Schutz von Art. 14 GG nicht zwingend. Grundrechtlichen Schutz können bspw. auch **Betriebs- und Geschäftsgeheimnisse** genießen, die ebenfalls in Form von Daten vorliegen können. Zu denken ist im vorliegenden Zusammenhang vor allem an Betriebs- und Geschäftsgeheimnisse von Fahrzeugherstellern oder Anbietern innovativer Mobilitätsdienste. Soweit man neben der primär einschlägigen Berufsfreiheit gemäß Art. 12 GG in diesen Fällen ergänzend auch Art. 14 GG als einschlägig erachtet²⁶, ist darauf hinzuweisen, dass nicht alle fahrzeugbezogenen Daten Betriebs- und Geschäftsgeheimnisse darstellen²⁷. Denn neben dem

Bezug zum Unternehmen und dem Gemeincharakter ist hierzu erforderlich, dass der Unternehmer ein berechtigtes wirtschaftliches Interesse an der Geheimhaltung der Informationen hat. Dies wird auf einen Teil der im Fahrzeug anfallenden Daten zutreffen (bspw. zur Funktionsweise bestimmter Sicherheitssysteme), nicht aber auf Daten zu Position, Tankfüllstand, Wetter oder eingestelltem Radiosender.

Geschützt werden Betroffene von Datenerhebungen zudem durch das **Recht auf informationelle Selbstbestimmung**, welches das Bundesverfassungsgericht bereits 1983²⁸ aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) abgeleitet hat. Eingriffe in dieses Recht sind im überwiegenden Allgemeininteresse zulässig, erfordern aber eine normenklare gesetzliche Grundlage, die dem Grundsatz der Verhältnismäßigkeit entsprechen muss. Dies hat das BVerfG im Bereich staatlicher Überwachung immer wieder im Detail formuliert; zuletzt mit der Entscheidung zur Kfz-Kennzeichenüberwachung²⁹ auch im Automobilbereich. Voraussetzung für die Eröffnung des Schutzbereiches ist jedoch stets, dass es sich um personenbezogene Daten handelt³⁰. Bei nicht-personenbezogenen Daten bietet das Recht auf informationelle Selbstbestimmung dagegen keinen Schutz.

Gleiches gilt für das **Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**, welches das Bundesverfassungsrecht ebenfalls aus dem allgemeinen Persönlichkeitsrecht geschöpft hat³¹. Dieses schützt vor der Infiltration eigengenutzter informationstechnischer Systeme, welche heute oft in modernen Autos verbaut werden³². Dieses Recht tritt mit seiner lückenschließenden Funktion jedoch hinter das Recht auf informationelle Selbstbestimmung zurück und kommt nur dann zur Anwendung, wenn das Recht auf informationelle Selbstbestimmung keinen hinreichenden Schutz bietet. Dies ist etwa bei einer (ausschließlichen) Infiltration des

22 Aufgrund dieser Funktion der Grundrechte würde ein verfassungsrechtliches Dateneigentum zunächst nur vor staatlichen Maßnahmen schützen. Ein privatrechtliches Verfügungsrecht und ein Schutzrecht gegenüber anderen Privaten wäre Folge der mittelbaren Drittwirkung und seitens des Gesetzgebers aufgrund der Schutzpflichtdimension der Grundrechte im Zivilrecht nachzuvollziehen.

23 BVerfGE 70, 191 (199).

24 BVerfGE 112, 93 (107); 97, 350 (371); 123, 186 (258).

25 *Wendt*, in: *Sachs* (Hrsg.), GG, 7. Aufl. 2014, Art. 14 Rn. 22. Diese Eigenschaft des Art. 14 GG (normgeprägter Schutzbereich) bedeutet auch, dass für den Fall, dass das einfache (bürgerliche) Recht eine Zuordnung von Daten zu einem Verfügungsberechtigten vornimmt (im Sinne eines Dateneigentums), diese Entscheidung zugleich zum verfassungsrechtlichen Schutz über Art. 14 GG führt.

26 Offengelassen von BVerfGE 115, 205 (248); ablehnend z. B. *Wolff*, NJW 1997, 98 ff.; siehe aber *Beyerbach*, Die geheime Unternehmensinformation, 2012, S. 210 f.

27 Siehe dazu *Hornung*, DuD 2015, 359 (362); ausführlich dazu auch unter 3.2.4.

28 BVerfGE 65, 1 ff.; zur Innovationsgeschichte *Hornung*, Grundrechtsinnovationen, 2015, S. 266 ff.

29 Dazu BVerfGE 120, 378 ff.

30 Siehe vor allem unter 3.1.2.

31 BVerfGE 120, 274 ff.

32 Denkbar erscheint es auch, Fahrzeuge selbst als informationstechnisches System anzusehen.

Systems der Fall. Werden jedoch in Folge der Infiltration anschließend Daten erhoben, ist nach wie vor der Schutzbereich des Rechts auf informationelle Selbstbestimmung betroffen und das IT-Grundrecht tritt zurück³³.

Das in **Art. 10 Abs. 1 GG** gewährleistete **Fernmeldegeheimnis** sichert die freie Entfaltung der Persönlichkeit durch einen privaten Austausch von Informationen³⁴. Aufgrund der Entwicklungsoffenheit des Grundrechts ist nicht nur die Kommunikation mittels traditioneller Medien erfasst, sondern jegliche Kommunikation mittels der verfügbaren Telekommunikationstechniken³⁵. Telefonate über Festnetz und Mobiltelefone fallen genauso in den Schutzbereich wie SMS, MMS und E-Mails³⁶. Beschränkt wird der durch Art. 10 GG gewährte Schutz jedoch durch die Eingrenzung auf Inhalte und Umstände der laufenden Kommunikation. Nicht erfasst sind solche Inhalte und Umstände, die sich nach Abschluss des Kommunikationsvorganges im Herrschaftsbereich des Nutzers befinden³⁷. Zudem trifft Art. 10 GG ebenfalls keine Zuordnungsentscheidung, sondern erschöpft sich insoweit in der Gewährleistung des Vertrauensschutzes der Kommunikation³⁸.

In Bezug auf die **Fallstudien** folgt daraus, dass die in den dargestellten Situationen anfallenden Daten keinem der Betroffenen verfassungsrechtlich im Sinne eines Dateneigentums zugeordnet sind. Vielmehr können sich die Beteiligten bei einer Erhebung und Verarbeitung von **personenbezogenen** Daten vor allem auf den Schutz des Rechts auf informationelle Selbstbestimmung berufen. Dies ist aber nicht bei allen anfallenden Daten der Fall (wie etwa Temperaturdaten oder die Verschleißanzeige der Bremsen), sofern bei der verantwortlichen Stelle bzw. beim Empfänger nicht weitere Daten vorliegen, durch deren Verknüpfung ein Personenbezug herstellbar wird³⁹. Soweit es sich um laufende Kommunikation handelt, greift zudem der Schutz des Fernmeldegeheimnisses des Art. 10 Abs. 1 GG.

Zu beachten ist in den Fallstudien 1 bis 4 jedoch zudem, dass ausschließlich Private beteiligt sind. Da die Grundrechte primär Schutz vor staatlichen Eingriffen gewähren, ist insoweit auf die sog. mittelbare Drittwirkung der Grundrechte zurückzugreifen. Von **mittelbarer Drittwirkung** spricht man, wenn sich die Schutzwirkung eines Grundrechts nur mittelbar über eine Generalklausel entfaltet. Die Schutzwirkung tritt in diesen Fällen ein, weil bei Auslegung von Generalklauseln, wie z. B. § 242 BGB, die durch das Grundgesetz etablierte objektive Werteordnung zu berücksichtigen ist. In Fallstudie 5 findet hingegen eine Datenerhebung unmittelbar durch eine staatliche Stelle statt, so dass ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegen kann, soweit die Daten, die an die *Roadside-Unit* übermittelt werden, einen Personenbezug aufweisen, was in der Regel nicht der Fall sein wird. Anderenfalls führt dies aus verfassungsrechtlichen Gründen dazu, dass entweder eine gesetzliche Erlaubnis oder eine Einwilligung des Betroffenen zur Datenerhebung vorliegen muss⁴⁰ (für eine detaillierte Untersuchung aller Fallstudien, siehe Anhang II.i.).

Festzuhalten ist somit, dass sich aus den Grundrechten zum Teil **negative Abwehrrechte** in Bezug auf unzulässige Eingriffe ergeben (insbesondere aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Jedoch schützten sowohl das Recht auf informationelle Selbstbestimmung als auch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nur soweit es um **personenbezogene** Daten geht⁴¹. Zudem schützen die Grundrechte primär als Abwehrrechte zunächst vor allem vor Eingriffen des Staates. Erfolgt der Eingriff dagegen durch andere Private, ist ein Schutz allenfalls über die sog. mittelbare Drittwirkung möglich. Durch das Verfassungsrecht wird zudem **keine umfassende positive Verfügungsbefugnis** über Daten statuiert. Denkbar ist es allenfalls, dass bestimmte Datenbestände durch Art. 14 GG geschützt werden, soweit es sich

33 So zutreffend *Hoffmann-Riem*, JZ 2008, 1009 (1019), wenngleich das Verhältnis beider Ausprägungen des Allgemeinen Persönlichkeitsrechts als schwierig angesehen wird, vgl. dazu etwa *Britz*, DÖV 2008, 411 (413 f.); *Eifert*, NVwZ 2008, 521 (522); *Kutscha*, NJW 2008, 1042 (1043). Für eine Änderung des Verhältnisses beider Grundrechte vgl. *Hoffmann*, Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes, S. 129 ff.

34 BVerfGE 67, 157 (171); 106, 28 (35 f.); 110, 33 (53); 124, 43 (54).

35 BVerfGE 46, 120 (144); 115, 166 (182).

36 BVerfGE 113, 348 (383); 120, 274 (307); *Pagenkopf*, in: Sachs (Hrsg.), GG, Art. 10, Rn. 14; *Grote*, KritV 1999, 27 (39 f.); *Gurlit*, NJW 2010, 1035 (1036); vgl. zu der Veränderung der technischen und sozialen Bedingungen des durch Art. 10 GG gewährleisteten Schutzes *Albers*, DVBl. 2010, 1061 (1064).

37 BVerfGE 115, 166 (183 ff.); 120, 274 (307 f.).

38 BVerfGE 115, 166 (183 ff.); 120, 274 (307 f.).

39 Siehe hierzu unter Anhang II.i.

40 Siehe zum insoweit vorliegenden Gleichlauf mit dem einfachen (Datenschutz-)Recht unter Kapitel 3.2.1.

41 Das BVerfGE fordert in seinen Ausführungen ausdrücklich das Vorhandensein von personenbezogenen Daten, da nur durch Erhebung dieser Daten Persönlichkeitsgefährdungen entstehen können, vgl. BVerfGE 120, 274 (314): Den erhöhten Grundrechtsschutz sollen Systeme erfahren, »[...] die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten«.

um Geschäft- und Betriebsgeheimnisse handelt. Dies wird bei den hier in Rede stehenden Daten jedoch nur selten der Fall sein⁴².

3.2 Bereichsspezifische Zuordnung von Daten im (einfachen) geltenden Recht

Im Folgenden soll untersucht werden, ob im einfachen Recht bereits *de lege lata* bereichsspezifische Regelungen die Daten aus den gezeigten Fallstudien einem der Akteure zuweisen. Hierzu werden die folgenden Normkomplexe näher betrachtet:

- Datenschutzrecht,
- Urheberrecht,
- Strafrecht,
- Lauterkeitsrecht (Schutz von Betriebs- und Geschäftsgeheimnissen),
- allgemeines Zivilrecht.

Dies erfolgt einerseits unter dem Blickwinkel des Dateneigentums, also inwieweit eine Verfügungsberechtigung begründet und wem diese zugeordnet wird, andererseits in Orientierung an die relevanten datenbezogenen Vorgänge der Fallstudien⁴³. Zu untersuchen ist, ob die analysierten Regelungsbereiche eine Zuordnungsentscheidung enthalten bzw. voraussetzen. Bei diesen bereichsspezifischen Regelungen werden vornehmlich Ansätze untersucht, die Daten einer Person zuordnen bzw. den positiven Umgang eines Rechtssubjekts mit einem betreffenden Datum schützen. Sofern keine anderweitigen Belastungen vorliegen, folgt aus der jeweiligen Verfügungsberechtigung das Recht, die Daten ökonomisch frei zu nutzen und zu verwerten sowie daraus Wertschöpfung zu generieren.

Zu berücksichtigen ist bei der Analyse, dass es sich bei den meisten Vorschriften – so wie exemplarisch auch bei der Kernvorschrift des § 903 BGB für das Sacheigentum – um „Konsequenzvorschriften“ handelt, die Rechtsfolgen in

den Mittelpunkt rücken und eine Zuordnung voraussetzen bzw. zugleich enthalten (bzw. enthalten müssen, um ihren Zweck zu erfüllen).

3.2.1 Datenschutzrecht

Das Datenschutzrecht befindet sich derzeit in einem Umbruch. Nach mehrjähriger Reformdiskussion wurde im Frühjahr 2016 die **Europäische Datenschutz-Grundverordnung** (sowie eine Richtlinie für den Sicherheitsbereich) verabschiedet, die ab dem 25. Mai 2018 Anwendung findet⁴⁴. Sie enthält erhebliche Neuerungen in vielen Bereichen des materiellen sowie des Verfahrensrechts und ändert durch den Wechsel auf eine Verordnung grundlegend die Anwendungsbedingungen des Datenschutzrechts in Europa. Eine Aussage zu einem Dateneigentum oder zu spezifischen Nutzungsbefugnissen von Automobildaten enthält die neue Verordnung jedoch nicht. Überdies bleiben die – hier vor allem relevanten – Grundprinzipien des Datenschutzrechts im Wesentlichen gültig.

Datenschutzrecht existiert auf einer verfassungsrechtlichen und einer einfachgesetzlichen Ebene. Neben den deutschen Grundrechten (siehe Kapitel 3.1) wird es durch die Europäisierung zunehmend auf die Art. 7, 8 der Europäischen Grundrechtecharta und Art. 8 der Europäischen Menschenrechtskonvention ankommen. Diese gewährleisten neben dem allgemeinen Recht auf Achtung von Privat- und Familienleben, Wohnung und Kommunikation (Art. 7 GRC, Art. 8 EMRK) auch ein explizites Recht auf Schutz personenbezogener Daten (Art. 8 GRC). Diese Grundrechte sind in der Rechtsprechung der europäischen Gerichte konkretisiert worden⁴⁵. Die dogmatische Konzeption unterscheidet sich dabei zwar vom deutschen Recht auf informationelle Selbstbestimmung, auf der Rechtfertigungsebene (Verhältnismäßigkeitsprüfung) bestehen aber weitgehend ähnliche Anforderungen, auch wenn diese Prüfung im Einzelfall unterschiedlich ausfallen mag.

Einfachgesetzlich besteht im Datenschutzrecht bis zur Anwendung der Datenschutz-Grundverordnung eine Art „Grundregulierung“ durch das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sowie bereichsspezifische Vorgaben in einer Vielzahl von **Spezialgesetzen** etwa für die Bereiche der Telekommunikation (§§ 88 ff. TKG; diese sind wiederum teilweise europarechtlich durch die E-Privacy-Richtlinie vorgegeben) oder des Internets

⁴² Dazu unten Kapitel 3.2.4.

⁴³ Für eine detaillierte Darstellung der bereichsspezifischen Zuordnungsentscheidungen anhand der Fallstudien siehe Anhang II.

⁴⁴ Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (Datenschutz-Grundverordnung), ABl. EU Nr. 119/1 v. 4.5.2016.

⁴⁵ S. Schiedermaier, Der Schutz des Privaten als internationales Grundrecht, 2012.

(§§ 12 ff. TMG). Aus diesen ergeben sich jedoch keine inhaltlichen Aussagen, die für die Eigentumsordnung an Daten weiterführend sind. Das für den künftigen Straßenverkehr relevante Intelligente Verkehrssysteme-Gesetz (IVSG) verweist in § 3 S. 2 IVSG lediglich auf sonstige (nicht näher bezeichnete) Bundesgesetze.

Das Datenschutzrecht folgt einer Reihe von Grundprinzipien:⁴⁶

- Nach dem sog. **Verbotsprinzip** etwa in § 4 Abs. 1 BDSG und § 12 Abs. 1 TMG bedarf jeder Umgang mit personenbezogenen Daten einer Rechtsgrundlage, die entweder in einer Rechtsvorschrift (einschließlich § 28 Abs. 1 S. 1 Nr. 1 BDSG für Verträge) oder einer freiwilligen und informierten Einwilligung (§ 4a BDSG) liegt. In ähnlicher Weise stellt Art. 6 Abs. 1 DSGVO Anforderungen an die Rechtmäßigkeit der Datenverarbeitung.
- Daten dürfen nur für spezifische Zwecke erhoben und verwendet werden (**Zweckbindung**). Zweckänderungen bedürfen dementsprechend – wie sich beispielhaft aus § 12 Abs. 2 TMG ergibt – einer selbstständigen Grundlage und sind andernfalls rechtswidrig. Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DSGVO werden dies künftig neu justieren, ohne dass bisher klar ist, wie groß die Abweichungen zum deutschen Recht sein werden.
- Der konkrete Umgang mit den Daten muss in Bezug auf den Zweck erforderlich sein; dies ist bspw. in § 14 Abs. 1 und § 15 Abs. 1 TMG niedergelegt. Das **Erforderlichkeitsprinzip** (künftig „Datenminimierung“, Art. 5 Abs. 1 lit. c DSGVO) umfasst auch die Pflicht zur Löschung oder Anonymisierung, sobald die Daten entweder überhaupt nicht mehr oder jedenfalls nicht mehr in personenbezogener Form vorliegen müssen.
- Der **Grundsatz der Datenvermeidung und Datensparsamkeit** (§ 3a BDSG) enthält weitergehende Anforderungen auch an die Auswahl und Gestaltung von Datenverarbeitungssystemen. Soweit möglich und zumutbar sind Verfahren der Anonymisierung und Pseudonymisierung einzusetzen; dies wird für Telemedien nochmals in § 13 Abs. 6 TMG geregelt. Die Datenschutz-Grundverordnung enthält nur eingeschränkt vergleichbare Gestaltungsregelungen, etwa in Art. 25 DSGVO.
- Nach dem **Transparenzprinzip** müssen die Betroffenen über Art und Umfang der Datenverarbeitung informiert werden (künftig Art. 5 Abs. 1 lit. a DSGVO). Personenbezogene Daten sind folglich nach Möglichkeit direkt bei ihnen zu erheben (§ 4 Abs. 2 BDSG); daneben bestehen spezifische Informationspflichten wie in § 13 Abs. 1 TMG und korrespondierende Auskunftsansprüche.
- Das Datenschutzrecht enthält umfassende **Rechte der Betroffenen**, insbesondere auf Auskunft (§§ 19, 34 BDSG) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35 BDSG). Die Datenschutz-Grundverordnung fügt das Recht auf Datenübertragbarkeit hinzu und benennt den Lösungsanspruch nunmehr zusätzlich als „Recht auf Vergessenwerden“ (Art. 17 DSGVO). Die bisherigen Rechte können nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Ob dies auch unter der Datenschutz-Grundverordnung gilt, ist offen.
- Der Umgang mit sog. besonderen Arten personenbezogener Daten (§ 3 Abs. 9 BDSG und künftig Art. 9 DSGVO, bspw. Gesundheitsdaten) unterliegt besonderen **Restriktionen**. Im Bereich des Automobils wäre hierbei sowohl an Gesundheitsdaten als vor allem auch an biometrische Daten zu denken, die vom Fahrzeug zur Nutzeridentifizierung beim Öffnen oder Starten erhoben werden.
- Jede verantwortliche Stelle hat nach § 9 BDSG in Verbindung mit der zugehörigen Anlage (künftig nach Art. 32 DSGVO) **technische und organisatorische Maßnahmen** zu treffen, um die Einhaltung der datenschutzrechtlichen Anforderungen zu gewährleisten. Hinzu kommen spezielle Anforderungen wie in § 13 Abs. 4 TMG. Die entsprechenden Maßnahmen müssen verhältnismäßig sein und richten sich dementsprechend einerseits nach der Sensibilität der betroffenen Daten, andererseits nach dem Aufwand für die Umsetzung.
- Die Datenverarbeitung sowohl im öffentlichen als auch im nicht-öffentlichen Bereich unterliegt der **Kontrolle durch spezifische Behörden**, die ihre Aufgaben in völliger Unabhängigkeit wahrnehmen.

Für den Anwendungsbereich des Datenschutzrechts ist wesentlich, dass sowohl das geltende als auch das künftige Datenschutzrecht sämtliche **personenbezogenen Daten** (§ 3 Abs. 1 BDSG, Art. 4 Nr. 1 DSGVO) umfasst. Dies betrifft direkt personenbezogene, aber auch solche Daten, die lediglich mittels Zusatzwissens einer natürlichen Person

46 Die folgende Zusammenstellung bei Hornung, in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, Kap. 4 Rn. 16.

zugeordnet werden können und diese somit bestimmbar machen. Die Grenzen des Personenbezuges und damit der Anwendungsbereich des Datenschutzrechts werden weit verstanden. Der Europäische Gerichtshof hat am Beispiel von dynamischen IP-Adressen entschieden, dass diese für den Betreiber einer Webseite ein personenbezogenes Datum darstellen, „wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen.“⁴⁷ Folglich muss der Verantwortliche nicht schon alle Zusatzinformationen in den Händen halten, sondern es reicht die rechtliche Zugriffsmöglichkeit auf dieses Wissen aus. Hieran würde es lediglich bei einem gesetzlichen Verbot oder praktischer Nichtdurchführbarkeit fehlen.

Für **Automobildaten** bedeutet dies, dass auch Daten, die *prima facie* „lediglich“ technischer Natur sind, personenbezogen sind. Dabei ist nicht nur auf den oftmals (noch) nicht ermittelbaren Fahrer, sondern insbesondere auch auf den Halter abzustellen. Sollte dieser ermittelbar sein, ist der Anwendungsbereich des Datenschutzrechts eröffnet, auch wenn es um (vorgeblich) „belanglose“ Daten wie technische Betriebsinformationen des Automobils oder seiner Komponenten geht; weder der verfassungsrechtliche noch der einfachgesetzliche Datenschutz kennen einen Bagatellvorbehalt⁴⁸. Die technische Entwicklung im Bereich der Datenauswertung des Fahr- und Lenkverhaltens ist derweil soweit fortgeschritten, dass die Standortbestimmung ohne klassische Standortdaten (z. B. GPS oder Mobilfunk) möglich ist und damit **Bewegungsprofile** erstellt werden können, so dass folglich der Personenbezug nicht mehr in weiter Ferne liegt.

Die Besonderheit der technischen Daten eines Automobils besteht jedoch darin, dass die generierende Maschine oftmals eindeutig einer natürlichen Person zugeordnet ist (dem Halter). Anders als bei anderen Maschinendaten (etwa im Bereich von Infrastrukturkomponenten in der künftigen Verkehrstelematik oder auch in manchen Szenarien der Industrie 4.0)⁴⁹ wird der Anwendungsbereich des Da-

tenschutzrechts deshalb relativ schnell eröffnet. Er entfällt jedoch, wenn Daten technisch sicher anonymisiert sind, bevor sie erhoben und verwendet werden. Eine nachträgliche Entfernung des Personenbezugs ist mit anderen Worten zwar eine vielfach wünschenswerte datenschutzfreundliche Gestaltung, ändert aber nichts daran, dass zunächst personenbezogene Daten erhoben werden und für diesen Vorgang eine entsprechende Befugnis erforderlich ist.

Zumindest in deutscher, inzwischen aber auch in europäischer Tradition ist Datenschutz grundsätzlich als **persönlichkeitsrechtliches Abwehrrecht** ausgestaltet. Das BVerfG verknüpft den Schutz personenbezogener Daten eng mit Überlegungen der Persönlichkeitsentfaltung und der autonomen Selbstbestimmung der Person. Eigentumsorientierte Überlegungen existieren zwar⁵⁰, können diese dogmatische Fundierung aber nur ergänzen. Vorschläge z. B. aus den USA⁵¹ sind nur sehr eingeschränkt übertragbar, da sie vor dem Hintergrund völlig anderer verfassungsrechtlicher Rahmenbedingungen entwickelt worden sind (vergleichbare grundrechtliche Standards fehlen dort). Da es in den USA überdies keine allgemeinen Datenschutzgesetze nach europäischem Vorbild gibt, zielen die dortigen eigentumsrechtlichen Vorschläge außerdem gerade nicht auf eine wirtschaftliche Nutzungsordnung, sondern versuchen, durch eine Verknüpfung mit dem anerkannten Maß an rechtlich geschütztem Eigentum überhaupt erst zu begründen, warum personenbezogene Daten ebenfalls eines Schutzes bedürfen. Sie zielen also klar auf die Stärkung des Datenschutzes⁵².

Trotz dieser abwehrrechtlichen Konzeption bietet das geltende Datenschutzrecht Ansatzpunkte für die **Gestaltung von Verfügungsbefugnissen**. In der Praxis führt das erwähnte Verbotsprinzip dazu, dass im privaten Umfeld die Datennutzungsrechte durch Verträge und/oder Einwilligungen eingeräumt werden. Dies erfolgt regelmäßig für eine Gegenleistung, die oftmals in der entgeltfreien Nutzung eines Dienstes liegt. In diesem Sinne „gehören“ dem Betroffenen die Daten – da nur er wirksam Einwilligungen und Verträge abschließen kann – und er „handelt“

47 EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer/Deutschland.

48 S. Hornung, DuD 2015, 359 (361 f.).

49 Hier können etwa im Bereich der Produktions- und Produktüberwachung Messdaten entstehen, die Auskunft über Maschinen geben und zum Beispiel auf Fehler oder Verbesserungspotential hinweisen bzw. für eine zustandsbasierte Wartung notwendig sind, s. auch Ensthaler, NJW 2016, 3473 (3473). Auch die Standortfeststellung von Werkzeugen, zum Beispiel durch RFID-Chips sowie die Überwachung der Qualität bzw. der Abnutzung von Werkzeugen auf dem betrieblichen Hallenboden ist ein denkbarer Anwendungsfall – immer vorausgesetzt, dass die Abnutzung nicht auf eine einzelne bestimmte oder bestimmbare Person zurückführbar ist.

50 Z. B. Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 202 ff.; ders., in: Redeker/Hoppen (Hrsg.), DGRI Jahrbuch 2011, S. 53 ff.; Kilian, CRI 2012, 169 ff.; ders., GS Steinmüller, 2014, v. a. S. 204 ff.; Zech, Information als Schutzgegenstand, 2012.

51 S. z. B. Samuelson, 52 Stanford Law Review 1125 (2000); Schwarz, 117 Harvard Law Review 2056 (2004), 2094 ff.

52 Zu dieser Überlegung schon Hornung/Goebel, CR 2015, 265 (268).

mit ihnen durch diese Instrumente⁵³. Das Problem besteht dann freilich in der fehlenden Verhandlungsmöglichkeit auf Augenhöhe. Auch die Datenschutz-Grundverordnung wird hieran nichts ändern. Diese sind zum einen durch Informationsasymmetrien bedingt, derentwegen die Betroffenen den Wert der von ihnen „angebotenen“ Leistung nicht kennen; hinzu treten ökonomische Ungleichgewichte zwischen Privatpersonen einerseits, weltweit operierenden Oligopolen andererseits⁵⁴.

Da die Entscheidungsbefugnis über die Datenverarbeitung grundsätzlich beim Betroffenen liegt, wird in der Literatur zum Teil angenommen, dieser sei auch Rechteinhaber des Datums selbst und durch das **Datenschutzrecht** sei de lege lata eine **umfassende Zuordnungsentscheidung zum Persönlichkeitsträger** getroffen worden⁵⁵. Daher sei der Datenschutz als „neuartiges Eigentumsrecht“ zu qualifizieren und das Recht am eigenen Datum vermittele eigentumsrechtliche Ansprüche des Betroffenen⁵⁶.

Dieser Ansatz ist indes kritisch zu sehen. In der Tat werden die personenbezogenen Daten dem Betroffenen durch das BDSG in einem gewissen Maße zugeordnet. Dennoch handelt es sich hier richtigerweise um eine **bereichsspezifische Zuordnung** und nicht um ein vollumfängliches, eigentumsähnliches Recht, da dem Betroffenen **kein** gegenüber jedermann wirkendes, **positives Nutzungsrecht** an dem personenbezogenen Datum zusteht. Denkbar wäre allerdings die Normierung eines derartigen positiven Rechts auf die Nutzung der eigenen Daten⁵⁷. Wollte man das Datenschutzrecht derart verstehen, dass es dem Betroffenen auch ein positives Nutzungsrecht vermittelt, bedürfte es allerdings diverser Beschränkungen zur Sicherstellung von Rechten Dritter zum Umgang mit den Daten, die de lege lata jedoch nicht normiert sind. Das Datenschutzrecht weist dem Betroffenen gerade keine umfassende Verfügungsbefugnis über die auf ihn bezogenen Daten zu, sondern es handelt sich zugunsten der Meinungs- und Informationsfreiheit um ein abwägungsoffenes Recht⁵⁸.

Aus der Sicht des Datenschutzrechts erfolgt in den Fallstudien **keine generelle Zuweisung/Zuordnung der Daten zu einzelnen Personen** und dieses Rechtsgebiet trifft folglich keine Aussagen, die für eine Eigentumsordnung weiterführend sind. Aufgrund des aus dem Persönlichkeitsrecht folgenden abwehrrechtlichen Charakters des Datenschutz-

rechts sind darüber hinaus nur solche Datenvorgänge (Erhebungen, Verwendungen und Nutzungen) relevant, die einen Personenbezug aufweisen. Damit hat das Datenschutzrecht in **Fallstudie 5** überhaupt keine Relevanz. In den **Fallstudien 1 bis 4** trifft das Datenschutzrecht nur dann eine Aussage, wenn die jeweiligen Daten einen Personenbezug aufweisen (für eine detaillierte Untersuchung aller Fallstudien, siehe Anhang II.ii.). Tatsächlich wird in der Praxis das Vorliegen eines Personenbezuges in den ersten vier Fallstudien fast durchweg der Fall sein, auch wenn anonyme Umsetzungen technisch durchaus realisierbar sind. In gewisser Weise wird in diesen Situationen für die Daten, die einen einer Person zuzuordnenden Aussagegehalt aufweisen, eine aktive Verfügungsbefugnis hergestellt, indem sie dieser Person zugeordnet werden. Denn jeder Umgang mit diesen Daten bedarf einer Legitimation. Ansonsten ist die Datenerhebung und Datenverarbeitung ohne Legitimation in den vorliegenden Fällen verboten.

Eine Legitimation kann neben der **Einwilligung** auch in Form einer **Rechtsvorschrift** erfolgen, die die Erhebung, Verarbeitung und Nutzung erlaubt oder anordnet, wobei der exakte Umfang der mitgliedstaatlichen Regelungsmöglichkeiten nach der Datenschutz-Grundverordnung bislang umstritten ist und mutmaßlich erst in einigen Jahren durch den EuGH geklärt werden wird. Der für eine Vertragserfüllung erforderliche Datenumgang erfolgt systematisch nicht auf der Basis des Vertrags, sondern aufgrund der gesetzlichen Regelung in § 28 Abs. 1 S. 1 Nr. 1 BDSG. Folglich kommt es auf die Einwilligung nicht mehr an, wenn ein gesetzlicher Erlaubnistatbestand vorliegt. Die verantwortliche Stelle darf dann jedoch auch nicht durch eine parallele Einwilligung suggerieren, der Betroffene hätte eine Wahlfreiheit. In der Praxis liegen die Varianten der vertraglichen Regelung und der Einwilligung jedoch relativ eng beieinander. In den Fallstudien 1 bis 4 kann es deshalb dazu kommen, dass der Datenumgang entweder durch einen Vertrag mit relativ breitem Zweck (z. B. Nutzung einer Mobilitätsdienstplattform mit angeschlossenen Dienstleistungen) legitimiert wird, oder der Umgang wird – unter Transparenzgesichtspunkten vorzugswürdig, je nach Zahl aber aufwändig und nutzerunfreundlich – in spezifischen Einzelfällen durch Einwilligungen zugelassen. Die dabei erklärte Einwilligung muss freiwillig und informiert sein. Dies setzt die Kenntnis über die Tragweite der Entscheidung voraus. Eine Blankoeinwilligung oder eine Einwilli-

53 S. Hornung/Gooble, CR 2015, 265 (270).

54 S. Hornung/Gooble, CR 2015, 265, (270 f).

55 Kilian, Gedächtnisschrift für W. Steinmüller, 2014, 195 (207 ff.); Weichert, NJW 2001, 1463 (1469); Ladeur, DuD 2000, 12 (18).

56 Schwartmann/Hentsch, PinG 2016, 117 (122); Weichert, NJW 2001, 1463 (1469); Ladeur, DuD 2000, 12 (18).

57 Siehe dazu ausführlich unter 5.1.1.1.

58 Zech, GRUR 2015, 1151 (1155).

gung, die pauschal gehalten ist und einen sehr weiten (abstrakten) Zweck vorsieht, so dass für den Betroffenen nicht eindeutig erkennbar ist, wer seine Daten verarbeitet und nutzt, wäre dementsprechend unzulässig⁵⁹.

Das Instrument des freiwillig geschlossenen Vertrags mit dem Betroffenen steht dem Einsatz von Einwilligungen also nicht entgegen, sofern die Instrumente nicht parallel verwendet werden und dem Betroffenen damit eine Wahlfreiheit suggeriert wird, die nicht besteht. Verträge geben beiden Parteien (und damit vor allem auch dem Betroffenen) eine Möglichkeit, selbstbestimmt über die Preisgabe der Daten und eine etwaige Gegenleistung zu entscheiden. Die Freiwilligkeit, insbesondere gegenüber einem am Markt starken Anbieter wie dem Automobilhersteller oder einem Mobilitätsdiensteanbieter, wird dadurch gesichert, dass z. B. im Zusammenhang mit Werbezwecken die Einwilligung nicht von einer expliziten Gegenleistung, namentlich dem Vertragsschluss, abhängig gemacht werden darf (**Kopplungsverbot**). Dies gilt auch, wenn die Einwilligung zwingend für den Vertragsschluss vorgesehen wird, aber die Daten nicht zwingend zur Durchführung des Vertrages sind.

Damit kann im Ergebnis festgehalten werden, dass das Datenschutzrecht nur dann einschlägig ist, wenn es sich um personenbezogene Daten handelt, also um solche, die Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar Person darstellen. Aufgrund des Schutzzwecks des Datenschutzrechts, der den einzelnen Betroffenen in seinem Persönlichkeitsrecht schützt, gibt es diesem trotz der erläuterten Gestaltungsmöglichkeiten dogmatisch nur ein **negatives Abwehrrecht**, aber gerade keine positive Verfügungsbefugnis an die Hand⁶⁰. Folglich geht mit dem Datenschutzrecht keine umfassende Zuordnung einher, so dass im Ergebnis keine Aussagen getroffen werden können, die für die Eigentumsordnung weiterführend sind.

3.2.2 Urheberrecht

3.2.2.1 Überblick

Neben dem Urheberrecht (Teil 1) regelt das Urheberrechtsgesetz in Teil 2 die verwandten Schutzrechte. Die Schutzrechte nach dem Urheberrechtsgesetz entstehen unabhängig davon, ob die Inhalte einen Personenbezug im datenschutzrechtlichen Sinne aufweisen. Das **Urheberrecht** belohnt persönliche geistige Schöpfungen Werkschaffender (§ 2 Abs. 2 UrhG) und schützt als einheitliches Recht deren vermögensrechtlichen und ideellen Interessen, § 11 UrhG⁶¹. Dem Schöpferprinzip in § 7 UrhG folgend, entsteht das Urheberrecht selbst dann in den Händen der natürlichen Person des Schöpfers, wenn dieser das Werk als Arbeitnehmer oder gar Ghostwriter für einen anderen geschaffen hat. Anders als nach der US-amerikanischen „work made for hire doctrine“ müssen Arbeitgeber und andere Auftraggeber deshalb abgeleitete Nutzungsrechte (§ 31 Abs. 1 S. 1 UrhG) erwerben, um das Werk selber nutzen zu dürfen, vgl. § 43 UrhG⁶². Die verwandten Schutzrechte (**Leistungsschutzrechte**) betreffen Leistungen, die zwar keine schöpferischen sind, die der Gesetzgeber aber für die Kulturvermittlung als so wichtig ansieht, dass er sie mit einem Ausschließlichkeitsrecht bedacht hat⁶³, um sie zu einem marktfähigen Gut zu machen. Gegenstand dieser Leistungsschutzrechte können nichtschöpferische persönliche Leistungen sein, wie etwa diejenigen ausübender Künstler (§§ 73 ff. UrhG) oder Verfasser wissenschaftlicher Ausgaben (§ 70 UrhG). Andere Leistungsschutzrechte honorieren wirtschaftliche, technische und organisatorische Leistungen⁶⁴, wie z. B. die von Sendeunternehmen (§ 87 UrhG) oder Tonträgerherstellern (§§ 85 f. UrhG). Neu hinzugekommen ist im Jahr 2013 das Leistungsschutzrecht für Presseverleger (§ 87f UrhG), das diese insbesondere vor systematischen Zugriffen von Suchmaschinen schützen soll⁶⁵. Das auf der Richtlinie 96/9/EG beruhende Schutzrecht für den Hersteller von Datenbanken (§§ 87a ff. UrhG) sichert dessen Investitionen in moderne Datenspeicher- und Datenverarbeitungssysteme⁶⁶. Inhaber des Rechts ist der Hersteller der Datenbank (§ 87a Abs. 2 UrhG), also diejenige juristische oder natürliche Person, die das Investitionsrisiko trägt⁶⁷.

59 Zu den Einzelheiten siehe auch *Simitis*, Bundesdatenschutzgesetz, 8. Aufl. 2014, § 4a Rn. 77ff. und *Gola/Klug/Körffner*, in: *Gola/Schomerus* (Hrsg.), Bundesdatenschutzgesetz, 12. Aufl. 2015, § 4a Rn. 26f.

60 *Härting*, CR 2016, 646 (648).

61 Zum Schutzgegenstand des Urheberrechts und der monistischen Theorie Schack, UrhR, 7. Aufl. 2015, Rn. 339 ff.

62 Zum Schöpferprinzip Schack, UrhR, 7. Aufl. 2015, Rn. 300 ff.

63 *Loewenheim*, in: ders. (Hrsg.), HB UrhR, 2. Aufl. 2010, § 1 Rn. 3.

64 *Dreier*, in: *Dreier/Schulze* (Hrsg.), UrhG, 5. Aufl. 2015, Vorbem zu §§ 70 ff Rn. 2.

65 Reg. Begründung, BT-Drs. 17/11470, S. 6.

66 Vgl. § 87a Abs. 1 S. 1 UrhG und ErwGr. 7, 11 und 12 RL 96/9/EG. Zum Schutzgegenstand *Vogel*, in: *Schricker/Loewenheim* (Hrsg.), UrhG, 4. Aufl. 2010, § 87a Rn. 30 ff.

67 ErwGr. 41 RL 96/9/EG.

Anders als beim urheberrechtlichen Werkschutz entsteht dieses Leistungsschutzrecht nicht originär bei demjenigen, der die konkreten Arbeiten an den Datenbanken ausführt, sondern in den Händen des Geldgebers⁶⁸.

3.2.2.2 Anwendung auf die Fallstudien

Urheberrecht

Die vom Urheberrecht geschützten **persönlichen geistigen Schöpfungen** (§ 2 Abs. 2 UrhG) setzen eine menschliche Tätigkeit voraus, die über Individualität verfügt. Dazu muss das Werk einen eigenen geistigen Gehalt aufweisen, in dem sich die eigenpersönlichen Züge seines Schöpfers spiegeln⁶⁹. Hierzu kann der Urheber zwar technische Hilfsmittel einsetzen, so dass auch digitale Zeichnungen und Fotografien Werkschutz genießen können. Keine menschliche Tätigkeit liegt dagegen vor, wenn Maschinen ungesteuert vollautomatisch Informationen generieren⁷⁰. Darüber hinaus erreichen einzelne Worte kaum jemals die nötige Gestaltungshöhe, um hinreichend individuell zu sein⁷¹. Die **einzelnen Daten** aus den Fallstudien, wie die Kontaktinformationen der jeweiligen Fahrer oder deren PIN⁷² schützt das Urheberrecht daher nicht⁷³. Dies gilt erst recht für Einzelangaben, die die Fahrzeuge⁷⁴ oder andere Verkehrsinfrastruktureinrichtungen, wie die *Roadside-Units* in Fallstudie 5⁷⁵, automatisch erzeugen, da hier darüber hinaus die menschliche Hand keinen steuernden Einfluss ausübt.

Erst die persönliche schöpferische Auswahl und Anordnung von Einzelangaben belohnt das Urheberrecht im Einzelfall als **Sammel- bzw. Datenbankwerk**, § 4 UrhG⁷⁶. Hierzu zählen kreative Zusammenstellungen, die einen vorhandenen Gestaltungsspielraum ausschöpfen, wie etwa

die Wahl bestimmter Begriffe für ein medizinisches Lexikon⁷⁷ oder die Kriterien für eine Struktur eines Berichts zur Auswertung der Umsätze der pharmazeutischen Industrie⁷⁸. In den vorliegenden Fallstudien werden die Entwickler der Fahrzeughersteller, *Carsharing*-Anbieter und Mobilitätsplattformbetreiber die Daten meist aber nach technischen oder naturwissenschaftlichen Kriterien gruppieren, die ihren individuellen Gestaltungsspielraum begrenzen⁷⁹. Dieser fehlt insbesondere dann, wenn sie die Daten vollständig erfassen oder alphabetisch bzw. numerisch indexieren⁸⁰. In den konkreten Fallstudien deutet nichts darauf hin, dass die Beteiligten die jeweiligen Daten schöpferisch auswählen oder anordnen. In den den Fallstudien zugrundeliegenden Szenarien ist es jedoch gut vorstellbar, dass die Beteiligten die Angaben in einer Weise zusammenstellen, die die nötige Gestaltungshöhe übersteigt, so dass ein Sammelwerk vorläge. Das Urheberrecht der Entwickler würde dann aber nur die Sammlung als solche schützen und sich nicht auf die darin enthaltenen Daten erstrecken. Deren urheberrechtlicher Schutz wird eigenständig bewertet⁸¹, so dass jedermann weiterhin die gemeinfreien Elemente der Datenbankwerke entnehmen darf. Nur die Verwertung zumindest prägender Werkteile der geschützten Sammlungen verletzen die Rechte der Urheber. Das Sammelwerk bietet daher weder einen Schutz der Vertraulichkeit der Daten, noch schützt es den Rechtsinhaber vor Entnahmen einzelner Elemente.

Als schutzfähiges Werk kommt in den Fallstudien ferner die **Software** in Betracht, mit deren Hilfe die von den Sensoren erfassten Daten verarbeitet werden. Der Werkschutz des Computerprogramms (§ 69a Abs. 1 UrhG) umfasst jedoch weder die Datenbankstrukturen, noch die einzelnen Daten⁸², so dass das Urheberrecht auch insoweit die

68 Vogel, in: Schricker/Loewenheim (Hrsg.), UrhG, 4. Aufl. 2010, § 87b Rn. 70.

69 Schack, UrhR, 7. Aufl. 2015, Rn. 181 ff.; Bullinger, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 2 Rn. 15 ff.; Ohly, 70. DJT, Teil F S. 29. Zum europäischen Werkbegriff vgl. auch Ohly, 70. DJT, Teil F S. 27 f.

70 Schulze, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 2 Rn. 8.

71 Zu Sprachwerken allgemein Schack, UrhR, 7. Aufl. 2015, Rn. 202; Schulze, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 2 Rn. 83 f mit Beispielen.

72 Vgl. Fallstudie 2.

73 Zech, CR 2015, 137 (141); Schefzig, K&R Beiheft 3/2015, 3 (6).

74 Z. B. Diagnose-, Nutzungs- oder Positionsdaten.

75 Vgl. Fallstudie 5.

76 Das Datenbankwerk ist ein Unterfall des Sammelwerkes, Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 4 Rn. 16. Zum konventionsrechtlichen Schutz von Datenbanken Auer-Reinsdorff, in: Conrad/Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, § 15 Rn. 18.

77 OLG Hamburg, GRUR 2001, 831 ff.

78 OLG Frankfurt aM, MMR 2003, 45 (46).

79 Wiebe, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, § 4 UrhG Rn. 16. Mit Blick auf Big Data-Anwendungen bei Maschinen zurückhaltend Dörner, CR 2014, 617 (621); Zech, CR 2015, 137 (141).

80 Ahlberg, in: BeckOK UrhR, 13. Ed. 2016, § 4 Rn. 30 ff.; Loewenheim, in: ders. (Hrsg.), HB UrhR, 2. Aufl. 2010, § 9 Rn. 245 f.

81 Wiebe, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl. 2015, § 4 UrhG Rn. 15; Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 4 Rn. 4.

82 Grützmaker, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 69a Rn. 16; Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 69a Rn. 12.

Informationen nicht monopolisiert. § 69a Abs. 2 S. 2 UrhG nimmt Ideen und Schnittstellen der Computerprogramme vielmehr ausdrücklich vom Werkschutz aus. § 69e UrhG soll zudem ermöglichen, dass die Hersteller konkurrierender Programme die nötigen Informationen erhalten, um interoperable Anwendungen entwickeln zu können⁸³ (für eine detaillierte Untersuchung aller Fallstudien siehe Anhang II.iii.).

Leistungsschutzrecht des Datenbankherstellers

In Umsetzung der Vorgaben aus Art. 7 RL 96/9/EG regelt § 87a Abs. 1 S. 1 UrhG die Voraussetzungen des **Leistungsschutzrechts des Datenbankherstellers**⁸⁴. Diesen Leistungsschutz *sui generis* genießen alle Sammlungen von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Die Schutzwelle für wesentliche Investitionen setzt die Rechtsprechung niedrig an und fordert keine Investitionen von substanziellem Gewicht. Ausreichend seien vielmehr alle objektiv nicht ganz unbedeutenden, von jedermann leicht zu erbringenden Aufwendungen, die erforderlich waren, um die Datenbank zu erstellen⁸⁵. Ob die in der Datenbank enthaltenen Elemente selber urheberrechtlich geschützt sind, spielt dabei keine Rolle⁸⁶. Aufgrund der verschiedenen Schutzzwecke und damit korrespondierenden Voraussetzungen können der *sui generis* Schutz (§ 87a UrhG) und der Werkschutz (§ 4 UrhG) im Einzelfall nebeneinander bestehen⁸⁷.

Wie gezeigt, sammeln die einzelnen Akteure in den Fallstudien viele unverarbeitete **Rohdaten**, die unmittelbar

von den Sensoren der Fahrzeuge erzeugt werden. Für die entstehenden ungeordneten „Datenhaufen“ gilt das Leistungsschutzrecht zwar nicht⁸⁸. Typischerweise wollen die Akteure aus den maschinen-generierten Rohdaten aber einen Mehrwert generieren und werden die Einzelinformationen daher systematisch oder methodisch anordnen und mit Hilfe von Datenanalyse-Anwendungen – also elektronischen Mitteln – zugänglich machen. Ob das Leistungsschutzrecht im Einzelfall besteht, hängt daher vor allem davon ab, ob die jeweiligen Stellen eine nach Art und Umfang *wesentliche Investition* in die Beschaffung, Überprüfung oder Darstellung der einzelnen Daten tätigen.

Mit Blick auf den Schutzzweck begrenzt der EuGH aber den Kreis der **Kosten, die schutzbegründend wirken**⁸⁹. Das Leistungsschutzrecht soll nur denjenigen belohnen, der Investitionen in den „Aufbau von Datenbanken tätigt“, weil diese – angesichts der exponentiellen Zunahme von Daten – einen wichtigen Beitrag für das Entstehen eines Informationsmarktes leisten⁹⁰. Zur *Beschaffung* von Daten zählen daher nur solche Mittel, mit denen vorhandene Daten ermittelt werden, nicht aber solche, mit denen Daten erst erzeugt werden⁹¹. Schwierig ist die Abgrenzung zwischen schutzbegründenden Investitionen in die Beschaffung und unbeachtlichen in die Erzeugung von Daten, wenn die vermeintlichen Datenbankhersteller an der Datengenerierung – wie in den vorliegenden Fallstudien – mitwirken⁹². Der EuGH zieht diese Grenze mit einer wertenden Betrachtung und prüft, ob die Investition primär dem Aufbau einer Datenbank dient oder anderen Zwecken⁹³. Fallen die Daten als Nebenprodukt einer anderen selbstständigen Tätigkeit ab, erfasse der Schutzzweck des Leistungsschutzrechts nicht die Ausgaben in deren Erzeugung (*Spin-off-Theorie*)⁹⁴. Entsprechend ließ der EuGH

83 Grützmaker, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 69e Rn. 1; Loewenheim, in: Schricker/Loewenheim (Hrsg.), UrhG, 4. Aufl. 2010, § 69e Rn. 1 ff.

84 Zum entsprechenden Kollisionsrecht Spindler, in: Conrad/Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, § 21 Rn. 10 ff.

85 BGH, GRUR 2011, 724 (725); Vogel, in: Schricker/Loewenheim (Hrsg.), UrhG, 4. Aufl. 2010, § 87a Rn. 43; a.A. Schack, UrhR, 7. Aufl. 2015, Rn. 745. Vgl. auch Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 4 Rn. 14 f. mit weiteren Beispielen.

86 Vgl. ErwGr. 26 RL 96/9/EG.

87 BT-Drs. 13/7934, S. 51.

88 Thum/Hermes, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87a Rn. 24; Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 87a Rn. 7.

89 Metzger, GRUR 2012, 118 (124 f.).

90 Vgl. ErwGr. 7, 9 und 10 RL 96/9/EG. Zur Bedeutung von Datenbanken in der Informationsgesellschaft Auer-Reinsdorff, in: Conrad/Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, § 15 Rn. 10.

91 EuGH, Rs. C-203/02, ECLI:EU:C:2004:695 Tz. 42 – The British Horseracing Board Ltd; Rs. C-444/02, ECLI:EU:C:2004:697 Tz. 40 – Fixtures Marketing Ltd.; BGH, GRUR 2010, 1004 (1005); Ehmann, K&R 2014, 394 (397); Vogel, in: Schricker/Loewenheim (Hrsg.), UrhG, 4. Aufl. 2010, § 87a Rn. 52; Thum/Hermes, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87a Rn. 36.

92 Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 87a Rn. 13; Specht, CR 2015, 288 (293).

93 Koch, in: BeckOK UrhR, 13. Ed. 2016, § 87a Rn. 21; Vogel, in: Schricker/Loewenheim (Hrsg.), UrhG, 4. Aufl. 2010, § 87a Rn. 54. Vgl. EuGH, Rs. C-203/02, ECLI:EU:C:2004:695 Tz. 35 ff. – The British Horseracing Board Ltd; Rs. C-444/02, ECLI:EU:C:2004:697 Tz. 45 ff. – Fixtures Marketing Ltd.

94 Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 87a Rn. 13; Ehmann, K&R 2014, 394 (397 f.); Koch, in: BeckOK UrhR, 13. Ed. 2016, § 87a Rn. 24.

den Aufwand unberücksichtigt, den der Veranstalter der englischen Fußballliga aufgebracht hatte, um die Spielpläne der Saison zu erstellen. Die Aufbereitung dieser Daten für einen Kalender bedürfe keiner weiteren wesentlichen Investitionen⁹⁵. Auch die Kosten für das Erstellen der Startlisten von Pferderennen sind daher für den Veranstalter solcher Rennen keine eigenständigen Investitionen in eine Datenbank⁹⁶.

Der **Bundesgerichtshof** folgt im Ausgangspunkt der europäischen Rechtsprechung⁹⁷. Mit Rückgriff hierauf hat das Gericht zu Gunsten der *Toll Collect GmbH* entschieden, dass deren Aufwand in die Infrastruktur der Mauterfassung (stationäre Mautstellenterminals und mobile Fahrzeuggeräte) berücksichtigungsfähige Investitionen i. S. v. § 87a UrhG seien. Die mit dieser Infrastruktur erfassten Daten mautpflichtiger Fahrer, wie deren Kennzeichen und Länge der gefahrenen Strecken seien auch ohne die Erfassung vorhanden und würden daher von *Toll Collect* nicht erzeugt, sondern gesammelt. Etwas anderes gelte nur für die aus diesen Daten errechnete Maut⁹⁸.

Auf diese Weise ließen sich die Ausgaben in die Infrastruktur für die *Car-2-X*-Mitteilungen und späteren Verkehrslageübersichten (Fallstudie 5) als wesentliche Investition i. S. v. § 87a Abs. 1 S. 1 UrhG begreifen. Der BGH geht indes nicht weiter darauf ein, dass *Toll Collect* in die gezeigte Datenerfassungsinfrastruktur investiert hatte, um primär die Maut zu erheben und nicht um eine Datenbank aufzubauen. Dementsprechend könnten die gewonnenen Datenbanken im Rahmen der nötigen wertenden Betrachtung genauso gut als Nebenprodukt (*Spin-off*) des Hauptgeschäfts verstanden werden⁹⁹. Ob der BGH sich also wirklich auf der Linie des EuGH bewegt, können nur künftige Entscheidungen der Luxemburger Richter zeigen.

Darüber hinaus tendieren viele Stimmen in der **Literatur** dazu, die Daten aus den zahllosen Sensoren bei Smart-Cars (vgl. Fallstudien 1 bis 4) als bloße Nebenprodukte anderer Kerngeschäfte anzusehen, so dass die Investitionen hierin oft kein Leistungsschutzrecht begründen würden¹⁰⁰. Dieses enge Verständnis entspricht der teleologischen Auslegung des EuGH. In Zeiten der *Cloud* und des Internets der Dinge werden immer mehr Alltagsgegenstände mit Sensoren ausgestattet, die viele zusätzliche Daten verfügbar machen. Nicht das Anhäufen der Datenberge soll der *sui generis* Schutz belohnen, sondern die Investitionen in fortschrittliche Informationssysteme¹⁰¹, die diese Daten zusammenfassen und zugänglich machen. Generieren Datenbankhersteller selber Daten, fällt es vor dem Hintergrund der gezeigten Diskussion letztlich schwer, im Einzelfall schutzbegründende Ausgaben in die Beschaffung von Daten trennscharf von unerheblichen Aufwendungen für die Datenerzeugung abzugrenzen¹⁰².

Das Leistungsschutzrecht schützt weder die Vertraulichkeit, noch die Integrität einzelner Elemente der Datenbanken. Gemäß § 87b Abs. 1 S. 1 UrhG kann der Datenbankhersteller Dritten nur verbieten, wesentliche Teile der Datenbank zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Unwesentliche Teile der Datenbanken kann dagegen jeder frei nutzen, so dass der *sui generis* Schutz keine Informationen als solche monopolisiert¹⁰³. Die Wesentlichkeit der entnommenen Datenbankteile entscheidet daher über das Verhältnis von frei zugänglichen Informationen und dem Investitionsschutz des Datenbankherstellers, so dass im Ausgangspunkt weitgehend keine geringen Anforderungen hieran gestellt werden¹⁰⁴. Wann jemand wesentliche Teile übernimmt, entzieht sich einer schematischen Prüfung und wird durch Abwägung der aufgezeigten Interessen im Einzelfall beurteilt¹⁰⁵. Die Rechtsprechung arbeitet dennoch mit Richtwerten¹⁰⁶ und hält etwa die Übernahme eines Zehntels der in der Datenbank

95 EuGH, Rs. C-444/02, ECLI:EU:C:2004:697 Tz. 45 ff. – Fixtures Marketing Ltd.

96 EuGH, Rs. C-203/02, ECLI:EU:C:2004:695 Tz. 38 ff. – The British Horseracing.

97 Zuletzt BGH, GRUR 2011, 724 (725) m. w. N.

98 BGH, GRUR 2010, 1004 (1005). Kritisch *Ehmann*, der die erhobenen Verkehrsdaten als Nebenprodukt (*Spin-off*) des Geschäftskonzepts von *Toll Collect* ansieht, da diese die Infrastruktur für die Datenerhebung auch ohne das Leistungsschutzrecht betreiben würde, K&R 2014, 394 (398).

99 *Ehmann*, K&R 2014, 394 (398).

100 *Grützmacher*, CR 2016, 485 (488); *Sahl*, PinG 2016, 146 (148). Zurückhaltend auch *Zech* im Zusammenhang mit Big Data-Anwendungen, GRUR 2015, 1151 (1157 f.).

101 ErwGr. 11 RL 96/9/EG.

102 *Thum/Hermes*, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87a Rn. 41 ff.

103 ErwGr. 45, 46 RL 96/9/EG; Koch, in: BeckOK UrhR, 13. Ed. 2016, § 87b Rn. 12; *Thum/Hermes*, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87b Rn. 4.

104 *Dreier*, in: *Dreier/Schulze* (Hrsg.), UrhG, 5. Aufl. 2015, § 87b Rn. 5 m.w.N.; a.A. *Vogel*, in: *Schricker/Loewenheim* (Hrsg.), UrhG, 4. Aufl. 2010, § 87b Rn. 29.

105 *Vogel*, in: *Schricker/Loewenheim* (Hrsg.), UrhG, 4. Aufl. 2010, § 87b Rn. 26; *Loewenheim*, in: ders. (Hrsg.), HB UrhR, 2. Aufl. 2010, § 43 Rn. 16.

106 Dazu *Dreier*, in: *Dreier/Schulze* (Hrsg.), UrhG, 5. Aufl. 2015, § 87b Rn. 7.

enthaltenen Elemente grundsätzlich nicht als *quantitativ* wesentliche Entnahme¹⁰⁷. Auch die Entnahme einzelner Elemente kann der Schutzrechtinhaber nicht abwehren, da diese selbst dann in *qualitativer* Hinsicht keinen wesentlichen Teil der Datenbank ausmachen, wenn diese hoch sensible Informationen enthalten, die z. B. geheime Einblicke in Geschäftsprozesse bieten. Für den nötigen Schutz sorgen insoweit die Regeln über Betriebs- und Geschäftsgeheimnisse im Lauterkeitsrecht¹⁰⁸. § 87b Abs. 1 S. 2 UrhG schafft eine wichtige Ausnahme vom Grundsatz, dass jedermann unwesentliche Teile der Datenbanken frei verwenden darf. Die Norm soll verhindern, dass Personen planmäßig und wiederholt unwesentliche Teile der Datenbank nutzen und dadurch das Ausschließlichkeitsrecht umgehen¹⁰⁹. Um den gezeigten Grundsatz im Interesse der Freiheit einzelner Informationen zu erhalten, wird § 87b Abs. 1 S. 2 UrhG teleologisch eng verstanden¹¹⁰. Auch die Auswertung von Daten aus Datenbanken i. S. v. § 87a UrhG mit Data-Mining-Anwendungen¹¹¹ kann der Datenbankhersteller nicht *per se* abwehren¹¹². Wer fremde Datenbanken mit solchen Anwendungen durchsucht, entnimmt meist keine wesentlichen Teile der Datenbanken und gefährdet nicht das Amortisationsinteresse des Datenbankherstellers. Politisch wird ferner derzeit darüber diskutiert, bestehende Urheber- und Leistungsschutzrechte durch eine neue Data-Mining-Schranke zu begrenzen¹¹³ (für eine detaillierte Untersuchung aller Fallstudien, siehe Anhang II.iii.).

3.2.2.3 Zwischenfazit zum Urheberrecht

Die einzelnen Daten oder Informationen aus den Fallstudien genießen **keinen urheberrechtlichen Werk- und Leistungsrechtsschutz**¹¹⁴. Mangels schöpferischer Auswahl oder Anordnung der Daten besteht auch kein Schutz der Zusammenstellungen als Sammelwerk (§ 4 UrhG). Tätigen die Beteiligten eine nach Art und Umfang wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung

von Daten, steht ihnen dagegen das Leistungsschutzrecht gemäß § 87a UrhG zu. Ob die Ausgaben für die Sensorik in den Fallstudien schutzbegründend wirken, ist jedoch fraglich, da Investitionen in die Datenerzeugung nicht der Beschaffung von Daten dienen. Vor allem aber würde ein etwaiges Leistungsschutzrecht dem Datenbankhersteller kein Recht an den in der Datenbank enthaltenen Daten verschaffen. Mit dem Leistungsschutzrecht kann dieser Dritten nur untersagen, wesentliche Teile der Datenbank zu entnehmen, § 87a UrhG. Wann eine solche Entnahme vorliegt, wird mit einer wenig rechtssicheren Interessenabwägung im Einzelfall ermittelt. Diese beruht ferner auf dem Grundsatz, dass das Leistungsschutzrecht zu Gunsten der Allgemeinheit keine einzelnen Informationen monopolisiert. Letztlich bietet der *sui generis* Schutz den Beteiligten in den Fallstudien daher kein Recht an den erzeugten Mobilitätsdaten.

3.2.3 Strafrecht

Voranzustellen ist, dass im Strafrecht grundsätzlich keine Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten getroffen wird. § 303a StGB schützt den **Berechtigten** in der nicht beeinträchtigten Verwendbarkeit von gespeicherten Daten. Schutzgut ist demnach die **Verfügungsbefugnis über die Integrität von Daten**¹¹⁵. Auch die §§ 202a ff. StGB schützen den Verfügungsberechtigten in seinem formellen Geheimhaltungsinteresse bzw. seiner Verfügungsmacht hinsichtlich der in den Daten enthaltenen Informationen¹¹⁶.

Um den „Verfügungsbefugten“ zu ermitteln, ist es notwendig, eine Zuordnung von Daten zu einem Berechtigten im Sinne dieser Vorschrift vorzunehmen. Mangels einer Begrenzung auf Tatobjekte, die dem Täter fremd sind, bedarf es einer Einschränkung des Tatbestandes insofern, dass nur Daten erfasst sind, an denen einer anderen Person als dem

107 BGH, GRUR 2011, 724 (726); Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 87b Rn. 7.

108 Dazu unten Kapitel 3.2.4.

109 EuGH, Rs. C-203/02, ECLI:EU:C:2004:695 Tz. 91 – The British Horseracing Board Ltd; Vogel, in: Schricker/Loewenheim (Hrsg.), UrhG, 4. Aufl. 2010, § 87b Rn. 52; Thum/Hermes, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87b Rn. 66.

110 Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 87b Rn. 13; Thum/Hermes, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87b Rn. 66.

111 Data-Mining bezeichnet die Analyse großer Datensätze mit dem Ziel, für Entscheidungsträger relevante Muster und Zusammenhänge aufzudecken. Durch die Filterung, Extraktion und Aggregation von Daten, können aus der Untersuchung großer Datenbestände unternehmensrelevante Erkenntnisse gewonnen werden.

112 Auer-Reinsdorff, in: Conrad/Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, § 15 Rn. 35; Zieger/Smirra, MMR 2013, 418 (420); Thum/Hermes, in: Wandtke/Bullinger (Hrsg.), UrhG, 4. Aufl. 2014, § 87b Rn. 100.

113 Art. 3 im Entwurf der EU-Kommission vom 14.9.2016 für eine Directive on copyright in the Digital Single Market, COM(2016) 593 final; Schack, ZUM 2016, 266 (268 f.).

114 So allgemein Schack, UrhR, 7. Aufl. 2015, Rn. 742; Dorner, CR 2014, 617 (622 f.).

115 OLG Nürnberg, CR 2013, 212.

116 Weidemann, in: BeckOK StGB, § 202a Rn. 2; § 202b Rn. 2.

Täter ein unmittelbares rechtlich schutzwürdiges Interesse in Form einer **eigentümerähnlichen Verfügungsbefugnis** zusteht¹¹⁷.

Wem diese zustehen soll, regelt die Strafnorm hingegen nicht – vielmehr wird deren Existenz vorausgesetzt. Nach der Rechtsprechung stehe die Datenverfügungsbefugnis dabei grundsätzlich demjenigen zu, der die Speicherung der Daten unmittelbar selbst bewirkt hat¹¹⁸. Damit ist die Rechtsprechung der in der Literatur unter dem Oberbegriff des „**Skripturakts**“ diskutierten Ansicht gefolgt. *Welp* prägte schon 1988 in einem Aufsatz diesen Begriff und definierte den Skribenten als denjenigen, der die Daten erzeugt, also ihre Speicherung oder Übermittlung selbst unmittelbar bewirkt hat, sei es durch Eingabe der Daten, sei es durch den Start eines selbsttätig speichernden Programms oder durch Bewirkung der Einspeisung externer Daten¹¹⁹. Im Rahmen dieser Definition des Skribenten bleibt unklar, ob es eher auf die Speicherung oder Übermittlung ankommt. Ein Abstellen auf die erstmalige Übermittlung bietet sich lediglich in Fällen an, in denen der Datenerzeuger die Daten direkt ohne vorhergehende Speicherung weiterüberträgt. Für die Frage der Verfügungsmacht ist weder das Eigentum am Datenträger noch ein etwaiger inhaltlicher Personenbezug maßgeblich, sondern sie wird beim erstmaligen Erstellen mit dem Abspeichern begründet¹²⁰.

Da die strafrechtlich geschützte Rechtsposition als übertragbar gilt, kann ein wirtschaftlicher Zuweisungsgehalt angenommen werden¹²¹. Das Recht des Berechtigten an den Daten wird zum Teil als eigentumsähnliches Herrschaftsrecht, d. h. als Vollrecht in Analogie zu § 903 BGB ausgelegt¹²². Die strafrechtlich geschützte Berechtigung an den Daten habe Vorbildfunktion und sei im Sinne der **Einheit der Rechtsordnung** auf den zivilrechtlichen Bereich zu übertragen.

Richtigerweise existiert die beschriebene „Datenberechtigung“ bislang – und dies auch nicht ausdrücklich – lediglich im Bereich des Strafrechts und schützt den Berechtigten in dem Ausschluss der Benutzung der Daten durch

unerwünschte Dritte. Von den denkbaren zuweisbaren Handlungsbefugnissen wird einer Person lediglich das **Recht auf Schutz vor Beeinträchtigung der Integrität von Daten** indirekt zugewiesen; bezüglich des Rechts auf Zugang zu den Daten oder der Nutzung der Daten trifft der vorgenannte Straftatbestand keine Regelung¹²³. Hierin eine generelle Güterzuordnung zu sehen, liegt auf Grund der diversen Zuordnungsmöglichkeiten des Gesetzgebers, die auch in der Literatur zu § 303a StGB diskutiert wurden, fern. Die Rechtsprechung mag bezogen auf einzelne strafrechtliche Normen dem Ansatz des Skripturakts gefolgt sein, jedoch kann dies nicht verallgemeinert werden. Zur Existenz eines Ausschließlichkeitsrechts an Daten bedürfte es der Zuordnung ebendieser als Vermögensgegenstand zu einer Person im Sinne einer Güterzuordnung durch die Rechtsordnung¹²⁴.

Dies zeigt auch der Umstand, dass es bereits eine strafrechtliche Regelung gibt, in deren Rahmen ein anderer Zuordnungsmechanismus gilt. Mit § 17 UWG existiert eine Vorschrift des Nebenstrafrechts, die in Form des Geheimnisschutzes ebenfalls ein Handlungsverbot im Zusammenhang mit Daten statuiert. Die Norm schützt den Geheimbereich eines Unternehmens vor einem unredlichen Eingriff und gibt somit dem Unternehmensinhaber die Möglichkeit, durch faktische Geheimhaltung Dritte von der Nutzung eines Datums in rechtmäßiger Weise auszuschließen. Das Verhältnis der diversen bereichsspezifisch normierten Rechte zueinander ist in vielen Fällen ungeklärt¹²⁵. Bezüglich des Verhältnisses des Skribenten zu dem gem. § 17 UWG geschützten Unternehmensinhaber dürfte es sich in der Praxis – sofern man im Rahmen von Arbeitsverhältnissen den Arbeitgeber als Skribenten ansieht – um dieselbe Person handeln. Sollten Skribent und Unternehmensinhaber tatsächlich personenverschieden sein, handelt es sich *de lege lata* zum einen um unterschiedliche Schutzgüter (Integrität der Daten bzw. Geheimheit der Daten) und zum anderen kann mit der Nutzung des Datums durch den verfügbungsbefugten Skribenten im Falle einer damit verbundenen Offenkundigkeit des Datums der Schutz des Unternehmensinhabers nach § 17 UWG entfallen¹²⁶.

117 *Weidemann*, in: BeckOK StGB, § 303a Rn. 4 f.

118 OLG Nürnberg, CR 2013, 212.

119 *Welp*, iur 1988, 443 (447).

120 *Weidemann*, in: BeckOK StGB, § 202a Rn. 8.

121 *Zech*, GRUR 2015, 1151 (1159).

122 *Hilgendorf*, JuS 1996, 890 (892 f.); *Welp*, IuR 1988, 443 (448); *Wolf*, MMR 2003, S. XVI; *Hoeren*, MMR 2013, 486 (487).

123 *Zech*, CR 2015, 137 (139).

124 *Zech*, CR 2015, 137 (140).

125 *Heun/Assion*, Internetrecht der Dinge, Vortrag im Rahmen der Telemedicus Sommerkonferenz 2015, Präsentation abrufbar unter: https://www.telemedicus.info/uploads/Heun_Assion_InternetrechtderDinge.pdf.

126 Zum lauterkeitsrechtlichen Schutz siehe auch sogleich unter 3.2.4.

Einigkeit besteht darüber, dass die „eigenen“ Daten aufgrund der sonstigen Einbeziehung strafunwürdiger Verhaltensweisen nicht Schutzgut der Norm sein können¹²⁷. Die vorgenannte Einschränkung wird im Rahmen des § 303a StGB nach herrschender Ansicht über das Tatbestandsmerkmal der „Rechtswidrigkeit“ konstruiert¹²⁸. Nach einer anderen Ansicht ist die Fremdheit der Daten als ungeschriebenes Tatbestandsmerkmal und der Begriff „rechtswidrig“ als allgemeines Verbrechensmerkmal einzuordnen¹²⁹. Dies gilt auch für die §§ 202a ff. StGB, die jedoch ein entsprechendes Tatbestandsmerkmal („nicht für den Täter bestimmt“) aufweisen, das den Willen des Berechtigten zum Umgang des Täters mit den Daten als tatbestandsausschließend einbezieht.

Das Erfordernis einer Herrschaftsbeziehung von dem zu ermittelnden Berechtigten zu seinen Daten und die damit verbundene **nähere Beziehung des Straftatbestands zu den Eigentumsdelikten im Gegensatz zu den Persönlichkeitsrechtsdelikten** drückt sich auch in der systematischen Stellung dieser Vorschrift direkt nach der Sachbeschädigung aus¹³⁰. Der Berechtigte wird jedoch nur vor vorsätzlichem Löschen, Unterdrücken, Unbrauchbarmachen und Verändern seiner Daten geschützt; insoweit wird das Bestehen erheblicher Schutzlücken kritisiert¹³¹, insbesondere da sich die Verfügungsbefugnis des Berechtigten bei unerlaubter Kopie von Daten nicht fortsetzt¹³². Eine der Schutzlücken wurde durch den neu eingefügten § 202d StGB geschlossen, der das formelle Datengeheimnis vor einer Fortsetzung und Vertiefung seiner durch eine entsprechende Vortat erfolgten Verletzung schützt¹³³.

In der Praxis bereitet die konkrete Bestimmung der Person des Skribenten jedoch Schwierigkeiten; insoweit ist der Ansatz der Zuordnung nach dem Skripturakt noch nicht gänzlich ausgereift. Insbesondere bei maschinengenerierten Daten ist die Person des „Datenerstellers“ nicht eindeutig festzustellen. Skribent soll grundsätzlich derjenige sein, der durch Eingabe oder Ausführung eines Programms

Daten selbst erstellt¹³⁴ bzw. der die Erstabspeicherung – den Skripturakt – vorgenommen hat¹³⁵. In Bezug auf fahrzeugbezogene Daten kommen grundsätzlich zwei Akteure, namentlich der Nutzer, der eine konkrete Fahrt tätigt, als auch der „Herr“ der entsprechenden speichernden Programmautomatik als Datenersteller, in Betracht.

Während nach einer Ansicht strikt auf den technischen Vorgang der Datenerstellung abzustellen sei¹³⁶, könnten nach einer anderen Ansicht auch andere Faktoren, z. B. wirtschaftliche Gesichtspunkte, maßgeblich für die Zuordnung eines Datums sein¹³⁷. Dies führt jedoch bspw. im Rahmen von Auftrags- oder Arbeitsverhältnissen zu unterschiedlichen Ergebnissen, da sich im ersten Fall eine Berechtigung des Auftragnehmers bis zur Aushändigung ergibt¹³⁸, während bei wertender Betrachtung die Daten dem wirtschaftlich verantwortlichen Auftraggeber zuzuordnen sind¹³⁹.

Die Untersuchung der Fallstudien nach der bereichsspezifischen Regelung ergibt, dass die Daten dem **technischen Datenersteller**, der die Codierung bzw. die Erstabspeicherung veranlasst hat, zuzuweisen sind. Aufgrund der vorgenannten Schwierigkeiten, den Datenersteller in der Praxis konkret zu benennen, kann zum Teil jedoch keine eindeutige Aussage getroffen werden (für eine detaillierte Untersuchung aller Fallstudien, siehe Anhang II.iv.).

Bei den getroffenen Zuordnungen gilt es zu berücksichtigen, dass die Zuordnung nicht im Sinne eines umfassenden, eigentumsähnlichen Ausschließlichkeitsrechts erfolgt, sondern mit der Zuordnung der Berechtigte lediglich vor den in den Strafnormen aufgeführten Tathandlungen durch unberechtigte Dritte geschützt wird. Die Verfügungsmacht des Berechtigten bezieht sich bislang lediglich auf den strafrechtlichen Bereich und schützt vor unerwünschten, strafbewehrten Beeinträchtigungen. Insbesondere zu positiven Nutzungsrechten treffen die genannten Strafnormen keine Regelung.

127 Weidemann, in: BeckOK StGB, § 303a Rn. 5.

128 Weidemann, in: BeckOK StGB, § 303a Rn. 5 f.; Lackner/Kühl, StGB, § 303a Rn. 4; Hoyer, in: SK-StGB, § 303a Rn. 2, 12; Popp, JuS 2011, 385 (388); Hilgendorf, JuS 1996, 890 (892 f.); Sasdi, CR 2005, 235 (238); Kitz, CR 2005, 450 (453); Hilgendorf/Valerius, Strafrecht AT, Rn. 598; Spannbrucker, Convention on Cybercrime (ETS 185), S. 70; vgl. auch BT-Drs. 10/5058, S. 34.

129 Fischer, StGB, § 303a Rn. 13; Stree/Hecker, in: Schönke/Schröder (Hrsg.), StGB, § 303a Rn. 4; Lenckner/Winkelbauer, CR 1986, 824 (828).

130 Hoeren, MMR 2013, 486 (486).

131 Specht, CR 2016, 288 (289); Faust, NJW-Beil. 2016, 29 (32); a. A. Stree/Hecker, in: Schönke/Schröder (Hrsg.), StGB, § 303a Rn. 4.

132 OLG Nürnberg, CR 2013, 212; Fischer, StGB, § 303a Rn. 6; Wolff, in: LK-StGB, § 303a Rn. 16;

133 Weidemann, in: BeckOK StGB, § 202d Rn. 2; BR-Drs. 249/15, S. 49; Franck, RDV 2015, 180; Forgó/Heermann, KuR 2015, 753 (759).

134 Hoeren, MMR 2013, 486 (487).

135 Zech, CR 2015, 137 (143).

136 Hoeren, MMR 2013, 486 (487).

137 Zech, CR 2015, 137 (143 f.); Specht, CR 2016, 288 (294).

138 Hoeren, MMR 2013, 486 (487); OLG Nürnberg, ZD 2013, 282 m. Anm. Schröder.

139 Zech, GRUR 2015, 1151 (1159); Zech, CR 2015, 137 (144); Specht, CR 2016, 288 (294).

3.2.4 (Lauterkeitsrechtlicher) Schutz von Betriebs- und Geschäftsgeheimnissen

Vor allem die zahlreichen technikbezogenen Daten in den gezeigten Fallstudien gehören zum **Know-how** der speichernden Unternehmen¹⁴⁰. Die darin enthaltenen Informationen können Betriebs- und Geschäftsgeheimnisse sein, für die Art. 39 Abs. 1 TRIPS¹⁴¹ einen lauterkeitsrechtlichen Mindestschutz in den Vertragsstaaten verlangt¹⁴². Auf der Ebene der EU wird künftig die am 08.06.2016 erlassene Richtlinie 2016/943 (Geschäftsgeheimnis-RL)¹⁴³ die nationalen Vorschriften der Mitgliedstaaten zum Schutz von Geschäftsgeheimnissen weiter harmonisieren¹⁴⁴. Mit Blick auf die der Studie zu Grunde liegende Diskussion über „Eigentumsrechte an Daten“ macht die Richtlinie jedoch keine Vorgaben¹⁴⁵.

In Deutschland schützen bislang die §§ 17 bis 19 UWG strafrechtlich Unternehmensgeheimnisse vor dem Verrat durch eigene Mitarbeiter (§ 17 Abs. 1 UWG), der Betriebsespionage (§ 17 Abs. 2 Nr. 1 UWG), der Geheimnishehlerei (§ 17 Abs. 2 Nr. 2 UWG) und dem Verleiten bzw. Erbieten zum Verrat (§ 19 UWG). Die genannten Strafnormen schützen die **Vertraulichkeit** geheimer betriebsbezogener Informationen¹⁴⁶. Bei deren Verletzung können den geschützten Geheimnisträgern zivilrechtliche Schadens- (§ 823 Abs. 2 BGB) und Abwehransprüche (§ 1004 BGB analog) zustehen¹⁴⁷. Obgleich Unternehmensgeheimnisse einen enormen Wert haben¹⁴⁸ und verwertet werden können¹⁴⁹, ist die Geheimheit dieses Wissens nur eine faktische Position, die das Lauterkeitsrecht rechtlich absichert. Anders als bei klassischen Immaterialgüterrechten wird das Geheimnis

dessen Träger aber nicht abstrakt zugewiesen¹⁵⁰, was auch die RL 2016/943 nicht ändern wird¹⁵¹.

Der strafrechtliche Schutz nach § 17 UWG setzt in allen Handlungsalternativen voraus, dass Informationen ein **Geschäfts- bzw. Betriebsgeheimnis** darstellen. Auf den Personenbezug im datenschutzrechtlichen Sinne kommt es insoweit nicht an.

Anders als der neue Art. 2 Abs. 1 RL 2016/943 definiert das deutsche Recht den Begriff des Geschäfts- und Betriebsgeheimnisses nicht¹⁵². Die ständige Rechtsprechung fasst darunter jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheim gehalten werden soll¹⁵³.

Als Geschäftsgeheimnisse müssen Informationen ferner hinreichend deutlich einem Unternehmen zugeordnet werden können¹⁵⁴. Dieser **Unternehmensbezug** fehlt etwa bei Tatsachen, die die Sphären Dritter betreffen¹⁵⁵. Die Zugangsdaten der Kunden des *Carsharing*-Anbieters und die Informationen über deren gefahrene Strecken (Fallstudie 2) sind daher ebenso wenig Geschäftsgeheimnisse, wie die Positionsdaten aus Fallstudie 4 und die Telefonbücher, die die Nutzer von ihren Smartphones auf die Mobilitätsdienstesteplattform in ihrem Fahrzeug übertragen (Fallstudie 3). Die aus den *Car-2-X*-Nachrichten erzeugten Lagebilder eignen sich dagegen als eigenständiges Wirtschaftsgut, das dem Betrieb des Infrastrukturbetreibers wohl zugeordnet werden kann¹⁵⁶. Auch interne Messdaten von Maschinen

140 Zum Begriff „Know-how“ *Gennen*, in: Conrad/Grützmacher (Hrsg.), *Recht der Daten und Datenbanken im Unternehmen*, § 13 Rn. 5 ff.

141 Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums, Anhang 1 C des Übereinkommens zur Errichtung der Welthandelsorganisation (WTO) vom 15.4.1994, BGBl. II 1994, S. 1625.

142 *Ohly*, GRUR 2014, 1 (4).

143 RL (EU) 2016/943 vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. 2016 L 157, S. 1.

144 Zum bisherigen Schutz in der EU *Ohly*, in: *Ohly/Sosnitza* (Hrsg.), *UWG*, 7. Aufl. 2016, Vorb. §§ 17–19 Rn. 7 f. Den Umsetzungsbedarf zeigt *Kalbfus*, GRUR 2016, 1009 ff.

145 *Hauck*, NJW 2016, 2218 (2221).

146 Zerstören Mitbewerber gezielt Daten ihrer Konkurrenten handeln sie zudem unlauter i.S.v. § 4 Nr. 4 UWG, was die Ansprüche aus den §§ 8 ff. UWG auslöst, vgl. auch *Schefzig*, K&R Beiheft 3/2015, 3 (4 f.).

147 Zu den zivilrechtlichen Folgen der Verstöße gegen die §§ 17 ff. UWG *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), *UWG*, 34. Aufl. 2016, § 17 Rn. 51 ff.

148 *ErwGr.* 1 und 2 RL 2016/943.

149 Vgl. nur *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), *UWG*, 34. Aufl. 2016, Vorb. §§ 17–19 Rn. 3 f.

150 *Ohly*, GRUR 2014, 1 (3 f.); *Ann*, GRUR 2007, 39 ff.; *Harte-Bavendamm*, in: *Harte-Bavendamm/Henning-Bodewig* (Hrsg.), *UWG*, 3. Aufl. 2013, Vorb. §§ 17–19 Rn. 2; *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), *UWG*, 34. Aufl. 2016, Vorb. §§ 17–19 Rn. 2; *Zech*, GRUR 2015, 1151 (1156).

151 *ErwGr.* 16 RL 2016/943. *Hauck*, NJW 2016, 2218 (2221).

152 Inhaltlich decken sich das deutsche Verständnis und die Begriffsdefinition aus der Geschäftsgeheimnis-RL 2016/943 weitgehend, *Kalbfus*, GRUR 2016, 1009 (1010).

153 BGH, GRUR 2009, 603 (604) m.w.N.; *Harte-Bavendamm*, in: *Harte-Bavendamm/Henning-Bodewig* (Hrsg.), *UWG*, 3. Aufl. 2013, § 17 Rn. 1.

154 Zum Unternehmensbezug vgl. Art. 39 Abs. 2 TRIPS „information lawfully within their control“.

155 *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), *UWG*, 34. Aufl. 2016, § 17 Rn. 5; *Brammsen*, in: *MüKo UWG*, 2. Aufl. 2014, § 17 Rn. 14.

156 Vgl. allgemein *Brammsen*, in: *MüKo UWG*, 2. Aufl. 2014, § 17 Rn. 13.

können den nötigen Bezug zum Betrieb des Herstellers aufweisen¹⁵⁷, so dass die Diagnosedaten der Sensoren aus den Fahrzeugen (Fallstudie 1) und deren Bewegungsprofile (Fallstudie 2) mögliche Gegenstände von Unternehmensgeheimnissen sind. Die in einem Gerät enthaltenen Unternehmensgeheimnisse büßen diesen Bezug auch nicht dadurch ein, dass sie öffentlich vertrieben werden¹⁵⁸.

Die jeweiligen Informationen werden jedoch nur dann geschützt, wenn sie geheim sind. Dazu darf das Wissen **nicht offenkundig** sein, also weder allgemein bekannt, noch leicht zugänglich sein¹⁵⁹. Leicht zugänglich sind Informationen, von denen sich jeder Interessierte außerhalb der Betriebe mit den entsprechenden Kenntnissen und Fähigkeiten der betroffenen Fachkreise ohne größere Schwierigkeiten mit lauterem Mitteln Kenntnis verschaffen kann¹⁶⁰. Die Diagnosedaten in Fallstudie 1 bspw. können über die OBD-Schnittstelle am Fahrzeug ausgelesen¹⁶¹ werden und sind damit offenkundig. Selbst, wenn die jeweiligen Fachkreise ohne erheblichen Aufwand im Rahmen des *Reverse Engineering* Daten auslesen können, geht dies zu Lasten des Geheimnisinhabers¹⁶², so dass die Fahrzeugdaten über die gezeigten Fallbeispiele hinaus nicht geheim sind. Kein Geheimnis sind Informationen ferner dann, wenn der Wissensinhaber oder Dritte sie allgemein bekannt machen, indem sie diese in allgemein zugänglichen Medien, wie dem Internet oder Fachzeitschriften veröffentlichen¹⁶³. Gibt der Infrastrukturbetreiber seine Lagebilder (Fallstudie 5) im Rahmen von *Open-Data*-Initiativen frei oder an Anbieter von Drittanwendungen weiter, genießen sie keinen Geheimnisschutz (mehr). Das Geheimnis wahrt der Inhaber bei der Weitergabe des Wissens an Dritte nur dann, wenn diese (vertraglich) zur Verschwiegenheit verpflichtet sind¹⁶⁴. Die Offenkundigkeit ist also die Achillesverse des lauterkeitsrechtlichen Geheimnisschutzes, da deren Inhaber seinen Schutz verliert, soweit jemand das Wissen einem grö-

ßeren Personenkreis offenbart. Dies gilt selbst dann, wenn die Informationen durch Verrat offenbart werden¹⁶⁵.

Im Übrigen setzt das Unternehmensgeheimnis voraus, dass der Betriebsinhaber einen entsprechenden **Willen zur Geheimhaltung** hat. Hieran werden jedoch keine hohen Anforderungen gestellt und der entsprechende Wille für alle innerbetrieblichen Vorgänge vermutet¹⁶⁶. Auch für das darüber hinaus nötige **Geheimhaltungsinteresse** genügt jedes berechnigte wirtschaftliche Interesse des Geheimnisträgers¹⁶⁷.

Zusammenfassend sind die Daten in den hier betrachteten Fallstudien **weitestgehend keine Betriebs- und Geschäftsgeheimnisse**. In vielen anderen Szenarien fallen Mobilitätsdaten dagegen unter den lauterkeitsrechtlichen Geheimnisschutz¹⁶⁸, der jedoch nur einen unzureichenden Rechtsrahmen bildet¹⁶⁹. Die §§ 17 bis 19 UWG schützen dann zwar die Vertraulichkeit der Informationen. Der Geheimnisträger verliert diesen Schutz aber, wenn er oder ein Dritter das Wissen offenbart. Vor allem aber bietet das UWG kein echtes Ausschließlichkeitsrecht für Daten, sondern verstärkt nur rechtlich die faktische Geheimheit betriebsinterner Informationen (für eine detaillierte Untersuchung aller Fallstudien, siehe Anhang II.v.).

3.2.5 Allgemeines Zivilrecht

3.2.5.1 Daten als Eigentum i. S. d. § 903 BGB

Aus zivilrechtlicher Perspektive legt der Begriff „Dateneigentum“ nahe, sich zunächst mit den Vorgaben des BGB zum Sacheigentum (§§ 903 ff. BGB) zu befassen. An erster Stelle ist zu klären, ob Daten eine rechtliche Absicherung über das sachenrechtliche Rechtsregime erfahren haben.

157 *Schefzig*, K&R Beiheft 3/2015, 3 (4); vgl. auch OLG Stuttgart, GRUR 1982, 315 (316).

158 *Ohly*, in: *Ohly/Sosnitza* (Hrsg.), UWG, 7. Aufl. 2016, § 17 Rn. 6; *Harte-Bavendamm*, in: *Harte-Bavendamm/Henning-Bodewig* (Hrsg.), UWG, 3. Aufl. 2013, § 17 Rn. 2; *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), UWG, 34. Aufl. 2016, § 17 Rn. 5; a.A. *Dorner*, Know-how-Schutz im Umbruch, 2013, S. 130.

159 *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), UWG, 34. Aufl. 2016, § 17 Rn. 6.

160 *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), UWG, 34. Aufl. 2016, § 17 Rn. 8; *Ohly*, in: *Ohly/Sosnitza* (Hrsg.), UWG, 7. Aufl. 2016, § 17 Rn. 10; *Harte-Bavendamm*, in: *Harte-Bavendamm/Henning-Bodewig* (Hrsg.), UWG, 3. Aufl. 2013, § 17 Rn. 3.

161 In den Fallstudien lesen z. B. die Werkstätten (Fallstudie 1) und der Mobilitätsdiensteanbieter (Fallstudie 3) die Fahrzeugdaten aus.

162 *Ohly*, in: *Ohly/Sosnitza* (Hrsg.), UWG, 7. Aufl. 2016, § 17 Rn. 10.

163 *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), UWG, 34. Aufl. 2016, § 17 Rn. 7.

164 *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), UWG, 34. Aufl. 2016, § 17 Rn. 7a.

165 *Harte-Bavendamm*, in: *Harte-Bavendamm/Henning-Bodewig* (Hrsg.), UWG, 3. Aufl. 2013, § 17 Rn. 4.

166 *Köhler*, in: *Köhler/Bornkamm* (Hrsg.), UWG, 34. Aufl. 2016, § 17 Rn. 10; *Harte-Bavendamm*, in: *Harte-Bavendamm/Henning-Bodewig* (Hrsg.), UWG, 3. Aufl. 2013, § 17 Rn. 5. Zu den Änderungen durch die Geschäftsgeheimnis-RL 2016/943, *Hauck*, NJW 2016, 2218 (2220).

167 *Ohly*, in: *Ohly/Sosnitza* (Hrsg.), UWG, 7. Aufl. 2016, § 17 Rn. 12. Über das allgemeine Geheimhaltungsinteresse hinaus fordert Art. 2 Nr. 1 lit. b Geschäftsgeheimnis-RL künftig, dass die geschützten Informationen einen kommerziellen Wert haben. Den Harmonisierungsgrad der Richtlinie diskutiert mit Blick auf den Begriff des „Geschäftsgeheimnisses“ *Kalbfus*, GRUR 2016, 1009 (1011).

168 Vgl. *Zech*, GRUR, 2015, 1151 (1155).

169 *Zech*, GRUR 2015, 1151 (1156). Vgl. auch *Grützmacher*, CR 2016, 485 (488); *Dorner*, CR 2014, 617 (623).

Festzustellen ist dabei zunächst, dass Daten keine Sachen i. S. d. § 90 BGB sind. Hierzu zählen nur **körperliche Gegenstände** (in den drei möglichen Aggregatzuständen fest, flüssig und gasförmig), worunter zwar das physische Trägermedium¹⁷⁰ fällt, auf dem sich die Daten befinden, nicht aber die einzelnen Daten als solche, die letztlich nur elektrische Spannungszustände bilden. § 903 S. 1 BGB regelt daher jedenfalls nicht direkt die Beziehung von Personen zu Daten¹⁷¹.

3.2.5.2 Eigentumsschutz durch § 823 BGB

Daten werden zudem über das Deliktsrecht nur lückenhaft geschützt. Eine Verletzung des nach § 823 Abs. 1 BGB geschützten **Eigentums** allgemein beim Datenverlust wird aufgrund der angesprochenen fehlenden Körperlichkeit der in Rede stehenden Daten nach herrschender und zutreffender Ansicht abgelehnt¹⁷². Überwiegend bejaht wird allerdings die Annahme einer Eigentumsverletzung bei der Veränderung eines Datenträgers¹⁷³. Denn über das Deliktsrecht wird nach geltender Rechtsprechung mittelbar die Integrität der verkörperten Daten über das zivilrechtliche Eigentum am Datenträger geschützt. Für die Annahme einer Eigentumsverletzung genügt daher die Beeinträchtigung der in der Sache fixierten Benutzbarkeit¹⁷⁴. Das Löschen oder Verändern von Daten auf Datenträgern stellt folglich eine Sachbeschädigung dar¹⁷⁵. In der Folge wird der Eigentümer des betreffenden Trägermediums geschützt.

Da die Berechtigung an den Daten und das Eigentum am Trägermedium auseinanderfallen können, besteht jedoch in der Praxis das Bedürfnis nach Schutz des zum Umgang mit den Daten Befugten vor Datenverlust. Weitergehender Schutz ist lediglich rudimentär über § 823 Abs. 2 i. V. m. be-

reichsspezifischen Regelungen, z. B. § 202a StGB oder § 17 UWG, gegeben. Schutzlücken ergeben sich vor allem bei fahrlässigen Beschädigungen von Daten, die sich auf Datenträgern befinden, die nicht im Eigentum des Datenspeichernden stehen¹⁷⁶.

3.2.5.3 Sachgenerierte Daten als Früchte

Fraglich ist, ob Daten als „Früchte“ i. S. d. BGB angesehen werden können. Dies wird in der Literatur zum Teil zu Unrecht angenommen¹⁷⁷. Unmittelbare Rechtsfrüchte¹⁷⁸ nach § 99 Abs. 2 BGB sind per definitionem Erträge, die ein Recht seiner Bestimmung nach gewährt, während unmittelbare Sachfrüchte¹⁷⁹ nach § 99 Abs. 1 BGB die Erzeugnisse einer Sache sind. Früchte aus dem Eigentum an einer Sache (wie dem datengenerierenden Gegenstand) fallen unter § 99 Abs. 1 BGB¹⁸⁰. Bei maschinengenerierten Daten kann es sich jedoch nicht um Früchte i. S. d. Vorschrift handeln, da sich Maschinen weder ausbeuten lassen noch Erzeugnisse abwerfen¹⁸¹. Eine unmittelbare Anwendung des § 99 BGB scheitert folglich daran, dass es sich bei Daten weder um einen typischen Fall der Rechts- (§ 90 Abs. 2 BGB) noch der Sachfrüchte (§ 90 Abs. 1 BGB) handelt, die bestimmungsgemäß aus einer Sache gewonnen werden¹⁸².

3.2.5.4 Sachgenerierte Daten als Nutzungen

Die Verwendung einer Sache zur Erstellung von Daten sowie zur Weiterverwendung der gewonnenen Daten könnte jedoch als ein **Gebrauchsvorteil** dieser Sache zu qualifizieren sein. Nach § 100 BGB zählen Gebrauchsvorteile zu den Nutzungen, die bei Fehlen anderweitiger Regelungen dem Eigentümer der Sache zustehen (§ 903 BGB)¹⁸³. Mit der Einordnung der Datenerzeugung als Gebrauchsvorteil

170 Bspw. Server; Smartphones, Festplatten; USB-Sticks etc.

171 Sahl, PinG 2016, 146 (148); zur Frage der Ausweitung des engen Sachbegriffs siehe Wendehorst, NJW 2016, 2609 (2609).

172 LG Konstanz NJW 1996, 2662 ff.; a. A. Rombach, CR 1990, 101 (104).

173 OLG Karlsruhe NJW 1996, 200 ff.; Hoeren, in: Graf von Westphalen (Hrsg.), Vertragsrecht und AGB-Klauselwerke, IT-Verträge Rn. 84; a. A. Gerstenberg, NJW 1956, 530 ff.

174 Härtling, CR 2016, 646 (647).

175 Bartsch, CR 2010, 553 (554).

176 Siehe hierzu sowie zu entsprechenden Verbesserungsvorschlägen ausführlich unter 5.2.5.

177 So etwa Grosskopf, der die Auffassung vertritt, dass die erzeugten Geo- und Telemetriedaten dem Eigentümer des Fahrzeugs als „Früchte“ desselben gebührten. Er gibt aber zu Recht zu bedenken, dass die Nutzung durch den Berechtigten trotz dessen starker Rechtsposition aufgrund des geltenden Datenschutzrechts weiterhin unter dem Vorbehalt der Einwilligung des jeweiligen Fahrzeugnutzers stünde Grosskopf, IPRB 2011, 259 (260).

178 Beispiele für unmittelbare Rechtsfrüchte sind die Jagdbeute, Erträge aus Nießbrauch, Pacht oder Reallast, Gewinnanteile aus Gesellschaftsanteilen, Zinsen einer Kapitalforderung sowie monatliche Rentenleistungen, vgl. Fritzsche, in: Bamberger/Roth (Hrsg.), BeckOK BGB, § 99 Rn. 10.

179 Beispiele für unmittelbare Sachfrüchte sind Eier, Milch, Wolle und Nachwuchs als Tierprodukte, Jungpflanzen und Bäume als Bodenprodukte sowie Obst, Beeren und Getreide als Pflanzenprodukte, vgl. Fritzsche, in: Bamberger/Roth (Hrsg.), BeckOK BGB, § 99 Rn. 4.

180 Fritzsche, in: Bamberger/Roth (Hrsg.), BeckOK BGB, § 99 Rn. 10; Jickeli/Stieper, in: Staudinger (Hrsg.), BGB, § 99 Rn. 11.

181 Specht/Rohmer, PinG 2016, 127 (131).

182 Ob eine analoge Anwendung in Betracht kommt, wird unter 5.1.1.3. geprüft.

183 Heun/Assion, CR 2015, 812 (818); Bassenge, in: Palandt (Hrsg.), BGB, § 903 Rn. 5; Ellenberger, in: Palandt (Hrsg.), BGB, § 100 Rn. 1; OLG Naumburg v. 27.8.2014 – 6 U 3/14, Rn. 24 ff.

der datengenerierenden Sache wird das Erstnutzungsrecht dem Eigentümer der Sache zugewiesen. Darauf aufbauend ließen sich vertragliche Absprachen treffen, mittels derer das Nutzungsrecht auf Dritte übertragen werden kann¹⁸⁴.

Allerdings unterscheiden sich Daten grundlegend von dem typischen Erscheinungsbild der sonstigen von § 100 BGB erfassten Gebrauchsvorteile einer Sache. Es handelt sich bei den Gebrauchsvorteilen üblicherweise um sich verflüchtigende Vorteile, die aus dem Umgang mit einem Gegenstand resultieren und mit diesem eng verknüpft sind. Daten hingegen existieren dauerhaft, können beliebig vervielfältigt und übertragen werden und unterliegen diversen bereichsspezifischen, rechtlichen Regelungen. Daher lassen sich Daten nicht als Gebrauchsvorteil einer Sache einordnen.

3.2.5.5 Zwischenfazit zum allgemeinen Zivilrecht

Festhalten lässt sich, dass sich aus dem allgemeinen Zivilrecht keine umfassende Zuordnung der immateriellen Daten zu einem Berechtigten ergibt. Deliktischer Schutz besteht ausschließlich in Form von Integritätsschutz als Reflex des Eigentums am Datenträger. Weitergehender Schutz ist bei Verletzung bereichsspezifischer Regelungen über § 823 Abs. 2 BGB gegeben.

3.2.6 Fazit: Kein „Dateneigentum“ *de lege lata*

Es lässt sich also festhalten, dass *de lege lata* Daten zwar durch verschiedene Regelungsregime geschützt werden. Diese haben aber eigene unterschiedliche Voraussetzungen, Schutzzumfänge und Verfügungsberechtigte, die gemäß ihren jeweiligen Zielen, gegenläufige Zuordnungen vorsehen, für die keine Kollisionsregeln bestehen und diese somit unter Umständen im Widerspruch zueinander stehen können.

Daher besteht im geltenden Recht kein homogenes „Dateneigentum“¹⁸⁵, sondern ein „Flickenteppich“¹⁸⁶ divergierender Schutzrechte. Die in den Fallstudien beteiligten Akteure können deshalb oft nicht – jedenfalls nicht ohne erheblichen Aufwand – rechtssicher feststellen, ob Schutzrechte bestehen und welche Personen hierüber gegebenenfalls verfügen können. Dieser Flickenteppich durch bereichsspezifische Regelungen erschwert in der Praxis erheblich die Verwertung der in den Fallstudien beschriebenen Daten. Konkret wird dies in den komplexen Verarbeitungskonstellationen der digitalen Mobilität sichtbar (siehe auch Abbildung 16), indem verschiedene Akteure mit rechtlich geschützten Interessen gefunden werden können, wie bspw. der **datenschutzrechtlich Betroffene** in Form des Halters des Kfz (§ 4 BDSG), der **Skribent** in Person des Fahrers (§ 303a StGB) sowie Unternehmen der Automobilbranche durch Vorliegen von **Betriebs- und Geschäftsgeheimnissen** (§ 17 UWG) und zuletzt der **Eigentümer des Datenträgers**, der meist ein von dem Unternehmen beauftragter *Cloud*-Anbieter ist. Der Betroffene i. S. d. BDSG kann bei Fehlen einer gesetzlichen Legitimation jegliche Verarbeitung der auf ihn bezogenen Daten durch Verweigerung der Abgabe einer Einwilligungserklärung unterbinden. Der Skribent hingegen ist strafrechtlich in der unbeeinträchtigten Verwendbarkeit der von ihm gespeicherten Daten geschützt, während § 17 UWG den Betriebsinhaber vor Verletzungen seiner Geheimhaltungsinteressen in Bezug auf die das Geheimnis bildenden Tatsachen schützt. Insbesondere das Beispiel des Speicherns in der *Cloud* zeigt noch einmal einleuchtend, dass das sachenrechtliche Eigentum am Datenträgermedium nicht zwingend mit der Zuordnung der darauf gespeicherten Daten einhergehen kann. Die verschiedenen Anknüpfungspunkte von verschiedenen Personen stehen in einem bisher nicht auflösbaren Widerspruch¹⁸⁷.

184 Heun/Assion, CR 2015, 812 (818).

185 Bräutigam/Klindt, Digitalisierte Wirtschaft/Industrie 4.0, S. 23; Dorner, CR 2014, 617 (626); Specht, CR 2016, 288 (289); Zech, CR 2015, 137 (144).

186 Heymann, CR 2016, 650 (657).

187 Zu den divergierenden Zuordnungen nach dem BDSG, dem StGB sowie dem UWG, angewendet auf die Fallbeispiele, siehe Anhang Teil II.

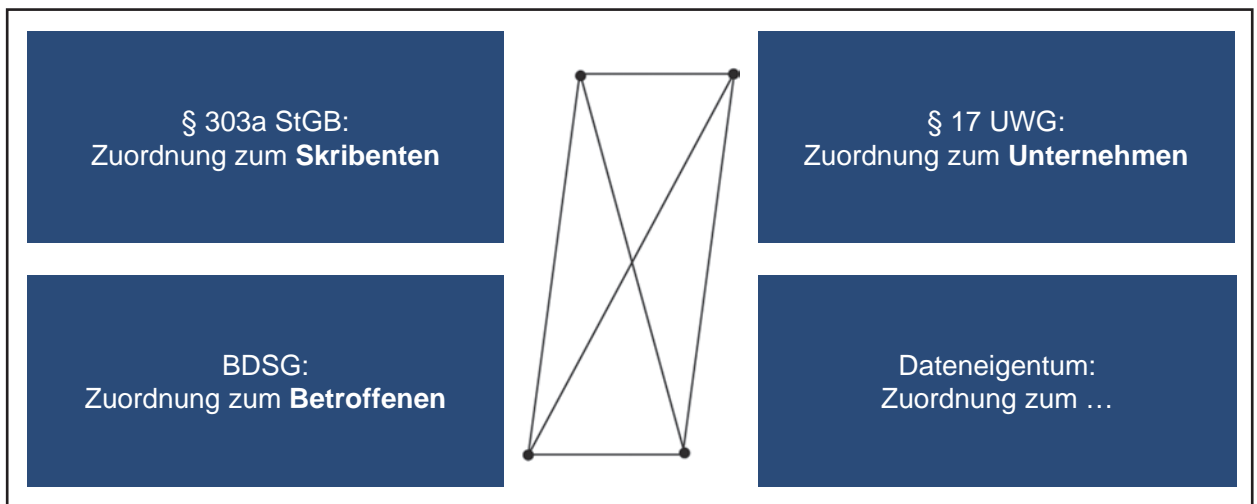


Abbildung 16: Kollision bereichsspezifischer Regelungen zur Frage „Dateneigentum“

3.3 Faktische Herrschaft als Äquivalent zum rechtlichen Eigentum

An Stelle der rechtlichen Zuordnung entscheiden derzeit oftmals die tatsächlichen Verhältnisse darüber, welche Akteure in den Fallstudien die Mobilitätsdaten verwenden können. Diejenigen, die die Dateninfrastruktur kontrollieren, haben die nötigen Zugriffsmöglichkeiten und können die Daten nutzen oder im Rahmen vertraglicher Vereinbarungen über sie verfügen. Diese faktische Verfügungsgewalt schafft eine eigentumsähnliche Position. Sie betrifft jedenfalls die rechtlich nicht geschützten Daten, wozu meist anonymisierte maschinen-generierte Rohdaten gehören¹⁸⁸. Wie im Folgenden gezeigt wird, erschwert die faktische Verfügungsgewalt jedoch auch bei rechtlich geschützten Daten dem Berechtigten, diese zu verwerten:

Der durchschnittliche Nutzer eines Fahrzeuges kann z. B. rein faktisch aufgrund des technischen Designs des Fahrzeuges auf viele „seiner“ personenbezogenen Daten aus den Mobilitätssystemen nicht zugreifen. Um diese Daten selber verwerten zu können, ist der Fahrzeugnutzer vielmehr darauf angewiesen, dass Automobilhersteller, Zulieferer oder Informationsanbieter die technischen Möglichkeiten schaffen, wie etwa entsprechende Schnittstellen. Dies gilt auch im Verhältnis zwischen Hersteller und Zulieferer. Hier könnten die Hersteller rein theoretisch versuchen – zum

Teil auch aus verständlichen Gründen, insbesondere um ihrer Gesamtverantwortung für die Sicherheit über das gesamte Fahrzeug gerecht zu werden – die Kontrolle über die Daten bei sich zu konzentrieren und damit die Zulieferer *de facto* vom Zugriff und der Nutzung auszuschließen. Dies hätte dann zur Folge, dass der Fahrzeugeigentümer bspw. im Wege der Produkthaftung nicht gegen den Hersteller vorgehen kann, da er seinen Anspruch ohne die benötigten Daten auf diesem Weg nicht beweisen kann. Damit entscheiden die Erstausrüster über den faktischen Zugriff durch Eigentümer, Mobilitätsdiensteanbieter, Plattformanbieter, etc. Die Wahrung der Sicherheitsinteressen der Hersteller und damit einhergehend auch die Produktbeobachtungspflicht über das „Komplettsystem Fahrzeug“ muss aber immer in einem angemessenen Verhältnis zu der Interessenlage anderer Beteiligter gesehen werden¹⁸⁹. Dies darf nicht dazu missbraucht werden, dass ökonomische Interessen der Hersteller, die freilich bestehen, über die Argumentationsschiene der Wahrung der Sicherheitsinteressen leichtfertig durchgesetzt werden. Die vollständige Ablehnung eines technisch abgesicherten Zuganges für Dritte erscheint zumindest aus dieser Sicht unverhältnismäßig. Die Automobilindustrie hat dies erkannt und folglich eigene Leitlinien und Prinzipien entwickelt, um sich selbst zu regulieren sowie die verschiedenen Daten zu kategorisieren und zuzuordnen. So verfolgt auch die Automobilindustrie die Ziele des Datenschutzes hinsichtlich des Schutzes der Einzelperson, der Transparenz über Erhebung und Nut-

¹⁸⁸ Siehe dazu Kapitel 3.2.

¹⁸⁹ Mielchen, SVR 2014, 81 (83). Siehe in diesem Zusammenhang auch Balzer/Nugel, Das Auslesen von Fahrzeugdaten zur Unfallrekonstruktion im Zivilprozess, NJW 2016, 193 ff. Siehe für den gesamten Abschnitt Hornung, DuD 2015, 359 (365) m. w. N.

zung von Daten im Fahrzeug sowie der Selbstbestimmung der Nutzer diesbezüglich¹⁹⁰.

Selbstverständlich ist die faktische Zugriffsmöglichkeit, und damit der Ausschluss anderer, auf die Daten nicht grenzenlos möglich, sondern findet ihre **Schranken** in der bestehenden Rechtsordnung. Hier ist zu allererst – zumindest soweit es sich um personenbezogene Daten handelt – an das Datenschutzrecht zu denken. Dieses sieht diverse Auskunfts-, Einsichts-, Nutzungs- und sonstige Rechte vor, die dem Betroffenen zustehen. Zusätzlich bestehen neben dem Datenschutzrecht noch weitere Regelungen, die die Datennutzung einschränken bzw. bestimmte Pflichten konstruieren, wie z. B. im Fall eines Verkehrsunfalls die allgemeinen Zeugen- und Herausgabepflichten.

Zu allererst ist im Rahmen des Datenschutzrechts – im Anwendungsbereich personenbezogener Daten – an den **Auskunftsanspruch** des Betroffenen nach § 34 Abs. 1 BDSG (künftig Art. 15 DSGVO) zu denken¹⁹¹. Hierunter sind im Verhältnis zwischen Hersteller und Halter sämtliche im Fahrzeug gespeicherten Daten zu subsumieren. § 34 Abs. 1 BDSG begründet jedoch weder einen Anspruch auf einen eigenen Zugriff auf die Daten, noch auf eine Bereitstellung, die eine direkte Weiterverarbeitung erlaubt¹⁹². Dies könnte vielmehr in einem Vertrag geregelt werden. Eine Nebenpflicht, die auch Gegenstand einer AGB-Kontrolle sein kann, könnte dann den Hersteller zur Herausgabe der Daten sowie zur Bereitstellung in einem geeigneten Format, das auch die Möglichkeit zur Weiterverarbeitung vorsieht, verpflichten, wenn nachvollziehbare Gründe bzw. ein berechtigtes Interesse bestehen, wie z. B. im Rahmen von Werkstattbesuchen¹⁹⁴.

Drittanbieter könnten hingegen einen Anspruch zur Herausgabe der Daten direkt gegenüber dem Hersteller aus dem Lauterkeits- und Kartellrecht haben oder müssten den „Umweg“ über den Betroffenen gehen¹⁹⁵. Zwar ist der Anwendungsbereich des Lauterkeits- und Kartellrechts für freie Werkstätten oder Mobilitätsdiensteanbieter relativ eng zu sehen, aber die Herstellung einer Exklusivität oder die willkürliche Vorenthaltung der Daten könnte eine gezielte Behinderung von Mitbewerbern nach § 4 Nr. 4 UWG sowie einen Verstoß gegen kartellrechtliche Missbrauchsverbote darstellen, wie z. B. die §§ 18 bis 20 GWB und Art. 102 AEUV. Exemplarisch sei nur auf den (neuen) § 3a UWG verwiesen, der vor rechtsmissbräulichem Marktverhalten schützt, so dass das Datenschutzrecht eine Marktverhaltensregel darstellen müsste¹⁹⁶.

Folglich ist festzustellen, dass es die Möglichkeit der faktischen Zugriffsmöglichkeiten gibt, die der jeweilige Fahrzeughersteller durch die Produktion des Fahrzeuges, vor allem durch die Programmierung der Schnittstellen, selbst bestimmen kann. Der Betroffene oder sonstige Berechtigte kann durch die Ausübung des ihm jeweils zustehenden Zugriffsrechts den Zugang öffnen. Falls ein verbindlicher Anspruch besteht, so „muss“ derjenige, der die faktische Zugriffsmöglichkeit besitzt – in der Regel ist dies der Hersteller – den Zugriff auf die Daten ermöglichen. Soweit ein solcher verbindlicher Anspruch nicht besteht, steht es dagegen im Ermessen des Herstellers, ob die Daten herausgegeben werden.

Dies führt zwar im Ergebnis nicht zu einer rechtlichen, aber zu einer **faktisch starken Position des Herstellers**, weil ohne sein Einverständnis und die durch ihn bestimmte technische Gestaltung der Schnittstellen niemand sonst auf die Daten zugreifen kann. Allerdings determiniert diese

190 Siehe zur Selbstregulierung in den Punkten Transparenz, Selbstbestimmung und Datensicherheit die vom VDA in Zusammenarbeit mit der Automobilindustrie entwickelten Prinzipien: „Datenschutz-Prinzipien für vernetzte Fahrzeuge“ vom 03.11.2014 unter <https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html>. Siehe des Weiteren die Position des VDA in Bezug auf den „Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten“ vom 19.09.2016 unter <https://www.vda.de/de/themen/innovation-und-technik/vernetzung/Zugang-zum-Fahrzeug-und-zu-im-Fahrzeug-generierten-Daten.html>.

191 Siehe auch die „Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)“ unter Nr. 5 zum Verständnis des Auskunftsrechts seitens der Automobilindustrie, <https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html>.

192 Siehe dazu auch das neue Recht auf Datenportabilität in Art. 20 DSGVO, das als Marktregulierungsvorschrift den Markt öffnen und zu einer Verringerung von „Lock-in“-Effekten führen soll, Kühling/Martini, EuZW 2016, 448 (450f.). Siehe auch Röttgen/v. Schönfeld/Jülicher, ZD 2016, 358 ff. Dies gilt auch, wenn Daten Dritter betroffen sind, Schantz, NJW 2016, 1841 (1845).

193 Siehe auch Roßnagel, Wem gehören die Daten im Fahrzeug? – Grundlegende Rechtsverhältnisse und Ansprüche, 52. Deutscher Verkehrsgerichtstag, Köln 2014, 257 (263f.).

194 Roßnagel, Wem gehören die Daten im Fahrzeug? – Grundlegende Rechtsverhältnisse und Ansprüche, 52. Deutscher Verkehrsgerichtstag, Köln 2014, 257 (272 ff.) mit Verweis auf die Euro-5/6-Verordnungen, die in Kapitel III der Verordnung (EG) 715/2007 vom 20.06.2007 den Zugang zu Reparatur- und Wartungsinformationen unabhängiger Marktteilnehmer regelt.

195 Hornung, DuD 2015, 359 (365).

196 Zur Streitdarstellung Podszun/de Toma, NJW 2016, 2987 (2989 ff.) sowie ausführlich zu der Frage, ob das Datenschutzrecht durch Verbraucherrecht, Lauterkeitsrecht und Kartellrecht durchgesetzt werden kann.

faktisch starke Position noch nicht die letztendlichen Nutzungsbefugnisse und die Zuordnung der damit verbundenen Gewinne. Trotz der *prima facie* starken Ausgangsposition kann es nämlich dazu kommen, dass in den sehr komplexen Marktstrukturen starke Nutzerpräferenzen für bestimmte Dienste oder Geräte (wie Smartphones mit ihren Betriebssystemen) sowie globale, marktmächtige Oligopole den Automobilherstellern letztlich die Bedingungen

für die Öffnung des Zugangs zu den Daten diktieren. Wie diese Entwicklung letztlich ausgeht, ist derzeit als offen zu beurteilen. Dass diese komplexe Entwicklung aber am Ende zu keiner angemessenen Verteilung der Wertschöpfung führt und die volkswirtschaftlichen Potentiale der Datennutzung nicht umfassend ausgenutzt werden, zeigt auch die folgende Betrachtung der ökonomischen Aspekte (siehe insbesondere Kapitel 4.3.3).

4 Ökonomische Analyse: Etablierung von Daten als Wirtschaftsgut als Voraussetzung für eine hohe wirtschaftliche Gesamtwertschöpfung

Der regulative Kontext für Daten und die Kultur im Umgang mit ihnen sind in Deutschland stark datenschutzrechtlich geprägt. Dies führt dazu, dass Daten erst sekundär als produktiver Rohstoff gesehen werden. Daten werden zwar *de facto* bereits wie ein wirtschaftliches Gut genutzt, diese Nutzung ist in der Regel aber nicht explizit: sie geschieht häufig im Tausch gegen einen scheinbar kostenfreien Dienst. In der Regel handelt es sich bei diesen Transaktionen betreffs der Datenweitergabe um „**Alles-oder-Nichts-Lösungen**“, bei denen nur **geringe Steuerungsmöglichkeiten** seitens des „Datengebenden“ bestehen. Diese Situation könnte geändert werden, wenn Daten grundsätzlich und explizit als **wirtschaftliches Gut anerkannt** wären und gehandhabt werden könnten. Die in diesem Kapitel vorgelegte Analyse hat daher zum Ziel, Anforderungen aus ökonomischer Sicht zu formulieren, um aus rechtlicher Sicht Lösungsoptionen für eine Regelung von Dateneigentum entwickeln und bewerten zu können. Dazu werden in den Dimensionen „Eigenschaften des Wirtschaftsguts Daten“, „Mechanismen für eine hohe Gesamtwertschöpfung“ und „Akteure mit Verfügungsgewalt“ konkrete Ansätze entwickelt.

Vor der Schaffung rechtlicher Schutzrechtserweiterungen ist zunächst nachzuweisen, dass dafür ein tatsächlicher **ökonomischer Bedarf** besteht¹⁹⁷. Die Rechtfertigung eines Ausschließlichkeitsrechts an Daten kann sich allein aus ökonomischen Gesichtspunkten ergeben. Die Normierung von Dateneigentum könnte bspw. einen Anreiz zu Investitionen in die Datenerfassung, einen gesamtwirtschaftlichen Mehrwert durch Offenbarungsanreize, die Schaffung von Märkten sowie eine ökonomisch sinnvolle Zuordnung des Datennutzens mit sich bringen¹⁹⁸. Wenn durch ein Verfügungsrecht an Daten aufgrund neuer Produkte und Dienstleistungen die Entwicklung innovativer Geschäftsmodelle möglich ist, kann dies ein massives Wachstum der Wirtschaft nach sich ziehen¹⁹⁹.

Die hier vorgestellte ökonomische Bewertung beginnt mit einem Überblick zum Hintergrund und zur Bedeutung der Digitalisierung im Mobilitätsbereich, wobei neben allgemeinen **Charakteristiken** der Entwicklung insbesondere **veränderte Kundenanforderungen** untersucht werden. Die Analyse verschiedener Möglichkeiten der Daten-

nutzung anhand einer **abstrakten Wertschöpfungskette** verdeutlicht die große Bedeutung des Themas für die Mobilitätsbranche. In einem zweiten Schritt werden die Auswirkungen auf die Automobilbranche vertieft und die individuellen und gesellschaftlichen sowie regulatorische **Implikationen** beleuchtet. Anschließend wird darauf eingegangen, wie Daten als **Wirtschaftsgut** zu klassifizieren sind und welche typischen Wertschöpfungsketten es im Bereich der automobilen Mobilität gibt. Es folgt schließlich die Beschreibung eines Lösungsansatzes aus ökonomischer Sicht nach Analyse der Rahmenbedingungen für die Erschließung des ökonomischen Potenzials; wesentliche Stichworte sind hier **Datensouveränität** und die Entwicklung eines **Marktes** für Mobilitätsdaten.

Nachdem im Rahmen von Kapitel 2 bestehende Möglichkeiten für datenbasierte Geschäftsmodelle anhand der fünf Fallstudien auf der Mikroebene konkretisiert wurden, stehen die Analyse von **Möglichkeiten der Datenkommerzialisierung** sowie die Identifikation von Wirtschaftsteilnehmern mit **berechtigtetem Interesse** an der Datennutzung auf der Makroebene im Blickwinkel dieses Kapitels. Insbesondere wurden auch Trends und Entwicklungen im bzw. aus dem Ausland untersucht („Apple CarPlay“, „Android Auto“, *Automatic.com*). Die Implikationen von *Open Data*, sowohl im Hinblick auf Transparenz für Bürger als auch für eine unternehmerische oder zivilgesellschaftliche Nachnutzung werden am Ende dieses Kapitels im Rahmen der Analyse von Daten als Wirtschaftsgut beurteilt.

4.1 Veränderte Kundenanforderungen als Treiber der Digitalisierung im Mobilitätsbereich

Die Digitalisierung bewirkt im Automobilsektor und im automobilen Mobilitätssektor seit einigen Jahren einen deutlichen Umbruch und hat erhebliche Auswirkungen auf Geschäftsmodelle und Wertschöpfung. So sind auch die relevanten Charakteristiken der Digitalisierung (Dematerialisierung, Netzwerkeffekte, Plattformen, mehrseitige Geschäftsmodelle und Einführung einer Datenschicht) verstärkt im Mobilitätsbereich festzustellen (Abbildung 17).

197 Dorner, CR 2014, 617 (626).

198 Zech, CR 2015, 137 (144 f.); Specht, CR 2016, 288 (294).

199 Reiners, ZD 2015, 51 (52).

Kategorie	Beschreibung	Beispiel Mobilität
Dematerialisierung	<ul style="list-style-type: none"> ▪ Prozessschritte werden nach Digitalisierung von neuen Marktspielern übernommen ▪ Etablierte Wertschöpfungsketten werden aufgesprengt 	<ul style="list-style-type: none"> ▪ Betreiber wie Uber und Lyft etablieren neue Geschäftsmodelle für persönliche Mobilität
Netzwerkeffekte	<ul style="list-style-type: none"> ▪ Die Utilität von Diensten wächst überproportional mit der Zahl der Nutzer/Anbieter ▪ Marktstruktur häufig durch Monopol oder Oligopol geprägt 	<ul style="list-style-type: none"> ▪ Perspektivisch: Apple CarPlay und Android Auto werden auf den Infotainment-Systemen der OEMs betrieben und bringen eigene Apps für Standardfunktionen mit
Plattformen	<ul style="list-style-type: none"> ▪ Die Interaktion von Nutzern geschieht nicht n:n, sondern 1:n über eine zentrale Plattform ▪ In der Regel werden Daten der Nutzer oder die von Nutzern eingestellt werden, monetarisiert 	<ul style="list-style-type: none"> ▪ Angebote wie Uber und Lyft, die Bewertungen von Fahrern durch Fahrgäste verwenden, um ihr Angebot zu verbessern
Mehrseitige Geschäftsmodelle	<ul style="list-style-type: none"> ▪ Geschäftsmodelle, bei denen ein Anbieter mit mehreren Kundengruppen interagiert, z. B. Suchmaschinen – die Gruppen sind Werbekunden und Kunden der Suchmaschine i.e.S. 	<ul style="list-style-type: none"> ▪ Tanktaler: Überwachung von Fahrzeug-Informationen; Nutzung der Standortdaten der Kunden zum Brokern von Geschäften mit Partnerunternehmen
Einführung einer Datenschicht	<ul style="list-style-type: none"> ▪ Die Digitalisierung hat zur Folge, dass viele bisher nicht-digital ablaufende Prozesse und nicht-digitalisierte Objekte eine zusätzliche Datenschicht erhalten 	<ul style="list-style-type: none"> ▪ Die Funktion der technischen Systeme in Fahrzeugen wird überwacht und der Zustand der Systeme bzw. der Einsatz bestimmter Fahrzeugfunktionen werden erfasst
Daten werden bereits heute im Austausch gegen eine Leistung als wirtschaftliches Gut gehandelt.		

Abbildung 17: Charakteristiken der Digitalisierung

Neben technischen Entwicklungen (siehe Kapitel 1.1 und 2) sind **veränderte Kundenpräferenzen** der zentrale Treiber der Digitalisierung im Automobil. Zwei Entwicklungen sind auf Basis einer Umfrage von McKinsey&Company gezeigt (Abbildung 18)²⁰⁰. Im Rahmen der im Juli und August 2015 durchgeführten Erhebung wurden insgesamt 3.184 Personen in Deutschland, den USA und China befragt;

gezeigt sind die Ergebnisse der Erhebung für den deutschen Markt (1.123 Befragte). Ziel der Umfrage war es, das Interesse von Kunden an und die Zahlungsbereitschaft für vernetzte, automatisierte und autonome Fahrfunktionen unter Berücksichtigung möglicher Bedenken bezüglich der Sicherheit ihrer Daten zu ermitteln.

200 McKinsey&Company, Wettlauf um den vernetzten Kunden, 2015.

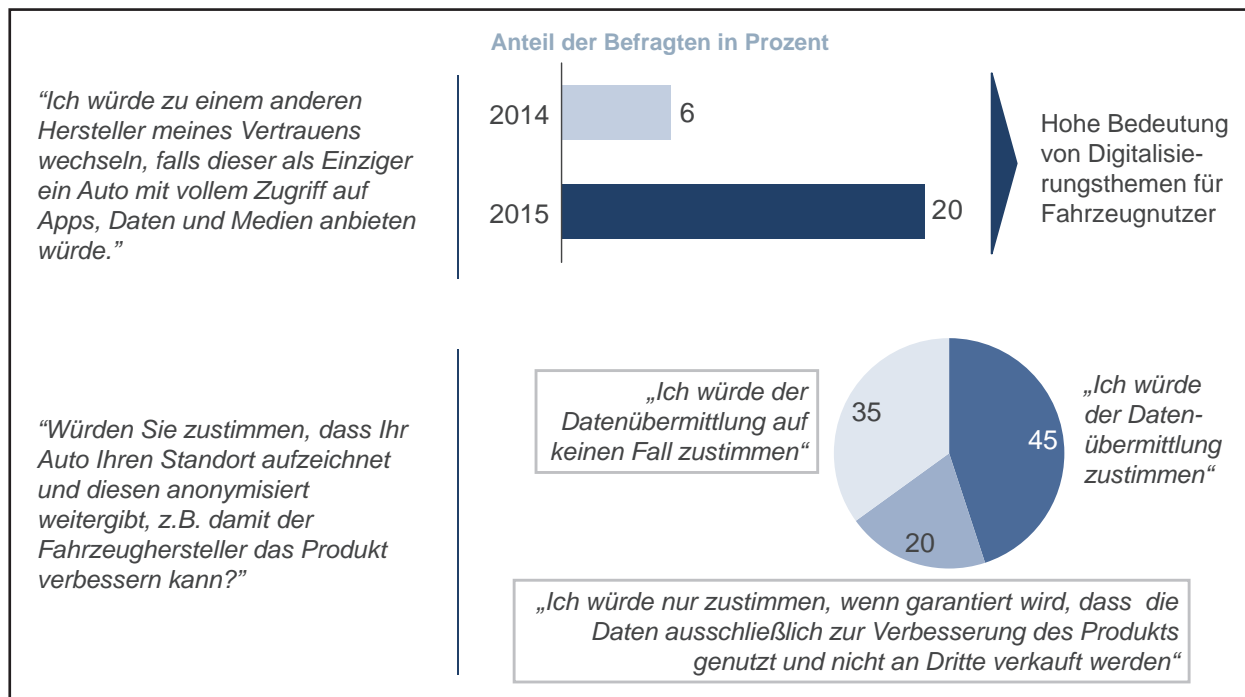


Abbildung 18: Anforderungen deutscher Kunden im Kontext der Digitalisierung²⁰¹

Wo gestern noch Benzinverbrauch, Motorleistung und technische Qualität standen, sind **vernetzte Dienste im Automobil** innerhalb von nur zwei Jahren vor allem bei der jungen, Smartphone nutzenden Generation zu einem **zentralen bis sogar ausschlaggebenden Kaufkriterium** geworden²⁰². So hat sich die Anzahl der deutschen Autofahrer, die bereit sind, aufgrund des Angebots vernetzter Dienste den Hersteller zu wechseln, in nur zwölf Monaten von 6 % (2014) auf 20 % (2015) mehr als verdreifacht. Und auch die Zahl der deutschen Kunden, die bereit sind, für solche Dienste zu zahlen, hat sich verdoppelt und ist – wenn auch verglichen mit den USA oder China insgesamt eher gering – durchaus sichtbar²⁰³. Bei der Bereitschaft, den Standort z. B. für eine Produktverbesserung anonymisiert weiterzugeben, zeigt sich aktuell ein gemischtes Bild: 45% der Befragten würden einer Übermittlung zustimmen, 20% würden einer Übermittlung unter bestimmten Bedingungen zustimmen und 35% würden die Übermittlung

ablehnen. In den USA und insbesondere in China sind die Vorbehalte diesbezüglich deutlich geringer²⁰⁴. Insgesamt zeichnet sich ab, dass fahrerunterstützende Anwendungen wie vernetzte Navigation und Parkassistenten deutlich stärker nachgefragt werden als integrierte Kommunikation oder Entertainmentdienste. Auch die Bereitschaft der Fahrzeugnutzer, für diese Funktionalitäten Daten bereitzustellen, ist im Vergleich deutlich höher, und steht insgesamt in engem Zusammenhang mit einem konkreten Nutzen/einer Produktverbesserung, die sich der Nutzer von der Bereitstellung seiner Daten verspricht²⁰⁵. Allgemein bedeutet Digitalisierung für den Kunden **„Convenience“**, also Komfort oder Annehmlichkeiten, und hat unbestritten einen hohen Nutzen für den Fahrzeugnutzer.

Insgesamt betrachtet können durch die Digitalisierung auch **neue Ansätze für Mobilität** entwickelt werden, welche in Anbetracht von Klimawandel, demografischen Ent-

201 McKinsey&Company, Wettlauf um den vernetzten Kunden, 2015.

202 Mobile International GmbH, Connected Car: PS schlägt Konnektivität, 2014, abrufbar unter: <http://newsroom.mobile.de/presseinformation/connected-car-ps-schlaegt-konnektivitaet-beim-autokauf>; Bearingpoint, Connected Car in Europe. Strategies and technologies for connected driving, 2015.

203 McKinsey&Company, Wettlauf um den vernetzten Kunden, 2015; In der Zeit von 2014 auf 2015 ist der Anteil der deutschen Kunden, der bereit ist, für die Vernetzung seines Fahrzeugs zu zahlen, von 4% auf 8% gestiegen. In den USA (Verdopplung von 13% auf 26%) und China (Anstieg von 24% auf 64%), ist im selben Zeitraum ein ähnlicher Trend zu erkennen, wenn auch in einer anderen Größenordnung.

204 McKinsey&Company, Wettlauf um den vernetzten Kunden, 2015.

205 Ernst & Young, Connected Car – Das Auto der Zukunft, 2012; Mobile International GmbH, Connected Car: PS schlägt Konnektivität, 2014, abrufbar unter: <http://newsroom.mobile.de/presseinformation/connected-car-ps-schlaegt-konnektivitaet-beim-autokauf>; McKinsey&Company, Wettlauf um den vernetzten Kunden, 2015; Bearingpoint, Connected Car in Europe. Strategies and technologies for connected driving, 2015.

wicklungen und der Verdichtung von Städten dringend erforderlich erscheinen: z. B. *Carsharing*-Modelle, Mobilitätslösungen basierend auf Modellen der sogenannten *sharing economy* oder der Trend zum automatisierten Fahren. In Konsequenz treten neben den etablierten auch neue, z. B. wesentlich datengetriebene und in der Regel in den USA entstandene Marktspieler mit völlig anderen Kernkompetenzen auf den Plan, seien es der US-Automobilhersteller *Tesla*, „Sharing-Dienste“ wie *Uber* und *Lyft* oder sektorfremde Unternehmen wie *Apple* und *Google*.

Allgemein gilt, dass Digitalisierung und die mit ihr aufkommenden digitalen Geschäftsmodelle neuer Akteure bereits zu einem **tiefgreifenden Wandel** in vielen traditionellen

Wirtschaftszweigen geführt haben (Beispiele: Endkundenhandel, Musikindustrie, Zeitungsverlage). Zu erwarten ist dies auch in der Mobilitätsbranche. So ist das Thema inzwischen in den **Blickwinkel traditioneller Hersteller gerückt**, welche die **Digitalisierung zum strategischen Ziel und Schlüssel zur Aufrechterhaltung ihrer Verbindung zum Kunden** erklärt haben²⁰⁶. Übergreifend ist erkennbar, dass datengetriebene Geschäftsmodelle eine besondere Rolle unter den digitalen Geschäftsmodellen einnehmen. Verdeutlicht wird dies durch die ökonomische Analyse der fünf Fallstudien (siehe Kapitel 2). In Abbildung 19 wird eine abstrahierte Version der beschriebenen **Wertschöpfungsketten bzw. -netzwerke** gezeigt.²⁰⁷

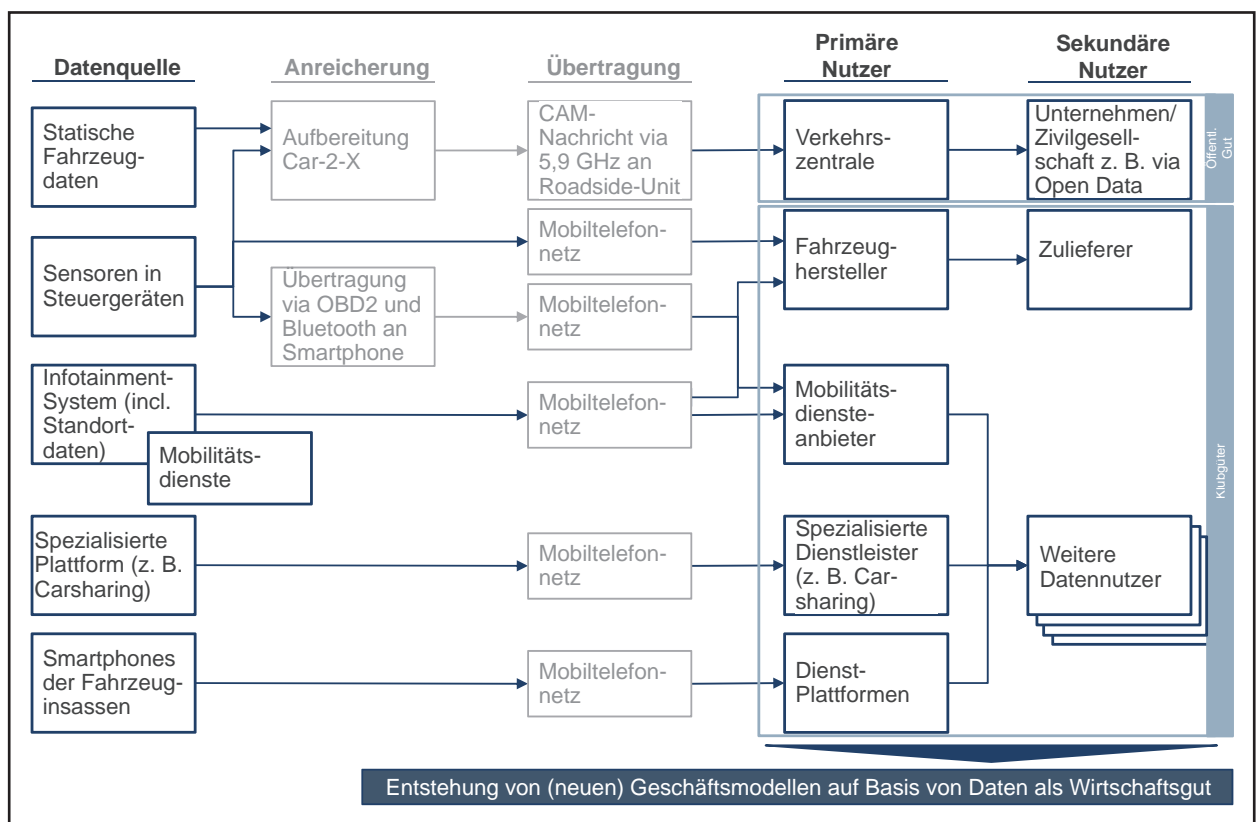


Abbildung 19: Abstrakte Wertschöpfungskette der Datennutzung und -verwertung

206 Der anfängliche Fokus lag vor allem auf Konnektivität im Auto, so dass inzwischen alle großen deutschen Automobilhersteller **eigene Infotainmentsysteme** anbieten. Was sich bei *Volkswagen* „car-net“ nennt, heißt bei *Daimler* „Command-Online“, bei *BMW* „Connected Drive“, bei *Audi* „Audi Connect“, bei *Opel* „Onstar“ und bei *Porsche* „Porsche Communication Management (PCM)“. Was alle diese Anwendungen gemein haben ist, dass sie den Fahrzeugnutzer mit Fahrzeug, Infrastruktur und Internet verbinden. In einer zweiten Generation konzentriert sich die Branche vorwiegend auf **Car-2-X-Konnektivität**. So hat *BMW* im Juli 2016 beispielsweise ein Projekt zum autonomen Fahren mit *Intel* und *MobilEye* bekanntgegeben. Auch *Audi* erforscht die Themen *Car-2-Car*- und *Car-2-Infrastructure*-Kommunikation, so z. B. in dem Projekt „Travolution“, gemeinsam mit der TU München und dem Unternehmen *GEVAS software*. Siehe: Bearingpoint, *Connected Car in Europe. Strategies and technologies for connected driving*, 2015; Kalenda, *BMW, Intel und Mobileye stellen Connected-Car-Pläne vor*, 2016 (www.zdnet.de/88273557/autonomes-fahren-bmw-kooperiert-angeblich-mit-intel-und-mobileye); *Travolution Website* (www.travolution-ingolstadt.de), 2016.

207 Lesebeispiel: Im Fall von *Car-2-Infrastructure*-Kommunikation werden Sensordaten von Steuergeräten mit zusätzlichen, das Fahrzeug selbst beschreibenden, Daten angereichert (Schritt „Aufbereitung Car-2-X“) und an die Roadside-Unit übertragen. Diese Daten können in der Verkehrszentrale ausgewertet und in Form von *Open Data* veröffentlicht werden.

Generell gilt, dass es primäre und sekundäre Nutzer gibt. In der Regel gibt es zumindest bei der **primären Nutzung einen starken direkten situativen Mobilitätsbezug** (z. B. Verarbeitung von Fahrzeuginformationen, Navigationsdaten oder Daten im Kontext einer Fahrzeugvermietung). Bei **sekundären Nutzungen steht der Mobilitätsbezug häufig im Hintergrund** (z. B. bei Zulieferern die Nutzung von Daten zur Qualitätsoptimierung in der Fertigung und bei weiteren Datennutzern das Angebot von standortbezogenen Kaufangeboten).

Jeder Schritt in der Wertschöpfungskette bedeutet potenziell weiteren Nutzen. Die Beteiligung von weiteren Akteuren und damit die Ausschöpfung einer längeren Wertschöpfungskette bedeutet damit auch eine **größere gesamtgesellschaftliche Wertschöpfung**. Dies geht, da es sich in der Regel um andere Marktspieler handelt, auch mit der **Schaffung von neuen Märkten** einher.

Im vorhergehenden Kapitel 3 wurde im Detail untersucht, wie Daten im geltenden Recht zuzuordnen sind. Die Vielzahl von Rechtsgebieten, die betroffen sind, und die damit einhergehende Komplexität hat die Nutzung von Daten in der Praxis allerdings kaum gebremst. Es ist denkbar, dass die komplexe Rechtslage sogar das aktuell übliche Phänomen der pauschalen Datenbereitstellung im Gegenzug für die Bereitstellung monetär kostenloser Dienste befördert hat, weil geeignete Differenzierungen und für Daten spezifische Zuschreibungen im geltenden Recht nicht möglich sind. Die im folgenden Abschnitt beschriebenen Implikationen für die verschiedenen Akteure (Automobilhersteller, Fahrzeugnutzer und Staat) zeigen im Detail auf, dass **Handlungsbedarf** besteht.

4.2 Implikationen für Fahrzeugnutzer, Automobilindustrie und den Staat

Ein Trend, der sich aus den Fallstudien abzeichnet (siehe insbesondere Fallstudien 3 und 4), ist der **Eintritt neuer Marktteilnehmer**, deren Kerngeschäft außerhalb der Automobilindustrie angesiedelt ist. Häufig haben diese Konkurrenten **plattformgetriebene Geschäftsmodelle**, die es ihnen erlauben könnten, erhebliche Anteile des Gewinns abzuschöpfen. Diese Tendenz ist symptomatisch für die Digitalisierung und betrifft neben der Automobilbranche auch zahlreiche andere Industriezweige. Das bekannteste Beispiel ist sicherlich *Google*, dessen wirtschaftlicher Erfolg auf dem mehrseitigen Geschäftsmodell der Schaltung kontextsensitiver Werbung beruht, gesteuert von der Analyse

des Internetnutzer-Verhaltens. Ein weiteres Beispiel sind sogenannte Sharing-Plattformen wie jene der amerikanischen Unternehmen *Uber* und *Airbnb*. Sie erwirtschaften durch die Monetarisierung privater Dienstleistungen einen erheblichen Umsatz und üben so Druck auf etablierte Marktspieler aus.

Zwei wichtige Facetten dieser Geschäftsmodelle sind zum einen die tiefgreifenden Veränderungen für etablierte Unternehmen und ihre Wertschöpfungsstrukturen und zum anderen der Zusammenhang mit rechtlichen und gesellschaftlichen Themen wie **informationeller Selbstbestimmung** und **Privatheit**. Somit hat die Digitalisierung im Mobilitätsbereich Implikationen für Automobilindustrie, Individuen und Gesellschaft sowie für den Staat in seiner Rolle als Regulierer. Grundsätzlich von dem hier behandelten Thema der Mobilitätsdaten abzugrenzen, aber nicht minder wichtig für die Automobilindustrie, ist das Thema Industrie 4.0. Darunter wird die Digitalisierung der Fertigung und damit der Wertschöpfungs- und Lieferketten verstanden. Endkunden sind hier in der Regel nicht betroffen. Dennoch ist zu erwarten, dass auch hier die oben genannten Digitalisierungstrends greifen werden, beispielsweise Dematerialisierung, Einführung einer Datenschicht und die Etablierung von (B2B-)Plattformen. Auch hier wird die Frage der Regulierung ein wesentliches Thema sein.

Für zwei der in den folgenden Abschnitten behandelten Themenkomplexe („Konfliktfeld Convenience vs. Privatheit“ und „Regulierung im ökonomischen Kontext“) ist offensichtlich, dass eine **Weiterentwicklung der rechtlichen Grundlagen der Datennutzung unverzichtbar** ist, z. B. in der Form einer Ausgestaltung eines Dateneigentums und mit ihm verbundenen Zuordnungsansätzen.

4.2.1 Konfliktfeld Convenience vs. Privatheit

Mit der Entstehung von datengetriebenen Märkten und Geschäftsmodellen im Rahmen der Digitalisierung ist es zu einem **enormen Anstieg personenbezogener und -beziehbarer Daten** gekommen. Die durch die massenhafte Analyse dieser Daten ermöglichten Vorteile im Bereich „Convenience“ sind jedoch nur eine Seite der Medaille. Zusätzlich zu Diskussionen über Überwachung durch Vorratsdatenspeicherung, den *Snowden*-Enthüllungen oder diversen Hacker-Angriffen auf Datenbanken mit persönlichen Informationen häufen sich die Berichte, in denen die Phänomene Digitalisierung und *Big Data* eher negativ konnotiert sind. Die **möglichen negativen Auswirkungen der Digitalisierung** im Mobilitätsbereich für Datenschutz und Privatheit des Fahrzeugnutzers werden im Folgenden detailliert, um später eine chancenorientierte Lösungsvariante erläutern zu können.

Die meisten datenbasierten Geschäftsmodelle basieren auf der Erstellung von Persönlichkeits- und Verhaltensprofilen ihrer Nutzer zum Zweck der Produktoptimierung oder des Weiterverkaufs für individualisierte Werbemaßnahmen. Die Nutzer der diversen Dienste wissen meist nicht, welche Daten zu welchem Zweck über sie erhoben werden und welche positiven oder negativen Folgen dies haben kann. Dieses neue Ausmaß von Datenerhebung, -analyse und -nutzung zeichnet sich seit circa einer Dekade ab und führt seither zu **Herausforderungen für den Schutz der Privatsphäre und für den Datenschutz**.

In einer Situation, in der der wirtschaftliche Wert von Daten bei den Endkunden kaum explizite Beachtung findet, versuchen Plattform-Unternehmen diesen Wert durch die Einholung **weitreichender Nutzungsrechte** für die Daten ihrer Kunden mittels Einwilligung in ihre AGB zu erschließen. Die Einwilligung des Nutzers erfolgt hier meist aus einem Mangel an Verständnis der in der Regel komplex formulierten AGB und aus einem Gefühl der **Alternativlosigkeit**. Dies ist zurückzuführen auf die häufig monopolistische Marktstruktur und darauf, dass die Kunden, ganz im Einklang mit den Geschäftsmodellen der Unternehmen, **keine abgestuften Handlungsmöglichkeiten** haben, sondern vielfach vor die Wahl zwischen vollständiger Freigabe der Daten oder Nichtnutzung des Dienstes gestellt werden. Diese Handhabung der Informationspflichten in der Praxis trägt nicht zu einer transparenten Aufklärung bei und kann somit nicht als Basis einer willentlich eingegangenen Transaktion bzw. eines validen Austauschverhältnisses einer Serviceleistung gegen die Bereitstellung von Daten gelten.

Der **Mangel an Information** und die Alternativlosigkeit führen zu einem scheinbar ambivalenten Verhalten der Nutzer im Konflikt zwischen Convenience und Privatheit. Umfragen ergeben, dass bei vielen der Umfang der Datennutzung zu Bedenken, Ängsten und Vorbehalten führt, sie aber dann dennoch für die Nutzung der Dienste optieren. Diese Situation wird auch als **'privacy paradox'** bezeichnet: Die häufige Nutzung datenbasierter Dienste koexistiert mit Sorgen um einen Verlust von Privatheit.

Nach Aussage des ADAC ist diese **Informationsasymmetrie** hinsichtlich der Datenerhebung und -nutzung auch kennzeichnend für den Mobilitätssektor. Gemäß einer Studie aus dem Jahr 2015 werden über das Diagnosesys-

tem (OBD-System) eines Fahrzeugs große Datenmengen, die Rückschlüsse auf dessen technischen Zustand oder das Nutzungsprofil des Fahrers erlauben, an den Hersteller übermittelt, **„ohne dass der Verbraucher davon weiß“**²⁰⁸. So werden Fahrziele oder Telefonkontakte erfasst, ohne vorher die Zustimmung der Fahrer einzuholen. Der Umfang und die fehlende Transparenz bezüglich der Datenerhebung, -weiterleitung und -nutzung aus dem Fahrzeug wurden von Verbraucherschutzorganisationen und dem ADAC stark kritisiert²⁰⁹. Hierbei handelt es sich um ein Beispiel dafür, dass derzeit vor allem die **faktische Zugriffsmöglichkeit** über die Erhebung und den Umgang mit Daten entscheidet (siehe Kapitel 3.3).

Auch aus ökonomischer Sicht sind diese Ängste vor Gefährdung der Privatheit durchaus bedenklich, da eine **geringere Akzeptanz datengetriebener Geschäftsmodelle** zu befürchten ist. Im Mobilitätssektor sind gerade in Deutschland die Vorbehalte groß. So sind, wie oben bereits erwähnt, ungeachtet der steigenden Wichtigkeit vernetzter Dienste im Auto über die Hälfte der deutschen Kunden nicht oder nur eingeschränkt bereit, ihre Standortdaten zur weiteren Verwendung an den Fahrzeughersteller zu übermitteln²¹⁰.

4.2.2 Traditionelle Automobilindustrie im Wandel

Das Auftauchen von neuen Marktspielern wie *Tesla*, *Google*, *Apple* oder *Uber* im automobilen Mobilitätssektor hat zu einem **Wandel der Wettbewerbslandschaft** und einer Herausforderung etablierter Automobilhersteller geführt. Die entstehende digitale Konkurrenz ist zwar heterogen aber trotz ihres geringen Alters im Markt bereits sehr präsent²¹¹. So hat der Fahrdienstvermittlungsdienst Uber in weniger als sechs Jahren seit Firmengründung das Taxigeschäft in einigen Metropolen weltweit auf den Kopf gestellt. Auch die Produkte „Android Auto“ (*Google*) und „CarPlay“ (*Apple*) sind nur wenige Jahre nach Markteinführung mit den *Infotainmentsystemen* führender Automobilhersteller kompatibel.

Damit einhergehend ist zu erwarten, dass zumindest für die Geschäftsmodelle eines Teils dieser Marktspieler die oben genannten ökonomischen Effekte greifen werden. Dazu gehört, neben der **Abschöpfung der Rendite** besonders profitabler Wertschöpfungsschritte, auch die Entstehung **monopolistischer bzw. oligopolistischer Marktstrukturen**.

208 ADAC, Datenkrake Pkw, 2016, abrufbar unter: https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/datenkrake_auto.aspx.

209 ADAC, Datenkrake Pkw, 2016, abrufbar unter: https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/datenkrake_auto.aspx.

210 McKinsey&Company, Wettlauf um den vernetzten Kunden, 2015.

211 Gründung von Uber im Jahr 2009, Gründung von Lyft im Jahr 2012, Gründung von Tesla im Jahr 2003 mit Verkaufsstart einer Kleinserie im Jahr 2007, Markteinführung von Apple „Car Play“ im Jahr 2014, Markteinführung von „Android Auto“ im Jahr 2015.

Erläutert werden kann dies am Beispiel von **Infotainment-Plattformen**, die eine große Nähe zu datengetriebenen Geschäftsmodellen haben. Jeder der großen Automobilhersteller hat eine eigene Infotainmentplattform entwickelt, die Funktionen wie Navigation, Telefonie und Musikwiedergabe abbildet. Trotzdem erlauben fast alle großen Hersteller die Nutzung der Systeme von Apple („CarPlay“) und Google („Android Auto“), die nach Anschluss des Smartphones zumindest dieselben der genannten Funktionen zulassen, dies aber bei tendenziell höherem Nutzen, da beispielsweise die Kontaktliste und Musikauswahl auf dem Smartphone in der Regel aktuell sind²¹². Außerdem erlauben die genannten Systeme die Erweiterung durch zusätzliche Applikationen, von denen viele dem Fahrzeugnutzer bereits durch Nutzung auf dem Smartphone oder Computer bekannt sind (z. B. die Einbindung von Services wie „Google Earth“ oder „Google Street View“). Vorteile für den Nutzer ergeben sich nicht nur aus dem **breiteren Applikationsangebot**, sondern vor allem auch aus dem **Markenwert** und Bekanntheitsgrad. Den genannten Digitalunternehmen ist es damit gelungen, sich direkt und für die Fahrzeugnutzer sehr sichtbar in die Systemlandschaft des Fahrzeugs einzuklinken. Die einheitliche Benutzeroberfläche des herstellereigenen Infotainmentsystems wird durch die der Apple- bzw. Google-Systeme verdrängt und sowohl die Connectivity-Dienste als auch beispielsweise das Navigationssystem des Herstellers werden redundant. Die Implikationen im Hinblick auf die wirtschaftliche Verwertung der erstellten Daten sind offensichtlich.

Smartphone im Automobil: Ein Blick in die USA

Amerikanische Technologiekonzerne haben – alleine oder in Kooperation mit führenden Automobilherstellern – die führenden Verbindungstechnologien für den Anschluss des Smartphones an das Auto entwickelt. Zu nennen sind die Marktführer „Android Auto“, „CarPlay“ und „Mirrorlink“. Alle drei Produkte erlauben die Verbindung des Smartphones mit der Head Unit des Infotainmentsystems via Kabel und haben Zugriff auf ausgewählte Sensordaten, die die Funktionsweise der Applikationen unterstützen. Welche der Daten die Au-

tomobilhersteller weitergeben, variiert und kann neben Geschwindigkeit, Position und Tankfüllstand bspw. auch die Belegung des Beifahrersitzes einschließen.

Deutsche Hersteller haben erkannt, dass sich die **Wertschöpfung** im Automobilsektor von der Hardware in Richtung **Software** und (insbesondere auch **datenbezogener Dienstleistungen**) verschiebt und dass die Digitalisierung im Mobilitätssektor ein radikales Umdenken erfordert. Es gibt verschiedene Ansätze, wie auf den Druck durch neue Marktspieler reagiert wird. Herstellerübergreifend zeichnet sich ab, dass die deutsche Automobilindustrie das Thema Digitalisierung durch strategische Partnerschaften mit Softwareunternehmen, **Investitionen** in Tech-Startups (z. B. *Porsche* in *EvoPark*) und **Rekrutierung** von IT-Experten aus dem Silicon Valley forciert²¹³. Ob nun ein Smartphone auf Rädern oder ein Auto mit Computer – die Unklarheit bezüglich der künftigen Rolle traditioneller Kernthemen wird auch in Zukunft nicht abnehmen. Der Markt für „connected driving“ wird hart umkämpft sein.

4.2.3 Regulierung im ökonomischen Kontext

Aus den skizzierten Implikationen für Wirtschaft und Gesellschaft ergibt sich – unter Umständen regulatorischer – Handlungsbedarf sowohl um die Wettbewerbsfähigkeit der heimischen Automobilindustrie zu erhalten und auch Startups in diesem Bereich zu fördern als auch um Chancen und Bedenken der Verbraucher im Spannungsfeld von Datennutzung und Datenschutz bzw. Privatheit zu adressieren. Obwohl datenschutzrechtliche Regulierung kein neues Thema ist, hat die Entstehung einer „data-driven economy“ im Rahmen der Digitalisierung und dem damit verbundenen Wachstum anfallender personenbezogener Daten die Frage nach einer adäquaten Regulierung auf eine neue Ebene gehoben.

Nicht zuletzt wegen des hohen Innovationstempos zeigt die Digitalisierung die **Grenzen staatlicher Regulierung** auf. So entstehen das Internet betreffende Gesetze und Regulierungsvorhaben aufgrund unverzichtbarer, legislativer Prozesse oft verzögert und hinken so technischen Entwick-

²¹² „Carplay“ und „Android Auto“ werden inzwischen in fast allen Neuwagen meist als zubuchbare Option für Infotainmentsysteme angeboten.

²¹³ Leiter der *Porsche Digital GmbH* wird Thilo Koslowski, welcher erst kürzlich vom amerikanischen IT-Beratungsunternehmen Gartner aus dem Silicon Valley zu Porsche gewechselt hat. Auch andere Hersteller holen sich Unterstützung aus dem Silicon Valley. So hat VW Johann Jungwirth, welcher ehemals bei Apple am iCar mitgearbeitet hat, zum Leiter für Digitales gemacht, und BMW Jens Monsees, ehemaliger Automotive Director bei Google, zum neuen Vice President für Digital Strategy ernannt (*Porsche*, Porsche gründet Kompetenz-Zentrum für Digitalisierung, 2016, abrufbar unter: <https://newsroom.porsche.com/de/unternehmen/porsche-kompetenz-zentrum-digital-gmbh-12569.html>; *Doll*, Dieser VW-Mann soll die schöne, neue Welt bauen, 2016, abrufbar unter: <https://www.welt.de/wirtschaft/article152788253/Dieser-VW-Mann-soll-die-schoene-neue-Welt-bauen.html>; *Eisert & Dämon*, Wie Harald Krüger BMW digitalisieren will, 2016, abrufbar unter: <http://www.wiwo.de/unternehmen/auto/bmw-wie-harald-krueger-bmw-digitalisieren-will/13045742.html>).

lungen und den damit verbundenen Geschäftsmodellen hinterher. Umso bemerkenswerter ist der Umstand, dass der Europäische Gerichtshof die Materie des Datenschutzrechts kurz nach Inkrafttreten der Europäischen Grundrechte-Charta 2009 zum Anlass nahm, seine nunmehr auch als Grundrechtsgerichtshof definierte Rolle auszufüllen und eine autonome und spezifische Grundrechtsdogmatik zu entwickeln²¹⁴.

In einer Situation, in der Datenschutzbestimmungen zu einem wichtigen Wettbewerbsfaktor werden könnten, führt eine **fragmentierte und lückenhafte Regulierungslandschaft** zu Standortunterschieden. Daraus resultieren eine große Disparität zwischen den Datenschutzbestimmungen verschiedener Länder und folglich **rechtliche Spielräume**, welche Unternehmen zu ihren Gunsten auslegen können, um minimalen Einschränkungen durch Datenschutzbestimmungen unterworfen zu sein. Die europäische Datenschutz-Grundverordnung wird zwar ab dem Jahr 2018 eine einheitliche Rechtsgrundlage schaffen²¹⁵. Mindestens genauso wichtig ist allerdings die **Durchsetzung des Rechtsrahmens**, die weiterhin in der Hand der nationalen Behörden liegt und EU-weit sehr unterschiedlich ausgeprägt ist²¹⁶.

Eine Anwendung **regulatorischer und fiskalischer Arbitrage** lässt sich beim Eintritt amerikanischer Internetkonzerne in den europäischen Markt beobachten. So ist es kein Zufall, dass bspw. *Google*, *Facebook*, *Apple* und *Airbnb* ihr Europageschäft von den europäischen Staaten aus steuern, in denen sie von niedrigeren Steuersätzen, insbesondere in Verbindung mit sehr spezifischen rechtlichen Konstruktionen, profitieren. Häufig entsteht so eine Situation, in der durch geeignete rechtliche Konstrukte große Vorteile seitens der Unternehmen realisiert werden können.

Die Themen Regulierung und Formen der Regulierung des Umgangs mit personenbezogenen Daten sind insgesamt eine Problematik, die von oft **konträren Interessen** und entsprechenden Handlungsempfehlungen geprägt sind. Das weitgehend am Schutz persönlicher Daten ausgerichtete und daher eher **restriktive Datenschutzrecht** zeigt der Entwicklung datenbasierter Geschäftsmodelle Grenzen auf, wird aber zunehmend als **Wirtschaftsbarriere** betrachtet. Die produktive und steuerbare Nutzung von Daten durch das Wirtschaftssubjekt spielt, wenn überhaupt, nur eine sehr eingeschränkte Rolle. In Anbetracht aktueller

Datenskandale mehren sich gleichzeitig die **Bedenken** der Bürger über den sicheren Umgang mit ihren Daten. Da auch der Erfolg datenbasierter Geschäftsmodelle auf dem **Vertrauen** der Nutzer und der damit einhergehenden Bereitschaft ihre Daten bereitzustellen zusammenhängt, stehen beide Aspekte in engem Zusammenhang.

Somit steht die Politik vor der zentralen Herausforderung, eine Balance zwischen **adäquatem Schutz von Privatheit** und **innovations- und investitionsfördernder Regulierung** zu schaffen. Auch die Form der Regulierung ist eine zentrale Frage. Naturgemäß erfolgt **staatliche Regulierung** in Form von Gesetzgebungsmaßnahmen oft erst spät und langsam – politische Prozesse und die damit verbundenen Aushandlungen sind zeitintensiv. Aus diesem Grund könnten Formen der Eigeninitiative und **Selbstregulierung** durch die Industrie ebenso in Betracht gezogen werden. Ein konkretes Beispiel sind Standards, z. B. die (Selbst-)Verpflichtung, Fahrzeugnutzer in einfacher und einheitlicher Form über die bei der Fahrzeugnutzung aufgezeichneten und übertragenen Daten zu informieren (siehe Handlungsempfehlung 7.2 (Standardisierung)). Schließlich wäre es möglich, dem betroffenen Individuum eine individuelle Entscheidungsmöglichkeit zur Datennutzung zuzuweisen. Eine Möglichkeit diesbezüglich wäre eine souveräne **Entscheidungsgewalt** des Einzelnen oder einer geeigneten juristischen Person als mündiges Wirtschaftssubjekt über die Erhebung und Verwendung von Daten. Eine solche Lösung würde die Frage nach dem **richtigen Maß an Regulierung** im Sinne eines individuell bestimmbaren Gleichgewichts zwischen Datennutzung und Privatheit beantworten.

4.3 Daten als Wirtschaftsgut: Datensouveränität und Markt als Erfolgsfaktoren

Das **Marktpotenzial von vernetzten Diensten** in und um das Automobil ist hoch. Eine im Rahmen der hier vorgelegten Studie durchgeführte sehr grobe Abschätzung hat ergeben, dass der Wert der Mobilitätsdaten eines privaten Fahrzeugnutzers in Deutschland (Positionsdaten sowie Fahrzeugdaten) in der Größenordnung von ca. 350 EUR/Jahr liegen könnte. Multipliziert mit der Anzahl der privaten Kfz in Deutschland zeigt dies, dass es sich um einen Markt von der Größe eines zweistelligen Milliarden-Euro-

214 EuGH, Rechtssache C-131/12, Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González.

215 Siehe dazu bereits ausführlich unter 3.2.1.

216 Siehe dazu *Europäische Kommission*, Factsheet Digitaler Binnenmarkt – Wirksamerer Schutz der Privatsphäre in der elektronischen Kommunikation, 10.01.2017, abrufbar unter: http://europa.eu/rapid/press-release_MEMO-17-17_de.htm.

Betrags handelt. In einer anderen Studie²¹⁷ wurde der Wert der Daten eines drei Jahre währenden *Leasing*vertrags mit ca. 1.500 bis 2.000 EUR angegeben, entsprechend ca. 500 bis 650 EUR p. a..

Diese Zahlen unterstreichen die Aussage, dass Daten eine **signifikante wirtschaftliche Bedeutung** besitzen. Gleichwohl ist es schwierig bis unmöglich, deren wirtschaftliches Potenzial seriös zu quantifizieren. So führen Berechnungen des monetären Werts von personenbezogenen Daten abhängig vom jeweiligen Kontext und Berechnungsansatz zu stark variierenden Ergebnissen²¹⁸. Nicht ohne Grund sind Quantifizierungen in der Literatur kaum verfügbar. Hinzu kommt, dass neben dem monetären Wert auch sozioökonomische Effekte, die sich aus der Datennutzung ergeben, bei der Berechnung des Wertes – im weiteren Sinne – berücksichtigt werden müssten. Schlussendlich hängt der Wert von Daten davon ab, welche Preise sich auf dem entsprechenden Markt bilden. Dieser **Preisbildungsmechanismus** ist u. a. der Grund dafür, dass in diesem Kapitel später vorgeschlagen wird, Marktstrukturen für Mobilitätsdaten zu etablieren. Darüber hinaus gilt: Daten haben keinen Wert an sich, sondern nur einen Wert im Kontext konkreter Nutzungen in Geschäftsmodellen, bei denen wiederum ein komplexes Wechselspiel aus Angebot und Nachfrage besteht.

Vor diesem Hintergrund wurde ein Ansatz gewählt, in dessen Fokus die Schaffung der notwendigen Voraussetzungen für eine möglichst hohe Gesamtwertschöpfung durch Datennutzung steht. Die Analyse und Einordnung von **Daten als Wirtschaftsgut** ist ein notwendiger Schritt zur Erarbeitung dieser Voraussetzungen in diesem Kapitel. Neben der Maximierung des volkswirtschaftlichen Nutzens spielt auch die Balance von wirtschaftlichen Interessen und Persönlichkeitsrechten bzw. Privatheit eine Rolle.

Es ist hilfreich, in einem ersten Schritt das Wirtschaftsgut Daten in das klassische Schema nach **Rivalität und Ausschließbarkeit** einzusortieren. Für „klassische“ Güter ist diese Struktur in Abbildung 20 illustriert, die Einteilung erfolgt in die Klassen **öffentliches Gut**, **Allmendegut**, **Klubgut** und **privates Gut**. Ein Wirtschaftsgut ist rival, wenn es sich bei der Konsumption erschöpft und nicht rival, wenn es von mehreren Akteuren gleichzeitig konsumiert werden kann. Ein Wirtschaftsgut ist nicht ausschließbar, wenn der Konsum des Gutes nicht verhindert werden kann, und ausschließbar, wenn ein Akteur vom Gut ausgeschlossen werden kann.

²¹⁷ Schwartmann/Hentsch, PinG 2016, 117 ff.

²¹⁸ OECD, 2013, Exploring the economics of personal data: A survey of methodologies for measuring monetary value; In der genannten Studie wurde der monetäre Wert persönlicher Daten unter Heranziehung verschiedener Berechnungsansätze abgeschätzt: basierend unter anderem auf der Marktkapitalisierung, dem Unternehmenseinkommen pro Nutzerprofil, dem Marktpreis verschiedener Datensätze oder ökonomischen Experimenten. Die Ergebnisse zeigen in Abhängigkeit vom Markt und vom Berechnungsansatz ein weites Spektrum des möglichen monetären Wertes persönlicher Daten auf. So sind die Erträge, die Facebook im Jahr 2011 pro Nutzer machte, stark vom geografischen Markt abhängig (USA und Kanada: USD 9,51/Nutzer, Europa: USD 4,86/Nutzer, Asien: USD 1,79/Nutzer, Rest der Welt: USD 1,42/Nutzer). Der Wert von Daten kann auch dadurch bemessen werden, dass die Marktkapitalisierung eines Unternehmens in Bezug zur Anzahl seiner Nutzer gesetzt wird. Dieser Wert schwankte für Facebook zwischen USD 40 und USD 300 im Zeitraum von 2006 bis 2012. Auch das Geschäftsmodell der Unternehmen spielt eine Rolle: Die Geschäftsmodelle von Facebook und Experian sind beide datengetrieben; die Erträge bewegen sich im Bereich von USD 4 und USD 7 pro Datensatz und Jahr. Auch der Typ der Daten ist von hoher Bedeutung: In den USA wurde eine Anschrift für USD 0,50 gehandelt, ein Geburtsdatum für USD 2 und eine *social security number* für USD 8 (alle vorgenannten Daten aus der zitierten Studie). Schließlich ist auch die Berechnungsmethode von hoher Bedeutung; der Wert eines regulär gehandelten personenbezogenen Datensatzes wird verschieden sein von den Kosten, die pro Datensatz für Folgekosten entstehen, wenn in IT-Systeme eingebrochen wird, und dieser wiederum wird verschieden sein von dem Wert, den Versuchspersonen ihren Daten in Laborexperimenten zumessen. Alle diese Werte lassen sich als Wert der betreffenden Daten interpretieren.

		Rivalität		
		Nicht rival	Rival	
Aus-schließ-barkeit	Nicht aus-schließ-bar	Öffentliches Gut , z. B. <ul style="list-style-type: none"> Luft Küstenschutz Klimaschutz Landesverteidigung Nicht-überfüllte Straßen 	Allmendegut , z. B. <ul style="list-style-type: none"> Allmenden Fischbestände in öffentlichen Gewässern Überfüllte Straßen 	Nicht ausschließbare Güter sind in der Regel natürliche Güter oder staatlich bereitgestellte (und damit durch die Allgemeinheit finanzierte) Güter
	Aus-schließ-bar	Klubgut , z. B. <ul style="list-style-type: none"> Golfclubs Fitnessstudios eBook mit Campus-Lizenz Öffentlicher Nahverkehr 	Privates Gut , z. B. <ul style="list-style-type: none"> Zeitung Speiseeis Privates Kraftfahrzeug 	

Abbildung 20: Klassifikation wirtschaftlicher Güter nach Rivalität und Ausschließbarkeit

Zwei Beobachtungen seien hervorgehoben:

- Nicht ausschließbare Güter sind in der Regel natürliche Güter oder staatlich bereitgestellt (und damit durch die Allgemeinheit finanziert).
- Es gibt bei dieser Klassifikation Grauzonen: Eine Straße ist nur dann nicht rival, wenn sie nicht überfüllt ist.

Hal Varian hat 1998 **Informationsgüter** (die Daten einschließen) klassifiziert²¹⁹. Da in der allgemein verfügbaren Literatur die Klassifikation von Daten bisweilen nicht ausreichend argumentiert wird, seien an dieser Stelle zu den Kategorien Rivalität und Ausschließbarkeit einige der relevanten Textpassagen zitiert (Abbildung 21).

²¹⁹ Varian, Markets for information goods, 1998.

	Definition	Anmerkung
Rivalität	<ul style="list-style-type: none"> ▪ <i>“Nonrival means that one person’s consumption doesn’t diminish the amount available to other people [...].”</i> ▪ <i>“Nonrivalness is a property of the good itself [...].”</i> ▪ <i>“Information goods are inherently nonrival, due to the tiny cost of reproduction.”</i> 	<ul style="list-style-type: none"> ▪ Rivalität ist eine Eigenschaft eines Gutes an sich ▪ <u>Daten als Gut sind in der Regel nicht rival</u>
Ausschließbarkeit	<ul style="list-style-type: none"> ▪ <i>“[...] nonexcludable means that one person cannot exclude another person from consuming the good in question.”</i> ▪ <i>“Excludability [...] depends, at least in part, on the legal regime.”</i> ▪ <i>“Exclusion is not an inherent property of goods [...], but is rather a social choice.”</i> ▪ <i>“[...] whether [information goods] are excludable or not depends on the legal regime</i> 	<ul style="list-style-type: none"> ▪ <u>Regulierung ist Grundlage für Ausschließbarkeit</u> ▪ Ausschließbarkeit für Daten kann darauf aufbauend durch technische (z. B. Zugangsschutz/ Verschlüsselung) oder organisatorische Maßnahmen unterstützt werden

Abbildung 21: Eigenschaften wirtschaftlicher Güter: Rivalität und Ausschließbarkeit²²⁰

Rivalität ist eine Eigenschaft eines Gutes an sich. Da Daten sich bei der Konsumption nicht erschöpfen, sind sie grundsätzlich, bei Verfügbarkeit (dazu unten mehr) **nicht rival**; ein wesentlicher Grund dafür ist, dass die Reproduktionskosten für Daten sehr gering sind. Ausschließbarkeit ist eine rechtliche Kategorie (bei Varian: „social choice“), die

bspw. technisch oder organisatorisch durchgesetzt werden kann. Damit ist **Regulierung** (und die Durchsetzung derselben) die **Grundlage für Ausschließbarkeit**. In Abbildung 22 sind Daten als Wirtschaftsgut in das klassische Schema einsortiert.

		Rivalität		
		Nicht rival	Rival	
Ausschließbarkeit	Nicht ausschließbar	Daten als öffentliches Gut: Open Data – jeder kann darüber verfügen (Annahme: nur wenig einschränkende Nutzungslizenz)	<i>Daten sind nur in Ausnahmefällen rival, z. B. wenn besonderer Aufwand bei der Reproduktion auftritt (Bsp.: gleichzeitiger Zugriff auf große Datenmengen bei geringer Bandbreite in Kommunikationsnetzwerken)</i>	Daten sind aufgrund der geringen Kosten für Reproduktion in der Regel nicht rival.
	Ausschließbar	Daten als Klubgut: Akteur mit Verfügungsgewalt kann die Nutzung geeignet einschränken und die Daten damit einem begrenzten Nutzerkreis zur Verfügung stellen		Die Ausschließbarkeit hängt von den Gegebenheiten der Regulierung ab und ist damit steuerbar

Abbildung 22: Klassifikation von Daten als Wirtschaftsgut

²²⁰ Varian, Markets for information goods, 1998.

Wenn das rechtliche Umfeld für bestimmte Kategorien von Daten den Zugang für bestimmte Nutzer ausschließt, sind Daten ein Klubgut. In der Regel kann dann ein Akteur mit **Verfügungsgewalt** die Nutzung einschränken und einem begrenzten Nutzerkreis zur Verfügung stellen. Es gibt auch Daten, die als öffentliches Gut gelten können, und zwar insoweit, als keine Akteure von deren Nutzung ausgeschlossen sind. Ein Beispiel sind offene Daten mit einer nicht oder nur gering einschränkenden **Nutzungslizenz**. Wie oben bereits beschrieben, kann es Grauzonen geben. Im Fall von Daten kann es bspw. sein, dass der Zugriff aus technischen Gründen wie begrenzter Bandbreite eingeschränkt ist und nur jeweils ein Nutzer sinnvoll Zugriff hat, oder dass die Reproduktion aufgrund großer Volumina mit hohen Kosten verbunden ist. In diesem Fall sind Daten Allmendegüter oder private Güter. Streng genommen könnte man argumentieren, dass es sich um verschiedene Wirtschaftsgüter handelt: Daten, auf die ein Zugriff bereits vorliegt bzw. Daten, auf die noch zugegriffen werden muss. Diese Diskussion ist in der Regel allerdings akademisch. In der Praxis sind **Reproduktionskosten gering**.

Die vorangegangene Diskussion hat gezeigt, dass das regulatorische Umfeld im Zusammenhang mit technischen und organisatorischen Maßnahmen ein wesentlicher Faktor dafür ist, wie Daten als Wirtschaftsgut eingesetzt werden können.

Vor der Beschreibung eines Lösungsansatzes für eine möglichst hohe Gesamtwertschöpfung für Daten seien drei Beobachtungen genannt:

- Die weiter oben beschriebene abstrakte Wertschöpfungskette (Abbildung 19) zeigt, dass eine Vielzahl von Akteuren Mobilitätsdaten nutzen kann, mit unterschiedlichen Graden des Mobilitätsbezugs. Insbesondere können Daten, sofern sie weitergegeben werden können, in eine **Vielzahl von Nachnutzungen** einfließen.
- **Klassische Kunden von Produkten sind heute Produzenten von Daten:** dies gilt verstärkt auch für den Mobilitätsbereich. Sie haben aber in der Regel keine Transparenz über die Nutzung der erhobenen Daten (Asymmetrie) und wissen nicht, ob sie einen adäquaten Gegenwert erhalten. Dies führt dazu, dass (gerade in Deutschland) nur eine geringe Bereitschaft dafür besteht, Daten weiterzugeben (vgl. die oben genannte empirische Studie zur Weitergabe von Standortdaten). Höhere Transparenz, z. B. durch Angabe der gespeicherten bzw. übertragenen Daten (siehe dazu Handlungsempfehlung 7.2 („Datenausweis“)) sollte dazu führen, dass Kunden sachgerechtere Entscheidungen treffen und

auch den (ggf. monetären) Wert der Daten besser einschätzen können. Mangelnde Transparenz betrifft nicht nur die Erhebung, sondern auch die weitere Verarbeitung und Nutzung der Daten.

- **Die Weitergabe von Daten ist für die Akteure, die Daten erzeugen, mit (ggf. in der Zukunft liegenden) Kosten oder Risiken versehen:** Verbrauchern wird der Kauf geeigneter Produkte angeboten (z. B. auf Basis des Einsatzes von Standortdaten), sie haben Zeitaufwand für die Beschäftigung mit unter Umständen übermäßiger Werbung, die Transparenz über Produktnutzung kann die Herstellerhaftung unterbinden (z. B. bei fehlerhaftem Gebrauch eines Fahrzeugs, sofern dieser aus gespeicherten/übertragenen Daten ersichtlich ist), es besteht das Risiko, dass private Daten Akteuren zur Kenntnis kommen, die diese missbrauchen können (z. B. durch Veröffentlichung), es besteht das Risiko der unbefugten Verwendung privater Daten. Diese Kosten bzw. Risiken werden aktuell bei der Datenweitergabe nicht explizit bepreist.

Die im diesem Kapitel eingangs gestellte Frage „Welche Voraussetzungen müssen erfüllt sein, damit Daten als Wirtschaftsgut eine hohe Gesamtwertschöpfung ermöglichen?“ lässt sich in die drei folgenden Teilfragestellungen ausdifferenzieren:

1. **Welche Eigenschaften sollte das Wirtschaftsgut Daten besitzen?**
2. **Welche Mechanismen sind als Anreize für einen hohen Grad der Nachnutzung sinnvoll?**
3. **Welche Akteure sollten die Verfügungsgewalt über das Wirtschaftsgut Daten besitzen?**

Diese drei Fragen sollen nun unter Berücksichtigung der genannten drei Beobachtungen im Sinne von einzelnen Anforderungen weiter detailliert und durch die Angabe von **Strukturelementen** beantwortet werden. Die ersten beiden Teilfragen adressieren dabei insbesondere die **Anreize für Erzeugung und Bereitstellung bzw. weiterführende Nutzung**, während sich die dritte Frage auf die **Zuordnung eines Akteurs** für die initiale Nutzung von Daten bezieht. Die Strukturelemente beschreiben aus ökonomischer Sicht die Eigenschaften, die schließlich durch ein geeignetes regulatorisches Umfeld sichergestellt werden können.

Im Anschluss an die Angabe der Strukturelemente wird im weiteren Verlauf dieses Kapitels auf Trends und Entwicklungen bei datenbasierten Geschäftsmodellen eingegangen und das Thema *Open Data* vertieft.

4.3.1 Wünschenswerte Eigenschaften des Wirtschaftsguts Daten

Grundlegend für die folgenden Überlegungen ist, dass Daten als Wirtschaftsgut eingesetzt werden können. Dafür sind geeignete rechtliche Mechanismen notwendig, die es Akteuren erlauben, Daten analog zu anderen Wirtschaftsgütern zu nutzen, d. h. insbesondere auch handelbar zu machen. Aus ökonomischer Sicht geht es zunächst um **Datensouveränität**. Darunter soll hier verstanden werden, dass für bestimmte Akteure die Verfügungsgewalt über Daten besteht, die in der Regel auch die Möglichkeit zur Ausschließbarkeit beinhaltet²²¹.

Datensouveränität schafft eine Situation, in der der Verfügungsberechtigte eine explizite monetäre oder nicht-monetäre Kompensation für die Bereitstellung seiner Daten zur Nutzung erhalten kann. Daten werden damit als werthaltiges Wirtschaftsgut behandelt. Dies steht im Gegensatz zur aktuellen Praxis, bei der Daten vielfach undifferenziert zur Verfügung gestellt werden. Das klare Herausstellen einer Verfügungsgewalt ist mit zahlreichen Vorteilen verbunden:

- Es ist zu erwarten, dass auf diesem Wege eine größere **Bereitschaft zur Datenfreigabe** im Austausch gegen eine Dienstleistung oder monetäre Kompensation entstehen wird, wie sich dies auch in Laborversuchen abzeichnet²²².
- Im Gegensatz zur momentanen Situation, in der der Betroffene langen und komplexen AGB und Datenschutzerklärungen routinemäßig und in der Regel unüberlegt zustimmt, wird er zu einer **selbstbestimmten, informierten Entscheidung** befähigt. Im Umgang mit Plattform-Unternehmen haben Nutzer, wie bei den Charakteristiken der Digitalisierung aufgeführt, aufgrund der oftmals monopolistischen oder oligopolistischen Marktstruktur und der sehr weitreichenden Nutzungserlaubnisse über AGB häufig keine ausreichenden Wahlmöglichkeiten – die Datennachnutzung ist zur Zeit an einen einzigen Abnehmer gebunden. Datensouveränität wäre ein erster Schritt, um diese Einschränkung aufzuheben.

- Datensouveränität ermöglicht es dem Betroffenen, über einen ökonomischen Mechanismus gegensätzliche Interessen hinsichtlich **wirtschaftlichem Nutzen und dem Schutz der Privatheit ins Gleichgewicht zu bringen**. Dies wäre z. B. durch eine abgestufte, gesteuerte Datenfreigabe zur Nutzung für bestimmte Zwecke möglich, also eine explizite Autorisierung im Sinne eines abgestuften *Opt-in* für einzelne, klar definierte Datenkategorien²²³. Dies ermöglicht es ihm, in jeder Situation seine Präferenzen abzuwägen und dementsprechend selbstbestimmt zu entscheiden. Eine vertiefte Diskussion zu möglichen Abstufungen findet sich bei den Ausführungen zum dritten Strukturelement.
- Der Fahrzeugnutzer erhält Dienstleistungen und Produkte, die besser auf seine persönlichen Präferenzen und Bedürfnisse abgestimmt sind. Die souveräne/gezielte Freigabe von Daten optimiert die Kundenerfahrung.

Datensouveränität ist also insbesondere ein **Anreiz** für die betroffenen Akteure, damit Daten trotz der Datenschutz- und Privatheitsanforderungen erzeugt bzw. bereitgestellt werden. Dies kann bspw. auch dadurch unterstützt werden, dass es für die Akteure ausreichend transparent ist, welche Daten als Wirtschaftsgut genutzt und in welcher Form diese weiterverarbeitet werden (siehe Handlungsempfehlung 7.2 („Datenausweis“)). Dies verhindert oder reduziert Informationsasymmetrien. Transparenz in diesem Sinne befähigt die Akteure zu souveränem Handeln.

Zusammengefasst lautet das **erste Strukturelement**:

Datensouveränität: Wirtschaftliche Akteure (sowohl natürliche als auch juristische Personen), die am Beginn der Verwertungskette stehen, haben eine selbstbestimmte und aktive Verfügungsgewalt über die Nutzung der betroffenen Daten und können diese mit bestimmten Einschränkungen versehen.

221 Wie in der obigen Betrachtung vertieft worden ist, basiert Ausschließbarkeit auf technischen, organisatorischen, aber insbesondere auch rechtlichen Gegebenheiten.

222 Acquisti et al., What is privacy worth?, The Journal of Legal Studies 42(2), 2013, S. 249 - 274.

223 Bsp.: Bei Installation bzw. vor Nutzung von betroffenen Apps separate Zustimmung zur Nutzung von GPS-Daten, Fotos, Kontaktdaten etc. Jede Datenkategorie sollte mit einer handhabbaren Granularität separat abgefragt werden und zur Nutzung freigegeben werden, entweder vor jeder Anwendung oder im Sinne von „immer bei Nutzung dieser App freigeben“.

4.3.2 Mechanismen für einen hohen Grad der Nachnutzung

Das zweite Element für eine hohe Gesamtwertschöpfung ist die **Vereinfachung der Nachnutzbarkeit** von Daten. Aus ökonomischer Sicht kann dies dadurch erreicht werden, dass das Wirtschaftsgut Daten einfach handelbar gemacht wird und insbesondere entsprechende **Marktmechanismen** ermöglicht werden.

Akteure in einem solchen Markt für Mobilitätsdaten wären sowohl Unternehmen und Fahrzeugnutzer, aber auch die öffentliche Verwaltung und Vertreter der Zivilgesellschaft. Die Voraussetzungen für einen funktionierenden Markt im Sinne eines Ordnungsrahmens können durch regulatorische Eingriffe oder Selbstverpflichtungen der Marktteilnehmer geschaffen werden. Für den Handel von (Mobilitäts-)Daten haben Märkte Vorteile:

- Märkte bringen Angebot und Nachfrage in ein Gleichgewicht und sind dadurch ein Mechanismus für **Preissetzung**. Dies führt zu einer Nutzenmaximierung der beteiligten Wirtschaftsakteure im volkswirtschaftlichen Sinn (Allokationseffizienz). Die Anerkennung und Operationalisierung des wirtschaftlichen Wertes von Daten ist unabdingbar für langfristiges, tragfähiges Wachstum der digitalen Wirtschaft. Damit faire Preise ausgehandelt werden können und kein Marktteilnehmer andere übervorteilen kann, ist **Informationssymmetrie** notwendig. Ein weiteres Merkmal funktionierender Märkte ist, dass es Wettbewerb gibt, so dass die Marktteilnehmer dazu angehalten sind, ihre Effizienz zu erhöhen. Preissetzung durch einen Markt hat den weiteren Vorteil, dass jeder Marktteilnehmer den Wert des gehandelten Guts mit geringem Aufwand einschätzen kann. Dies ist insbesondere für ein so abstraktes Gut wie Daten bzw. Datensätze vorteilhaft.
- Ein marktbasierter Ordnungsrahmen schafft **Rechtssicherheit** für alle Akteure. Durch die Einhaltung klarer Nutzungsberechtigungen innerhalb eines definierten Rechtsrahmens können etwaige Rechtsstreitigkeiten bezüglich unerlaubter Datennutzung vermieden werden. Rechtssicherheit ist eine wichtige Grundlage für wirtschaftliches Handeln, da erst dann Verbindlichkeit garantiert und ein gesteuerter Umgang mit Risiken (bzw. deren Vermeidung) möglich ist. Geeignete Kontroll- und Sanktionsmechanismen gewährleisten die Einhaltung des Ordnungsrahmens. Der jeweilige Datensouverän hat somit die Sicherheit, dass nur von ihm autorisierte Daten zweckgebunden verwendet werden und seine Daten ansonsten geschützt sind.

- Ein marktbasierter Ordnungsrahmen ist die Basis für **mobilitätsdatenbasierte Geschäftsmodelle**. Die Verwertung von Daten schafft neue Möglichkeiten der Wertschöpfung durch Produktentwicklungen und -optimierungen. Sie ermöglicht weiterhin die Verbesserungen und Vertiefung der Kundenbindung.
- Im Zusammenhang mit Märkten stellt sich auch die Frage nach **Standardisierung** (bspw. über einheitliche Datenformate, unterstützende Systeme und Schnittstellen), denn diese vereinfachen Transaktionen und reduzieren Transaktionskosten durch eine Reduktion der Komplexität im Markt. Ansatzpunkte diesbezüglich wären die Entwicklung einheitlicher Standards (siehe Handlungsempfehlung 7.2) oder die Schaffung einer herstellerübergreifenden Plattform (Deutschland bzw. EU) für *Infotainment*-Systeme.

Im Zusammenhang mit der Einführung eines Marktes ist wichtig, dass es für die Akteure tatsächlich möglich ist, am Handel auf dem Markt freiwillig teilzunehmen. Dazu ist sicherzustellen, dass keine „Alles-oder-nichts-Kopplungen“ des Einsatzes der Datennutzung an das Mobilitätsinstrument bestehen.

Zusammengefasst lautet das **zweite Strukturelement**:

Markt für Mobilitätsdaten: Mobilitätsdaten können wie andere Wirtschaftsgüter auf einem Markt gehandelt werden.

4.3.3 Akteure mit Verfügungsgewalt

Schließlich ist festzulegen, welche Akteure die initiale Verfügungsgewalt über Daten haben sollen. Die Zuordnung der Datensouveränität zu Akteuren soll so gestaltet sein, dass Aushandlungsprozesse möglichst einfach sind und – als wesentliche Bedingung – Investitionen sich auszahlen können. Vorteilhaft ist daher, dass der Datensouverän derjenige ist, der die **wirtschaftliche Berechtigung** über das Mobilitätsinstrument, im konkreten Fall über das Fahrzeug, hat. Dieser Akteur handelt in der Regel die Nutzungsbedingungen aus (Kauf bzw. *Leasing*/Miete des Fahrzeugs). Regeln zur Datennutzung werden dann in den entsprechenden Verträgen als Zusatzvereinbarungen festgelegt.

Die Zuweisung der Datensouveränität zum wirtschaftlich Berechtigten des Mobilitätsinstruments ist aus zweifacher Hinsicht sinnvoll.

- Neben der Verknüpfung des potenziellen wirtschaftlichen Nutzens mit der vorhergehenden Investition ist diese **Zuordnung in der Regel eindeutig** und auch **in der Praxis einfach anwendbar**.
- Auch praktische Erwägungen sprechen für diese Zuweisung, denn in der Regel werden dann **Datensouveränität und Anforderungen aus Sicht des Datenschutzes einfach vereinbar** sein – in der überwiegenden Zahl der Fälle ist der Nutzer des Fahrzeugs, der einen Anspruch auf Datenschutz hat, auch der wirtschaftlich Berechtigte (durch Kauf, *Leasing* oder Miete).

Diese Argumentation zeigt auch, dass die in Kapitel 3.3 erwähnte starke faktische Verfügungsgewalt nicht das Optimum in Bezug auf maximale Wertschöpfung sein kann, da sie beide der oben genannten Kriterien verletzt: Der Aushandlungsprozess ist nicht einfach, da bspw. bei personenbezogenen Daten ein anderer Akteur ein Mitspracherecht hat. Zudem wird der Entwicklungsaufwand für die notwendige Technik im Fahrzeug in der Regel durch den Kaufpreis abgegolten, so dass dadurch der wirtschaftlich Berechtigte und der Datensouverän voneinander verschieden wären.

Neben der Festlegung eines Akteurs mit Verfügungsgewalt sind auch **Nutzungsrechte** wichtig. Hier gibt es eine Vielzahl möglicher Ausgestaltungen. Ein Modell, das Abstufungen erlaubt, erscheint grundsätzlich attraktiv. Es gibt eine Vielzahl von Nutzungsdimensionen, für die Abstufungen möglich sind; einige repräsentative Dimensionen sind die im Folgenden genannten:

- **Begrenzte Weitergabe, Möglichkeit zum Widerruf.** Es könnte z. B. im Interesse eines Nutzers sein, dass seine Daten zwar von dem ihm bekannten Akteur, an den er diese weitergegeben hat, genutzt werden dürfen, diese dann aber nicht an weitere Akteure weitergegeben werden dürfen. Noch restriktiver wäre eine Bedingung, dass die Datennutzung widerrufbar ist.
- **Parallele Nutzung.** Möglich ist auch, dass nicht nur einem, sondern mehreren Akteuren die Nutzung bzw. Nachnutzung ermöglicht wird. Eine parallele Nutzung würde grundsätzlich in Summe eine höhere Wertschöpfung ermöglichen. Zu beachten ist aber, dass fehlende Ausschließlichkeit auch den individuellen Wert der Daten für jeden nachnutzenden Akteur verringern kann.
- **Anonymisierung, Pseudonymisierung.** Ebenso ist denkbar, dass Daten mit der Einschränkung verfügbar gemacht werden, dass sie nur in anonymisierter oder pseudonymisierter Form verarbeitet werden sollen.

Eine Einschätzung *a priori*, welche Kombination der Varianten entlang der einzelnen Dimensionen zu einer maximalen Gesamtwertschöpfung führt, ist nicht möglich, denn diese hängt von den konkreten Geschäftsmodellen bei der Nachnutzung ab:

- Einige der genannten Abstufungen bzw. Einschränkungen setzen voraus, dass ein Datum stets von Metadaten begleitet wird, die die Rahmenbedingungen für die Nutzung dieses Datums beschreiben. Damit verbunden sind zur Wertschöpfung gegenläufige höhere Kosten und eine größere Komplexität von Transaktionen.
- Selbst wenn keine oder nur wenige Metadaten notwendig sein sollten, gibt es gegenläufige Effekte. So führt bspw. eine geforderte Anonymisierung dazu, dass es eine höhere Bereitschaft für die Datenfreigabe geben kann, der darauf basierende wirtschaftliche Mehrwert aber durch den geringeren Wert anonymisierter Daten kompensiert wird.

Aus Sicht des in dieser ökonomischen Analyse beschriebenen Modells wäre es vorzugswürdig so, dass auf dem Markt für Mobilitätsdaten verschiedene Modelle für Abstufungen konkurrieren und dasjenige mit der höchsten Gesamtwertschöpfung im Wettbewerb gewinnt. In der Praxis würden die Bedingungen, die an die Datennutzung gestellt werden, in Form von Nutzungslizenzen kodifiziert werden. Abgestuften Nutzungsrechten entsprächen dann auch abgestufte Nutzungslizenzen (es ist zu erwarten, dass abgestufte Nutzungslizenzen nur dann praktikabel sind, wenn es ein Kopplungsverbot gibt). In Konsequenz sollte also eine rechtliche Regelung zu möglichst wenigen Einschränkungen an Nutzungsvarianten führen.

Zusammengefasst lautet das **dritte Strukturelement**:

Akteur mit Verfügungsgewalt: Der wirtschaftlich Berechtigte des Mobilitätsinstruments ist der Datensouverän.

Im weiteren Verlauf des Dokuments werden die Strukturelemente der **Datensouveränität und der Verfügungsgewalt als Einheit** behandelt. Dies hat insbesondere den Grund, dass aus rechtlicher Sicht für Lösungsausprägungen diese beiden Themen stets zusammen auftreten. Datensouveränität ist erst dann aus rechtlicher Sicht abschließend geregelt, wenn klar ist, wer diese besitzt. Verfügungsgewalt ist nur dann sinnvoll zuzuweisen, wenn es ein übergreifendes Konzept gibt, das diese in einen Kontext stellt.

4.3.4 Trends und Entwicklungen bei daten-basierten Geschäftsmodellen

Ein Blick über die Grenzen zeigt, dass erste Unternehmen damit beginnen, ihren Nutzern ein gewisses Ausmaß von expliziter Verfügungsgewalt über ihre Daten zu geben. Im Mittelpunkt stehen wie im skizzierten Lösungsansatz **Datensouveränität** und die **Teilhabe der Nutzer an dem monetären Wert ihrer Daten**. Diese Geschäftsmodelle basieren meist auf Plattformen, die als Vermittler zwischen Nutzern (Verkäufern) und Unternehmen (Käufern) auftreten, die die freigegebenen Daten analysieren und in anonymisierter, aggregierter Form weitergeben. Zu nennen sind insbesondere die unten genauer vorgestellten amerikanischen *Start-ups* *Datawallet* und *Datacoup*, welche ihren Nutzern einen **plattformbasierten Ort für den Handel mit persönlichen Daten** bieten.

Beide Unternehmen ermöglichen es ihren Nutzern, Konten anderer Plattformen wie z. B. Facebook, Twitter, Instagram oder Pinterest mit den jeweiligen internen Plattformen zu verbinden und auszuwählen, welche Daten sie an welche Unternehmen verkaufen möchten (z. B. nur „Likes“ und Geburtsjahr, nicht aber Universität und E-Mail-Adresse des Facebook-Kontos). Bei beiden Modellen ist es derzeit so, dass *Datawallet/Datacoup* die Daten von den Nutzern kaufen und in **anonymisierter, aggregierter Form** an ihre Unternehmenskunden weitergeben. Der Nutzer erhält immer dann eine **Vergütung**, wenn seine Daten zur Generierung der jeweiligen Analysen verwendet wurden. Die Höhe der Vergütung ist stark variabel und abhängig von verschiedenen Faktoren. Da die Preise von den Nutzerzahlen auf beiden Seiten abhängig sind, stellt die noch geringe Marktgröße beider Unternehmen ein Hindernis dar. Ähnliche Ansätze verfolgen das englische *Start-up Handshake* und das australische *Start-up Meeco.me*.

Alternativ zu diesen plattformbasierten Modellen gibt es eine Entwicklung hin zu **Open-Source-Projekten**, die ebenfalls das Ziel verfolgen, den Nutzern die Kontrolle über die Verwendung ihrer Daten zurückzugeben. Beispielhaft ist die *MyData Initiative* Finnlands, die eine standardisierte Infrastruktur für das Management persönlicher Daten schaffen will. Die Nutzer sollen Transparenz über die sektorübergreifend existierenden Datensätze erlangen sowie die rechtlichen und technischen Möglichkeiten bekommen, diese zu kontrollieren und nach eigenem Ermessen für bestimmte Zwecke freizugeben.

Auch im Mobilitätssektor gibt es Entwicklungen hin zu Geschäftsmodellen, welche es den Nutzern diverser Mobilitätsdienste erlauben, an dem durch Datennachnutzung generierten wirtschaftlichen Mehrwert zu partizipieren. Exemplarisch sind das im Folgenden vorgestellte Produkt *TankTaler* des Münchener *Start-ups Thinxnet GmbH* und das amerikanische Unternehmen *Automatic.com*. Beide im Folgenden vorgestellten Unternehmen sind gute Beispiele dafür, wie im Bereich von Mobilitätsdaten Plattformen mit mehrseitigen Geschäftsmodellen entstehen können.

TankTaler

Das *TankTaler* System umfasst einen Hardwarestecker, welcher über die **OBD-II-Schnittstelle** mit dem Fahrzeug und über ein Smartphone, auf der die **TankTaler-App** installiert ist, mit dem Internet verbunden ist. Für den Endkunden erscheint der Dienst wie ein Bonusprogramm. Wie bei anderen Programmen dieser Form ist der Kern des Geschäftsmodells der Aufbau eines starken Kundennetzwerks und die damit verbundene Verhandlungsstärke bei der Aushandlung von Rabatten mit beteiligten Unternehmen. Vor diesem Hintergrund sind Hardwarestecker und App, anders als vergleichbare Möglichkeiten der **Auslese von Diagnose-daten** mittels OBD-II-Schnittstelle, kostenfrei.

Über die OBD-II-Schnittstelle werden kontinuierlich Informationen über Fahrzeugzustand und -position sowie über das Fahrverhalten ausgelesen, über Mobilfunk auf die Server des Unternehmens übertragen und dem Autofahrer über die zugehörige Smartphone-App auf dem Smartphone angezeigt.

Darüber hinaus erhält der Fahrer für die Bereitstellung der beim Fahren und Tanken entstehenden Daten (sowohl Diagnose- als auch Positionsdaten) eine Gutschrift in Form von Bonuspunkten („**TankTaler**“). Diese Gutschrift entspricht einem Wert von 0,1 Cent pro gefahrenem Kilometer und 2 Cent pro getanktem Liter Kraftstoff bei allen Tankstellen deutschlandweit. „TankTaler“ können ähnlich wie bei anderen Bonuspunktesystemen beim Einkauf bei Partnerunternehmen eingelöst werden. Anders als bestehende Bonus- oder Meilensysteme sendet das Unternehmen dem Fahrzeugnutzer **lokalisierte Werbung** und Prämienangebote der Partnerunternehmen per App zu. Für den Kauf bei diesen Partnerunternehmen gibt es weitere Bonuspunkte. Interessant ist, dass die Einblendung von Werbung via Push-Nachrichten auf dem Smartphone optional ist und vom Nutzer deaktiviert werden kann²²⁴.

224 Gocacher, TankTaler – GPS-Auto-Stecker – Deal oder Datenschleuder?, 2016, abrufbar unter: <http://www.gocacher.de/tanktaler-gps-auto-stecker-deal-oder-datenschleuder>

Die Fahrzeugnutzer profitieren durch den Erhalt von Informationen bezüglich Fahrzeugstatus, Convenience durch digitale Bezahlssysteme²²⁵ sowie Kostenvorteilen (z. B. sparsamere Fahrweise aufgrund der Analyse des Fahrverhaltens und Rabatte bei *TankTaler*-Partnern). TankTaler verdient durch Werbeanzeigen und Provision an Käufen von *TankTaler*-Nutzern bei Partnerunternehmen, die wiederum durch Zusatzgeschäft und eine neue Art der Kundeninteraktion profitieren.

Automatic.com

Auch beim amerikanischen Unternehmen *Automatic.com* werden Fahrzeugdaten über die **OBD-II-Schnittstelle** ausgelesen. Der Adapter stellt selbst eine 3G-Verbindung über das Mobiltelefonnetz her. Die Fahrzeugdaten werden auf die **Plattform** von *Automatic.com* hochgeladen. Eine Vielzahl von Diensten kann dann auf diese Daten zugreifen. Beispielsweise kann das Fahrzeug mit Hilfe des Systems geografisch getrackt werden und im Fall eines Unfalls Hilfe herbeigerufen werden. Im Angebot sind weiterhin eine **Vielzahl von Apps**, z. B. für Fahrtenbücher, Automatisierungsdienste und Zugriffsmöglichkeiten für Werkstätten. Die gespeicherten Informationen werden auf der Plattform im Format eines Dashboards aufbereitet. Eine Auswertung des Fahrverhaltens kann genutzt werden, um umweltfreundlicher zu fahren.

Automatic.com ist Partnerschaften mit Automobilunternehmen und Versicherungen eingegangen, die auf die Daten zugreifen können. Darüber hinaus sollen die Daten auch durch Stadtplaner und zur Entwicklung selbstfahrender Fahrzeuge genutzt werden können.

4.3.5 Public und Private Open Data

Abschließend soll noch ein Sonderfall, der bei den Strukturelementen angesprochen worden ist, vertieft werden. Im Zusammenhang mit datengetriebenen Anwendungen ist es sinnvoll, auch das Thema *Open Data* zu beleuchten.

Open Data sind in der Regel **Open Public Data**, d. h. staatliche Stellen können, soweit anderweitige Schranken, wie z. B. datenschutzrechtliche Vorschriften, dem nicht entgegen-

genstehen, Daten, die im öffentlichen Sektor erzeugt wurden, als Open Data zur Verfügung stellen. Die Öffnung von Daten kann unterschiedlichen Zwecken dienen. Grundsätzlich geht es entweder um die Schaffung von **Transparenz** für Bürger oder um die Bereitstellung von Daten für eine **unternehmerische oder zivilgesellschaftliche Nachnutzung**. Im Rahmen dieser Studie wird das Thema *Open Data* im Kontext der Nachnutzung verstanden. Im Mobilitätsbereich ist zu erwarten, dass eine große Menge nachnutzbarer Daten entsteht. Ein typischer Ansatz wäre die Bereitstellung von anonymisierten Daten, die im Rahmen von **Car-2-Infrastructure-Anwendungen** entstehen. Auf Basis dieser Daten kann bspw. die lokale Verkehrsdichte erhoben werden, die Anbieter von Navigationssystemen zur verbesserten Routenplanung einsetzen können. Der Einsatz im unternehmerischen Bereich erfordert allerdings eine breite Verfügbarkeit und hohe Qualität der Daten.

Neben offenen öffentlichen Daten gibt es auch öffentliche private Daten, also Private Open Data. Hierbei handelt es sich um offene Daten, die durch einen nicht-öffentlichen Marktspieler bereitgestellt werden und die in der Regel auch nicht durch eine öffentliche Institution gesammelt worden sind. Für ein solches Vorgehen kann es vielfältige Motive geben. Ein Vergleich mit Open-Source-Software bietet sich zur Illustration an. Manche Unternehmen veröffentlichen den Quellcode von Software mit sehr liberalen Nachnutzungsmöglichkeiten, um bspw. auf der Softwarenutzung aufbauend komplementäre Services anzubieten, weil sie grundsätzlich einen neuen Markt erschließen möchten, weil sie eine bestimmte Standardisierung vorantreiben wollen oder weil sie schlicht aufgrund von Open-Source-Lizenzbedingungen dazu gezwungen sind. Open-Source-Software hat in den vergangenen zwei Dekaden die Softwareindustrie stark geprägt. Die Aussage, dass ein ähnliches Phänomen auch für Private Open Data entstehen könnte, wäre natürlich reine Spekulation. Die Tatsache, dass es Unternehmen gibt, die Daten öffentlich bereitstellen, zeigt aber, dass in bestimmten Einzelfällen eine geeignete Motivation vorhanden sein kann²²⁶. Private Open Data sollte als eine Variante von offenen Daten in einem ggf. entstehenden regulativen Rahmen möglich sein.

²²⁵ An Tankstellen kann direkt über die App vom Auto aus gezahlt werden.

²²⁶ So stellt die *Stromnetz Berlin GmbH* über das Portal www.netzdaten-berlin.de Datenmaterial zum Berliner Stromverteilungsnetz als *Open Data* bereit.

4.4 Ergebnis: Hohe wirtschaftliche Gesamtwertschöpfung durch Datensouveränität und Schaffung eines Marktes für Daten

Die ökonomische Analyse hat ergeben, dass die explizite Einführung von Daten als Wirtschaftsgut eine wichtige Voraussetzung für eine hohe wirtschaftliche Gesamtwertschöpfung ist. Wesentliche Konzepte sind **Datensouveränität** im Sinne einer **Verfügungsgewalt** und die Schaffung der Voraussetzungen für einen **Markt für Daten**. Einige der erläuterten Geschäftsmodelle zeigen, dass sich erste Trends in diese Richtung abzeichnen. Die Etablierung eines auf Datensouveränität und Markt basierten Systems der Monetarisierung von Daten ist aber naturgemäß ein eher lang-

fristiges Unterfangen. Neben der Schaffung eines Rechtsrahmens müssen diese Ideen auch in der Gesellschaft breit verankert werden. Die Bedeutung dieser Entwicklung lässt sich auch daran ermessen, dass mit Daten ein weiterer Produktionsfaktor neben die wohlbekannten Faktoren Arbeit, Kapital und Boden tritt. Zwar verfolgen einige der größten Unternehmen der Welt²²⁷ datenbasierte Geschäftsmodelle und sind innerhalb weniger Jahre entstanden, es ist aber anzunehmen, dass diese erst den Anfang einer langfristigen und gleichwohl volatilen Entwicklung markieren. In Bezug auf *Open Data* fördert das Bundesministerium für Verkehr und digitale Infrastruktur mit dem *mFund* bereits digitale Geschäftsideen, die auf Mobilitäts-, Geo- und Wetterdaten basieren. Das Ministerium stellt auch vielfältige Datensätze in Form von *Open Data* im Rahmen des Nationalen Aktionsplans *Open-Data* bereit²²⁸.

227 Beispielsweise befinden sich *Google, Facebook, Alibaba, Tencent* und *Amazon* unter den nach Marktkapitalisierung 40 größten Unternehmen der Welt (PwC, Global Top 100 Companies by market capitalisation, 2015).

228 Siehe hierzu insbesondere die Webseite www.bmvi.de/DE/DigitalesUndRaumentwicklung/DigitalUndMobil/NationalerAktionsplanOpenData/open-data_node.html.

5 Optionen zur Realisierung von Datensouveränität

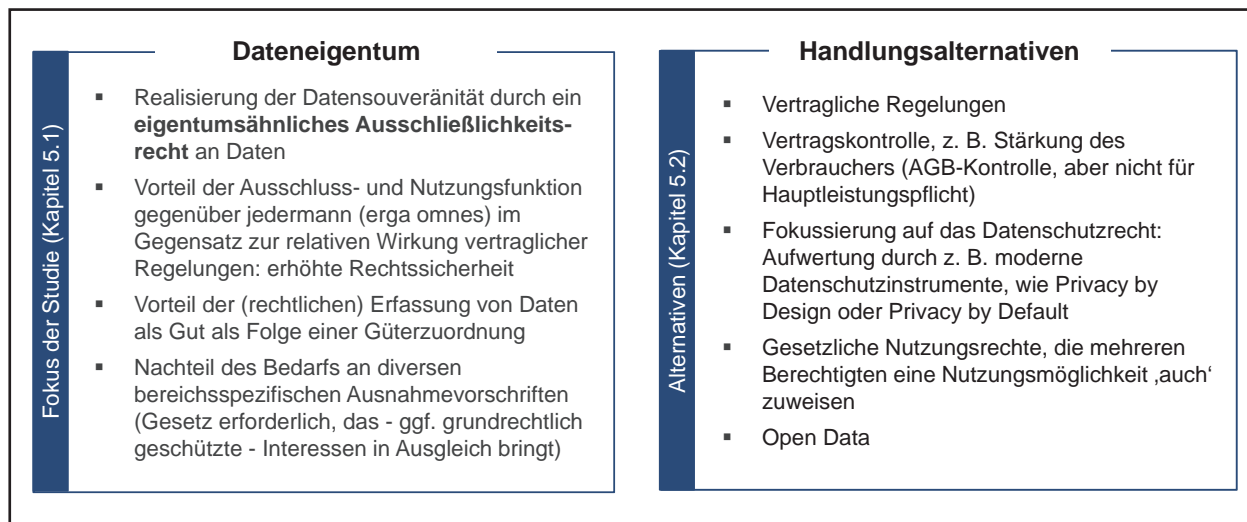


Abbildung 23: Rechtliche Regelungsoptionen zur Realisierung von Datensouveränität

Die Erkenntnisse der vorangehenden Analysen haben gezeigt, dass die Frage der Regelungsnotwendigkeit primär nach ökonomischen Aspekten zu beurteilen ist²²⁹. Aus diesen folgt, dass Datensouveränität im Sinne einer Verfügungsgewalt und die Schaffung der Voraussetzungen für einen Markt für Daten wesentlich sind, um eine hohe Gesamtwertschöpfung durch Datennutzung zu erreichen. Da der Fokus dieser Studie auf der Frage des Dateneigentums liegt, werden nachfolgend verschiedenen Optionen zur Realisierung einer solchen Datensouveränität – verstanden als wirtschaftliche, positive Verwertungsmöglichkeit – untersucht. Im Kern sind dabei zwei Möglichkeiten vorstellbar, welche beide in diesem Kapitel untersucht werden (siehe Abbildung 23).

Zum einen ist dies die bereits im Namen der Studie anklingende Option der Realisierung eines **umfassenden Dateneigentums im Sinne eines Ausschließlichkeitsrechts** (siehe Kapitel 5.1.). Die Fokussierung der Studie auf dieses Modell soll jedoch nicht automatisch eine diesbezügliche Präferenz andeuten, sondern ist dem Umstand geschuldet, dass vor allem in der juristischen Diskussion derzeit entsprechende Ansätze diskutiert werden. Ebenso denkbar und untersuchenswert sind denkbare **Alternativen**, die in einem umfassenden Ausschließlichkeitsrecht münden können (siehe Kapitel 5.2.).

5.1 Explizite – übergreifende – Zuordnung von Daten zu einem „Dateneigentümer“

Zunächst soll der Ansatz näher betrachtet werden, der Daten einer Person zuordnet und diese zu einer Art „**Dateneigentümer**“ macht. Verbunden damit ist die Hoffnung, mittels der Zuordnung der Daten zu einem Verfügungsberechtigten den beschriebenen Ist-Zustand zu beseitigen, bei dem die faktische Zugriffsmöglichkeit durch die tatsächlichen Gegebenheiten oftmals erschwert ist²³⁰, und derart die aus ökonomischer Sicht wünschenswerten Voraussetzungen des Wirtschaftsguts Daten²³¹ zu schaffen.

Diesbezüglich sind zwei grundsätzliche Herangehensweisen denkbar. Zum einen besteht die Möglichkeit, Dateneigentum durch eine **analoge Anwendung bestehender Vorschriften** zu konstruieren (siehe Kapitel 5.1.1.). Gelangt man hierdurch jedoch zu keinem befriedigenden Ergebnis, bleibt nur die Option, ein Ausschließlichkeitsrecht ggf. unter Weiterentwicklung im geltenden Recht angelegter Ansätze **neu zu konstruieren** und zu normieren (siehe Kapitel 5.1.2.).

²²⁹ Siehe dazu vor allem unter Kapitel 4.3.

²³⁰ Siehe dazu Kapitel 3.3.

²³¹ Siehe dazu Kapitel 4.3.

5.1.1 Bestimmung des Dateneigentümers durch analoge Anwendung des geltenden Rechts

Geprüft werden soll daher zunächst, ob sich aus den allgemeinen zivilrechtlichen Grundsätzen eine **allgemeine Verfügungsbefugnis** für Daten in analoger Anwendung der aufgezeigten bereichsspezifischen Zuordnungen ableiten lässt.

5.1.1.1 Analoge Anwendung des § 903 BGB

In Betracht kommt eine **analoge Anwendung des § 903 BGB** in Bezug auf Daten, um ein Dateneigentum zu konstruieren. Eine abstrakte rechtliche Zuweisung von Daten ist zwar im geltenden Zivilrecht nicht geregelt, jedoch ist in § 303a StGB bereits die Zuordnung von Daten zu einer Person, die zum Ausschluss Dritter vom Umgang mit den Daten berechtigt ist, angelegt²³². In der Literatur wird daher vertreten, eine derartige Stellung komme dem zivilrechtlichen Eigentum nahe und rechtfertige daher auch den Schluss auf eine dingliche Rechtsposition²³³.

Eine analoge Anwendung der Vorschrift überzeugt jedoch aus verschiedenen Gründen nicht. Zum einen kann wegen der Vielzahl von datenspezifischen Vorschriften an anderen Stellen der Rechtsordnung nicht auf eine planwidrige Regelungslücke im BGB geschlossen werden²³⁴. Weiterhin sind etliche sachenrechtliche Vorschriften auf körperliche Gegenstände zugeschnitten. So setzt bspw. eine Übereignung gem. § 929 BGB eine Übergabe voraus, durch die der vormalige Eigentümer seine Besitzposition aufgibt. Daten hingegen werden typischerweise ohne solchen Publizitätsakt übertragen, indem Kopien erzeugt werden und der Veräußerer weiterhin das Datum behält. Daher fehlt es aufgrund der mangelnden Körperlichkeit von Daten und deren regelmäßigem Wertverlust durch Zeitablauf an einer vergleichbaren Interessenlage²³⁵.

Zudem trifft § 903 BGB keine Zuordnungsentscheidung, sondern setzt diese voraus. § 903 BGB regelt nur die Befug-

nisse, die das zivilrechtliche Eigentum dem Berechtigten an dem jeweiligen Gegenstand verschafft (Ausschluss- und Nutzungsfunktion). Ohne weitergehende Aussage zur Zuordnungsentscheidung bietet eine analoge Anwendung dieser Vorschrift keinen Mehrwert. Lediglich die §§ 946 ff. bzw. §§ 953 ff. BGB regeln den originären Erwerb von Eigentum durch eine bestimmbare Person. Die §§ 929 ff. BGB regeln zudem den derivaten Erwerb von Eigentum an beweglichen Sachen. Diese Normen wiederum sind mangels Sacheigenschaft von Daten schwerlich auf solche übertragbar.

5.1.1.2 Anerkennung eines Rechts am eigenen Datenbestand

Da derzeit keine Erfassung über § 823 Abs. 1 BGB stattfindet²³⁶, wird erwogen, ein Recht am eigenen Datenbestand als „**sonstiges Recht**“ anzuerkennen²³⁷. Sonstige Rechte i. S. d. § 823 Abs. 1 BGB müssen jedoch eine Vergleichbarkeit mit den ausdrücklich aufgeführten, geschützten Rechtsgütern aufweisen, die allesamt als absolute Rechte Ausschluss- und Nutzungsfunktion besitzen²³⁸. Jedoch kann nicht darauf abgestellt werden, ob dem Datenbestand ein Zuweisungsgehalt und eine Ausschlussfunktion innewohnen, da die Möglichkeit, Dritte von der Nutzung eines Gutes auszuschließen, gerade von der Anerkennung als absolutes Recht durch die Rechtsordnung abhängt.

Das Recht am eigenen Datenbestand ließe sich durch die Rechtsprechung als sonstiges Recht mit der Folge einer absoluten Wirkung anerkennen. Zur Beurteilung dessen Sinnhaftigkeit bietet sich ein Vergleich der zu schützenden Rechtsposition mit den anderen bisher anerkannten absoluten Rechten unter allen – auch ökonomischen – Gesichtspunkten an²³⁹. Richtigerweise ist der Schutz über § 823 Abs. 1 BGB nur Folge der Anerkennung eines Gutes als absolutes Recht – eine derartige Anerkennung muss durch Legislative oder Judikative erfolgen. Sofern Dateneigentum, verstanden als Ausschließlichkeitsrecht, bereits *de lege lata* existiert (bspw. durch Anerkennung eines Dateneigentums in Analogie zu § 903 BGB oder Bejahung

²³² Siehe dazu Kapitel 3.2.3.

²³³ Hoeren, MMR 2013, 486 (486).

²³⁴ Sahl, PinG 2016, 146 (148); Peschel/Rockstroh, MMR 2014, 571 (572); Dorner, CR 2014, 617 (626); anders: Hoeren, MMR 2013, 486 ff.

²³⁵ Boesche/Rataj, Zivil- und datenschutzrechtliche Zuordnung von Daten vernetzter Elektrokraftfahrzeuge, S. 34.

²³⁶ Siehe dazu bereits unter 3.2.5.2.

²³⁷ Hoeren, Der strafrechtliche Schutz von Daten durch § 303a StGB und seine Auswirkungen auf ein Datenverkehrsrecht, in: Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 303 (305); siehe dazu auch BGH NJW 1996, 2924 (2925); Meyer/Wehlau, NJW 1998, 1585 (1588); Bartsch, Daten als Rechtsgut nach § 823 Abs. 1 BGB, in: Grützmacher (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, S. 297 ff.; siehe auch Dorner, CR 2014, 617 (619).

²³⁸ Wagner, in: MüKo BGB, § 823 Rn. 143.

²³⁹ Faust, 71. DJT, Teil A S. 82; siehe zu Gründen für die Schaffung von Ausschließlichkeitsrechten auch Jacob, Ausschließlichkeitsrechte an immateriellen Gütern, S. 8 ff.

einer der nachfolgend zu untersuchenden Ansätze), ergäbe sich auch ein Schutz über § 823 Abs. 1 BGB. Insofern gilt das bereits zu § 903 BGB Gesagte, dass es sich um eine reine **Konsequenzvorschrift** und keine Zuordnungsnorm handelt.

5.1.1.3 Anerkennung von Daten als Früchte der datengenerierenden Sache

Wie gezeigt wurde ist § 99 BGB nicht auf Daten anwendbar²⁴⁰. In Betracht käme jedoch eine **analoge Anwendung** von § 99 BGB. Diesbezüglich stellt sich indes die Frage, ob es sich im Hinblick auf diverse datenbezogene Vorschriften und das gesamte Immaterialgüterrecht überhaupt um eine planwidrige Regelungslücke handelt. In jedem Fall mangelt es aber an der Vergleichbarkeit der Rechts- und Interessenlage, da es sich bei dem Sachenrecht um ein **Regime der rivalen Nutzungen** handelt, das überwiegend Besitz voraussetzt bzw. an diesen anknüpft²⁴¹. Des Weiteren ergibt sich aus der Einordnung von Daten als Früchte selbst keine eigentumsrechtliche Zuweisung – insoweit hilft auch § 101 BGB nicht²⁴². Diese Vorschrift regelt lediglich den Umfang des Fruchtziehungsrechts. Die eigentumsrechtliche Zuordnung der Früchte ist in § 953 BGB geregelt, der das Eigentum an Erzeugnissen und sonstigen Bestandteilen dem Eigentümer der betreffenden Sache zuweist. Aufgrund fehlender Vergleichbarkeit von Daten und Sachen ist diese Regelung wiederum nicht auf „Dateneigentum“ übertragbar. Weiterer Schwachpunkt einer derartigen Zuweisung ist deren Anwendbarkeit lediglich auf eine bestimmte Schnittmenge von Daten. Von diesem Ansatz betroffen sind lediglich solche Daten, die von einem technischen Gerät erzeugt werden; hinsichtlich der dinglichen Zuweisung anderer Datenkategorien bedürfte es einer weiteren Zuordnungsmethode.

5.1.1.4 Sachgenerierte Daten als Nutzungen

Des Weiteren könnte darüber nachgedacht werden, § 100 BGB, nach dem Gebrauchsvorteile zu den Nutzungen zählen, die bei Fehlen anderweitiger Regelungen dem Eigentümer der Sache zustehen (§ 903 BGB), analog auf sachgenerierte Daten anwenden. Nachteil dieses Ansatzes ist jedoch, dass die alleinige Einordnung als Nutzung **keine dingliche Zuweisung** bewirkt. Eine solche entstünde erst, indem man annimmt, Daten seien derart eng mit dem datengenerierenden Gegenstand verbunden, dass sich die Berechtigung an der Sache (§ 903 BGB) auch an den erzeugten

Daten fortsetzt. Aufgrund der bereits dargelegten Abweichung von Daten vom typischen Erscheinungsbild sonstiger Gebrauchsvorteile²⁴³ lässt sich die genannte Vorschrift allerdings nicht – auch nicht analog – auf Daten anwenden. Ferner bestünde auch hier das bereits bei der Einordnung der Daten als Früchte auftretende Problem der Erfassung anderer Datenkategorien, die nicht von technischen Geräten erzeugt werden.

5.1.1.5 Zwischenergebnis

Mit der bloßen analogen Anwendung geltender Regelungen lässt sich ein **Dateneigentum nicht herleiten**. Die genannten bereichsspezifischen Regelungen lassen sich aus diversen, vielfältigen Gründen nicht verallgemeinern bzw. übertragen. Insofern sind die **existierenden Ansätze** im Hinblick auf die Begründung eines allgemeinen Dateneigentums **nicht zielführend**. Will man daher ein umfassendes Ausschließlichkeitsrecht entwickeln, bedarf es einer vollständigen Neuentwicklung. Bezüglich der Art und Weise einer Zuordnung des Ausschließlichkeitsrechts zu einem Rechtssubjekt sind verschiedene Ansätze denkbar.

5.1.2 Neuentwicklung eines Ausschließlichkeitsrechts an Daten/eines Dateneigentums (*de lege ferenda*)

Zur Neuentwicklung eines Ausschließlichkeitsrechts sollen zunächst die relevanten Merkmale eines Gutes dargestellt werden, dem von der Rechtsordnung Eigentums- oder eigentumsähnliche Funktionen zuerkannt werden (Ausschluss- und Nutzungsfunktion) (Kapitel 5.1.2.1.). Dabei sind die sonstigen Erwägungen, die zum rechtlichen Schutz des (Sach-)Eigentums geführt haben, zu extrahieren und ggf. für die Anerkennung eines absoluten Rechts an Daten zu verallgemeinern. Für die Bewertung kann es hilfreich sein, sich auch die historischen Überlegungen, die zur Schaffung von Immaterialgüterrechten führten, bewusst zu machen (Kapitel 5.1.2.2.). Darauf aufbauend lässt sich untersuchen, ob Daten diese Merkmale heute bereits aufweisen und sich daraus eine Rechtfertigung bzw. Notwendigkeit zur Schaffung von „Dateneigentum“ ergibt. Auf dieser Grundlage soll geprüft werden, wie ein „Dateneigentum“ dogmatisch begründet werden könnte. Hierfür sollen denkbare Ansätze für eine Zuordnung eines Ausschließlichkeitsrechts zu einem Berechtigten, die teilweise auf einer Weiterentwicklung bereits geltender bereichsspezifischer

²⁴⁰ Siehe dazu Kapitel 3.2.5.3.

²⁴¹ Zech, CR 2015, 137 (141 f.).

²⁴² Jickeli/Stieper, in: Staudinger (Hrsg.), BGB, § 99 Rn. 1; Zech, CR 2015, 137 (142).

²⁴³ Siehe dazu Kapitel 3.2.5.4.

scher Regelungen beruhen, vorgestellt und bewertet werden (Kapitel 5.1.2.3.).

5.1.2.1 Merkmale eines Ausschließlichkeitsrechts

Unter den Oberbegriff der Ausschließlichkeitsrechte fallen sowohl unübertragbare Persönlichkeitsrechte als auch übertragbare Herrschaftsrechte; zu letzteren zählen das Sacheigentum sowie die Immaterialgüterrechte²⁴⁴. Die Diskussion um ein mögliches Dateneigentum ist als Überlegung zur Normierung eines übertragbaren Herrschaftsrecht zu verstehen; ein unübertragbares Ausschließlichkeitsrecht an personenbezogenen Daten existiert bereits mit dem Recht auf informationelle Selbstbestimmung²⁴⁵. Die Existenz von Sacheigentum wurde notwendig, da Sachen i. S. d. § 90 BGB in ihrer Nutzbarkeit in der Regel rival sind²⁴⁶. Es bedurfte einer Güterzuordnung, die dem Eigentümer gegenüber jedermann (*erga omnes*) wirkende Befugnisse an seinem Gut einräumt. Diese Befugnisse bestehen in der grundsätzlichen Möglichkeit, nach freiem Belieben mit dem Gegenstand zu verfahren (**Nutzungsfunktion**), sowie in der Möglichkeit, andere von der Nutzung des Gutes auszuschließen (**Ausschlussfunktion**), § 903 BGB. Die übrigen Rechtssubjekte dürfen grundsätzlich auf den zugewiesenen Bereich weder einwirken noch diesen positiv nutzen; insoweit wird der Bereich der Privatautonomie der übrigen Rechtssubjekte zugunsten eines erweiterten Freiheitsraums des Berechtigten belastet²⁴⁷. Das primäre Recht des Berechtigten sollte weiterhin verkehrsfähig sein, um einen wirtschaftlichen Handel mit Gütern und somit Wertschöpfung zu ermöglichen.

Bei Daten handelt es sich um Wirtschaftsgüter, die regelmäßig in ihrer Nutzung nicht-rival sind (vgl. hierzu Kapitel 4.3, Abbildung 21 und Abbildung 22). Ausnahmefälle können bestehen, wenn die Reproduktionskosten bspw.

aufgrund großer Datenmengen, unzureichend verfügbarem Speicherplatz oder außergewöhnlichen Datenformaten sehr hoch sind. Dennoch besteht in der Praxis zunehmend ein Bedürfnis, eine Güterzuordnung in Bezug auf das Wirtschaftsgut „Datum“ zu treffen, da ein Interesse an einer dinglichen Berechtigung, die Wirkung gegenüber jedermann entfaltet, besteht. Aufgrund der Vielzahl von Akteuren, die Interessen an Daten geltend machen und der diversen bereichsspezifischen Regelungen sind vertragliche Absprachen zwischen zwei Parteien zunehmend ungeeignet, eine valide Rechtsposition für ein Rechtssubjekt zu schaffen. Da vertragliche Absprachen stets nur zwischen den beteiligten Parteien Geltung beanspruchen, besteht stets das Risiko, dass Dritte Daten in unerwünschter, ggf. beeinträchtigender Weise nutzen und dies rechtlich nicht unterbunden werden kann. Des Weiteren könnte ein Ausschließlichkeitsrecht den Handel mit Daten, die sich zu einem enormen Wirtschaftsfaktor entwickelt haben, erleichtern²⁴⁸. Mit einer dinglichen, eigentumsähnlichen Rechtsposition würde der Erwerber beim Datenkauf eine gegenüber jedermann wirkende Rechtsposition erlangen (Rechtssicherheit).

5.1.2.2 Historische Gründe für die Schaffung von Immaterialgüterrechten

Der Schaffung von Immaterialgüterrechten lag der Gedanke zugrunde, dass die Investition (technische bzw. geistige Leistung) in die Erzeugung immaterieller Güter, denen zunehmend wirtschaftlicher Wert beigemessen wurde, belohnt werden müsse. Ähnlich verhält es sich heute mit Daten – sie haben sich zweifelsfrei zu einem immateriellen Gut entwickelt. Daher liegt es auch nahe, dass demjenigen, der in die Erzeugung dieses Gutes investiert hat, dessen Verwertung nach der Rechtsordnung gebühren sollte²⁴⁹.

244 Eine Ausnahme stellt insoweit das Urheberrecht dar, das ein Hybridrecht mit vermögens- und persönlichkeitsrechtlichen Elementen darstellt; Ohly, Gibt es einen Numerus clausus der Immaterialgüterrechte?, in: Ohly u.a. (Hrsg.), Perspektiven des Geistigen Eigentums und Wettbewerbsrechts, Festschrift für Gerhard Schricker zum 70. Geburtstag, S. 105 ff.; zur monistischen Theorie Schack, UrhR, 7. Aufl. 2015, Rn. 339 ff.

245 Specht/Rohmer, PinG 2016, 127 (128).

246 Siehe zum Begriff bereits im ökonomischen Teil unter Kapitel 4.3.

247 Specht/Rohmer, PinG 2016, 127 (127).

248 Ausführlich dazu unter Kapitel 4.3.

249 Schefzig, K&R Beihefter 3/2015, 3.

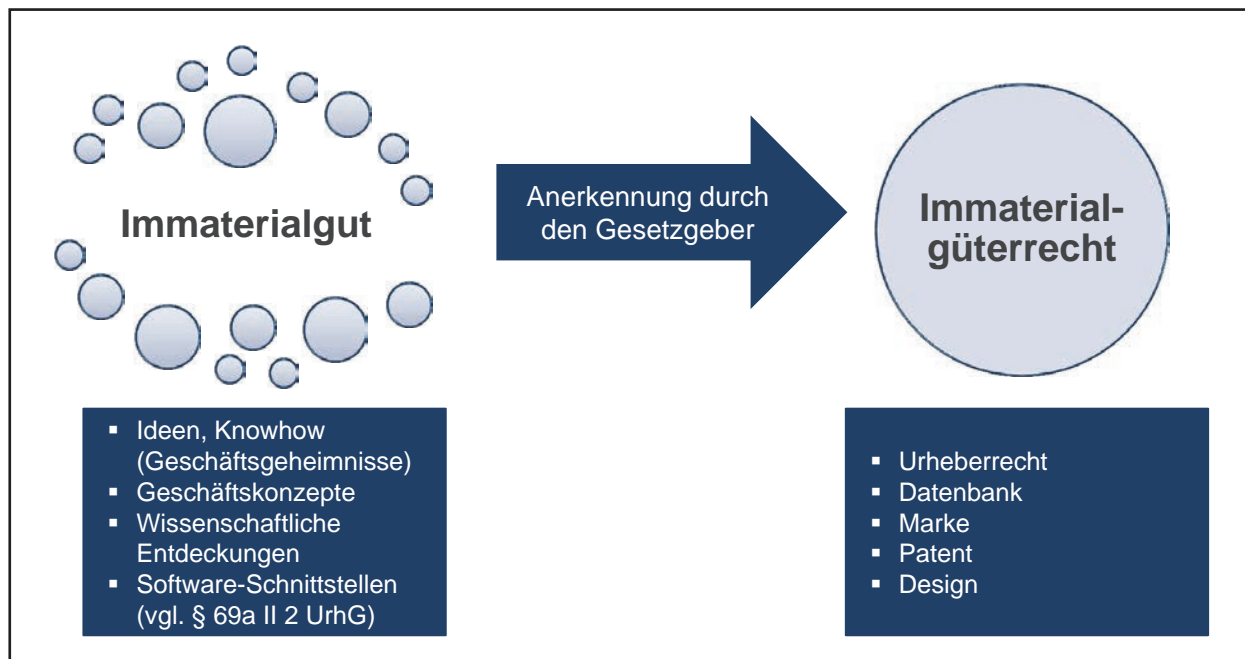


Abbildung 24: Gründe zur Schaffung von Immaterialgüterrechten

Mit den Immaterialgüterrechten hat der Gesetzgeber bereits an anderer Stelle Ausschließlichkeitsrechte geschaffen, um technische, unternehmerische oder schöpferische Leistungen zu belohnen, die immaterielle Güter betreffen. Auch Daten sind heute ein Immaterialgut, so dass es nahe liegt, deren gewachsene Bedeutung mit einem eigenständigen Ausschließlichkeitsrecht zu Gunsten des Investors anzuerkennen. Einen vergleichbareren Weg hat der Gesetzgeber beim Leistungsschutzrecht des Datenbankherstellers (§ 87a UrhG) beschritten.

„Pate“ für die Ausgestaltung eines zu schaffenden Rechts am Dateneigentum könnten daher die bestehenden Immaterialgüterrechte, allen voran die aus dem UrhG sein²⁵⁰. Es regelt in Teil 1 bspw. ausführlich Gegenstand (§§ 2 ff. UrhG), Inhaberschaft (§§ 7 ff. UrhG), Inhalt (§§ 11 ff. UrhG), Übertragbarkeit (§§ 28 ff. UrhG) und Schranken (§§ 44a ff. UrhG) der Rechte von Urhebern. Teil 2 enthält zudem zahlreiche Sonderregeln für verwandte Schutzrechte, die ebenfalls Vorbild für ein Dateneigentumsrecht sein können (siehe Kapitel 3.2.2).

Neben der Struktur liefert das Urheberrecht wichtige Erfahrungen und Lehren, die in die Entscheidung über die Einführung eines Ausschließlichkeitsrechts für Daten mit einfließen sollten: Um die Freiheitssphären Dritter zu be-

wahren, beruht auch das UrhG auf dem Grundsatz, dass Ideen, Methoden und Informationen frei bleiben müssen. Sie gehören bislang zur *domaine public* und entziehen sich damit der exklusiven rechtlichen Zuordnung durch Ausschließlichkeitsrechte²⁵¹. Wie schwer der Ausgleich der aufgezeigten Interessen ist, zeigt ferner die langjährige Diskussion über die Schranken des Urheberrechts. Um künftig einen gerechteren Ausgleich zwischen den Interessen der Werkschaffenden und denen von anderen Kreativen, von privaten Nutzern im Netz, Plattformbetreibern und vielen anderen Mitgliedern der Allgemeinheit zu erreichen, wird über die Öffnung des als zu starr empfundenen Schrankenkatalogs durch Öffnungsklauseln oder die Einführung einer „fair-use-clause“ nach US-Vorbild gerungen²⁵².

5.1.2.3 Denkbare Ansätze für eine Zuordnung von „Dateneigentum“

Näher betrachtet werden soll nunmehr, wie ein solches Ausschließlichkeitsrecht an Daten konkret umgesetzt werden könnte, ohne dass dabei zugleich eine Entscheidung für die Schaffung eines solchen getroffen werden soll.

Sicher ist zunächst, dass es für ein eigentumsähnliches Ausschließlichkeitsrecht entsprechender gesetzgeberischer Maßnahmen bzw. richterlicher Rechtsfortbildung bedarf.

²⁵⁰ Vgl. Schwartmann/Hentsch, PinG 2016, 117 (122).

²⁵¹ Schack, UrhR, 7. Aufl. 2015, Rn. 194 ff.; Dorner, CR 2014, 617 (622).

²⁵² Siehe nur Ohly, 70. DJT, Teil F, S. 62 ff.

Für die Zuweisung eines Ausschließlichkeitsrechts lassen sich **drei verschiedene Anknüpfungspunkte** ausmachen²⁵³: Zunächst könnte es sich anbieten, spezifische Zuordnungen, die lediglich für einen Teilbereich von Daten gelten, als Ausschließlichkeitsrechte zu perpetuieren. Ein anderer Ansatz knüpft bei der Neuregelung an gültige Vorschriften aus dem Sachenrecht an. Abschließend käme die Anknüpfung an den Akt der Datenerzeugung und ein darauf gerichtetes Tätigwerden von Rechtssubjekten in Betracht.

5.1.2.3.1 Datenspezifische Ansätze

Daten lassen sich in zahlreiche Kategorien einteilen, wovon die Unterscheidung nach dem Vorliegen eines inhaltlichen Personenbezugs die Relevanteste darstellt. Knüpft man hinsichtlich der Zuweisung exklusiver Rechte an die konkreten Eigenschaften der jeweiligen Gruppen von Daten an, lassen sich eventuell passend zugeschnittene Lösungen erzielen. Problematisch ist jedoch, dass es erstens Datenkategorien gibt, für die *de lege lata* keine bereichsspezifischen Regelungen existieren und hinsichtlich derer ein Zuweisungsmechanismus ausstünde und zweitens einige Daten eventuell mehreren bereichsspezifischen Regelungen unterfallen und sich daher keine eindeutige Zuordnung nach nur einem Ansatz ergibt. Daher scheint es sachgerechter einen allgemeinen Zuweisungsmechanismus zu entwickeln, der für alle Daten gilt.

Zuordnung zum Betroffenen im Sinne des Datenschutzrechts

In Bezug auf fahrzeugbezogene Daten, die einen Unterfall der sog. „**Sachdaten**“ darstellen – verstanden als Gegenbegriff zu personenbezogenen Daten – trifft das BDSG keine rechtliche Regelung. Der Anwendungsbereich dieses Gesetzes beschränkt sich auf die Erhebung, Verarbeitung und Nutzung von Daten über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbar Personen (vgl. §§ 1 Abs. 2, 3 Abs. 1 BDSG). Zweck des Gesetzes ist es nach § 1 Abs. 1 BDSG, den Einzelnen vor Beeinträchtigung in seinem Persönlichkeitsrecht durch Datenverarbeitung zu schützen²⁵⁴. Im Fokus der datenschutzrechtlichen Regelungen steht daher die Beeinträchtigung primär immaterieller Schutzgüter der Betroffenen; deren wirtschaft-

liche Interessen sowie solche anderer Akteure spielen bei der Schaffung des BDSG keine Rolle²⁵⁵.

Der Umgang mit (personenbezogenen) Daten hat sich jedoch stark gewandelt. Zu Recht wird angemerkt, dass mit der zunehmenden Vernetzung und automatisierten Analyse enormer Datenvolumina den Daten ein wirtschaftlicher Wert zukommt sowie verstärkt Personenbezüge im Sinne von Bestimmbarkeit zumindest potenziell hergestellt werden können. Mit dem stetigen Aufkommen neuer Technologien wandelt sich daher auch das Verhältnis von personenbezogenen zu nicht-personenbezogenen Daten und mitunter wird daher das Kriterium des Personenbezugs von Daten als untauglich bzw. zu weitreichend für den Persönlichkeitsschutz angesehen²⁵⁶. In Bezug auf das Kfz lässt sich über das Kennzeichen bzw. die Fahrgestellnummer der Halter eines Fahrzeugs ermitteln, so dass jedenfalls nach der Theorie vom absoluten Personenbezug²⁵⁷ bei allen fahrzeugbezogenen Daten ein Personenbezug besteht. Ungeachtet der immer noch nicht ganz geklärten Auslegung des Begriffs der Personenbestimmbarkeit – insoweit hat die Entscheidung des EuGH in einem Verfahren zum Personenbezug von IP-Adressen schon dahingehend etwas Klarheit gebracht, dass das Vorhandensein von rechtlichen Zugriffsmöglichkeiten auf Zusatzinformationen ausreicht²⁵⁸ – ist jedoch festzuhalten, dass nach § 4 Abs. 1 BDSG zum Schutz des Betroffenen eine Verarbeitung der auf ihn bezogenen Daten lediglich mit dessen Einwilligung oder im Falle eines gesetzlichen Erlaubnistatbestands zulässig ist. Durch das ihm gegenüber jedermann zustehende, absolut wirkende Abwehrrecht gegenüber einer nicht legitimierten Datenverarbeitung, erlangt der Betroffene eine starke Rechtsposition.

Es erscheint überlegenswert, auch im deutschen Rechtsraum eine **Property-Rights-basierte Konzeption des Datenschutzrechts** zu etablieren. Wesentliches Argument ist, dass die bisherige Ausgestaltung des Datenschutzes falsche Anreize für Unternehmen zur übermäßigen Nutzung personenbezogener Daten setze, da diese sämtliche Gewinne internalisieren könnten, während etwaige Nachteile zu Lasten des betreffenden Datensubjekts gehen würden²⁵⁹. In der strukturellen Asymmetrie der Verhandlungsmacht zwi-

253 Es handelt sich dabei ausschließlich um eine Darstellung der in der Literatur vertretenen Ansätze; zur rechtlichen sowie ökonomischen Bewertung derselben siehe unter 5.1.4.

254 Siehe zum geltenden (und zukünftigen) Datenschutzrecht bereits unter 3.2.1.

255 Gola/Klug/Körffner, in: Gola/Schomerus (Hrsg.), BDSG, § 1 Rn. 6 ff.

256 Dammann, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, § 3, Rn. 38.

257 Nach der Theorie vom absoluten Personenbezug ist es ausreichend, wenn irgendein Dritter in der Lage ist, einen Personenbezug herzustellen, während die Theorie vom relativen Personenbezug darauf abstellt, ob die datenverarbeitende Stelle in der Lage ist, eine Person mithilfe der ihr selbst zur Verfügung stehenden Mittel zu bestimmen. Siehe ausführlich zu dem Streitstand Dammann, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, § 3, Rn. 23 ff.

258 EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer/Deutschland.

259 Dorner, CR 2014, 617 (626); Kilian, in: GS Steinmüller, 2014, S. 195 (203).

schen Datensubjekten und datenverarbeitenden Unternehmen wird sogar ein Marktversagen gesehen, das sich auch auf monopolartige Stellungen weniger global agierender Unternehmen in diesem Marktsegment stützt²⁶⁰. Im Rahmen eines privatrechtlich geprägten Datenschutzes seien mit einer eigentumsrechtlichen Ausgestaltung angemessene Partizipationsmöglichkeiten der Datensubjekte gewährleistet. In der Befugnis des Persönlichkeitsträgers zur Entscheidung über die Verwendung personenbezogener Daten (§ 4 BDSG) kann ein Anknüpfungspunkt für eine güterrechtliche Zuweisungsentscheidung liegen²⁶¹. Es handelt sich bei dem de lege lata existierenden Ausschließlichkeitsrecht an personenbezogenen Daten in Form der informationellen Selbstbestimmung um ein Persönlichkeitsrecht; daneben könnte ein übertragbares Herrschaftsrecht des Persönlichkeitsträgers bestehen. Güterrechtlich liege es nach Specht nahe, auch den Schritt zu einer Zuweisung von Ausschließlichkeit zu gehen²⁶². Dann läge das Recht zur wirtschaftlichen Verwertung des Datums stets beim Betroffenen i. S. d. Datenschutzrechts.

Betrachtet man jedoch die genannten Gründe für die Schaffung von Immaterialgüterrechten²⁶³, gilt als grundsätzlich konstituierend für die Zuweisung von Herrschaftsrechten und der damit verbundenen Möglichkeit der wirtschaftlichen Verwertung eines Gutes eine erbrachte **Eigenleistung**²⁶⁴. Es ist fraglich, ob der Persönlichkeitsträger stets erheblichen Anteil an der Entstehung eines auf ihn bezogenen Datums hat²⁶⁵. Das Persönlichkeitsrecht und die damit verbundenen Rechte in Bezug auf personenbezogene Daten stehen dem Betroffenen nicht aufgrund von Leistung, sondern kraft seiner Existenz zu²⁶⁶. Die erforderliche Eigenleistung wird mitunter bei bekannten Persönlichkeiten in dem Aufbau ihres Images und der damit verbundenen Steigerung des Marktwerts der auf sie bezogenen Daten gesehen²⁶⁷ – diese Argumentation lässt sich jedoch nicht auf alle personenbezogenen Daten verallgemeinern. Im Falle des „Normalbürgers“ könnte man auf die erbrachte Opferleistung der Betroffenen abstellen, die in den Einschränkungen zu sehen ist, die durch die massenhafte Datenverarbeitung im Rahmen von *Big Data* entstehen

(gläserner Kunde, Zuschläge bei Versicherungstarifen, massenhafte individuelle Bewerbung von Potenzialkunden)²⁶⁸. Ob dies für die Rechtfertigung einer Güterzuordnung indes ausreichend ist, muss im Vergleich zu den für andere Ausschließlichkeitsrechte erforderlichen Leistungen bezweifelt werden²⁶⁹.

Fraglich ist zudem, ob der Normierung eines derartigen Vermögensrechts nicht schon verfassungsrechtliche Gründe entgegenstehen. Mit dem Volkszählungsurteil hat das BVerfG einen weiteren Teilschutzbereich des allgemeinen Persönlichkeitsrechts entwickelt: die **informationelle Selbstbestimmung**. Gewährleistet ist die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen²⁷⁰. Zugleich wurde betont, dass dieses Recht **keine absolute, uneinschränkbare Herrschaft über Daten** vermittele. Diese Passage wurde vielfach derart verstanden, dass sie einem Ausschließlichkeitsrecht des Betroffenen an personenbezogenen Daten entgegenstehe. Diese Auslegung ist nicht zwingend – im Gegensatz bezieht sich das BVerfG lediglich darauf, dass die informationelle Selbstbestimmung nicht schrankenlos gewährleistet sein könne. Im sog. Spickmich-Urteil²⁷¹, ergangen zu einer Zeit als Daten, anders als zur Zeit des Volkszählungsurteils, bereits kommerzieller Wert zukommt und das Internet etliche Lebensbereiche durchdrungen hat, beziehen sich die Ausführungen des BGH ausschließlich auf eine erforderliche Interessenabwägung zwischen dem Persönlichkeitsrecht der Klägerin und der Meinungsfreiheit der Allgemeinheit. Auch hier wird das informationelle Selbstbestimmungsrecht lediglich als nicht schrankenlos gewährleitetes, sondern im überwiegenden Allgemeininteresse beschränktes Recht qualifiziert. Eine Reihe von Ausschließlichkeitsrechten unterliegen jedoch derartigen Beschränkungen, betrachtet man nur die §§ 44a ff. UrhG, §§ 23 ff. MarkenG oder §§ 11 bis 13 PatG. Auch das Sacheigentum ist nach Art. 14 Abs. 2 GG nicht uneingeschränkt gewährleistet, sondern unterliegt dem Verfassungsgrundsatz der Sozialpflichtigkeit. Die Beschränkung eines Rechts spricht daher nicht prinzipiell gegen dessen Ausgestaltung als Ausschließlichkeitsrecht²⁷².

260 Dorner, CR 2014, 617 (626); Kilian, in: GS Steinmüller, 2014, S. 195 (212 f.).

261 Specht, CR 2016, 288 (292).

262 Specht, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, S. 79 m. w. N.

263 Siehe dazu Kapitel 5.1.2.

264 Specht/Rohmer, PinG 2016, 127 (131); Peukert, Güterzuordnung als Rechtsprinzip, 2008, S. 209.

265 Zech, GRUR 2015, 1051 (1055); Specht/Rohmer, PinG 2016, 127 (131).

266 Klüber, Persönlichkeitsschutz und Kommerzialisierung, 2007, S. 222.

267 Hermann, Der Werbewert der Prominenz, 2011, S. 216 m. w. N.

268 Specht/Rohmer, PinG 2016, 127 (131).

269 Specht/Rohmer, PinG 2016, 127 (131); kritisch auch Zech, GRUR 2015, 1051 (1055).

270 BVerfGE 65, 1 (43).

271 BGHZ 181, 328.

272 Specht, CR 2016, 288 (292 f.); Specht/Rohmer, PinG 2016, 127 (130).

Aus ökonomischer Sicht ist jedoch besonders **problematisch**, dass sich bei einem einheitlichen Akt der Datenerzeugung je nach Vorliegen eines Personenbezugs des betreffenden Datums eine **unterschiedliche Zuweisung** ergeben kann. Da von datengenerierenden Gegenständen vielfach in kurzer Zeit erhebliche Datenbestände erstellt werden, ist für die beteiligten Akteure bei diesem Zuweisungsmechanismus nicht auf den ersten Blick ersichtlich, wem das Ausschließlichkeitsrecht an welchem konkreten Datum zusteht. Dies erschwert die wirtschaftliche Nutzung der werthaltigen Daten enorm²⁷³.

Ein besonderes rechtliches Problem besteht auch in der **Zuordnung von Daten zu den Kategorien personenbezogen bzw. nicht-personenbezogen**²⁷⁴. Selbst vormalig nicht-personenbezogene Daten können mittels Verknüpfung anderer Informationen aus diversen Quellen einer bestimmten Person zugeordnet werden. Die Beurteilung der Schutzbedürftigkeit eines Datums ist in der Praxis dadurch stark erschwert, dass jede Einzelangabe im Kontext einer Vielzahl weiterer Daten betrachtet werden muss²⁷⁵. Hierbei ist unklar, wie die potenzielle Informationsbeschaffung zur Herstellung eines Personenbezugs zu bewerten ist. Die Einordnung eines Datums als personenbezogen kann nach der Theorie vom relativen oder der Theorie vom absoluten Personenbezug erfolgen. In der Literatur und nach der Rechtsprechung wird eindeutig die relative Theorie zur Bestimmung eines Personenbezugs favorisiert²⁷⁶. Dennoch ist auch hiernach unklar, ab welchem Grad der Aufwand zur Herstellung eines Personenbezugs für die konkrete datenverarbeitende Stelle als unverhältnismäßig anzusehen ist. Um den Personenbezug als taugliches Zuweisungskriterium für ein Ausschließlichkeitsrecht anzuerkennen, bedürfte es einer klaren Definition, die hinreichend Rechtssicherheit für die beteiligten Akteure bietet. Fraglich ist darüber hinaus, wie die Behandlung von vormalig personenbezogenen Daten bei einer nachträglichen Anonymisierung aussehen sollte – in diesen Fällen könnte das „Dateneigentum“ des Betroffenen erlöschen. Zur Lösung dieser Problematik bietet der Ansatz der Zuweisung nach dem Personenbezug in der aktuell in der Literatur vertretenen Form keinen überzeugenden Erklärungsansatz.

Vielfach wird einer Zuordnung nach dem Personenbezug die **Mehrrelationalität von Daten** entgegengehalten²⁷⁷. In der Tat beziehen sich Daten häufig auf mehrere Personen, etwa wenn Angaben zum Familienstand, zu Kindern und Angehörigen in einem Lebenslauf getätigt werden. Dieser Umstand erfährt durch die Industrie 4.0²⁷⁸ dadurch neue Dimensionen, dass etwa autonom von einem Fahrzeug generierte Daten Aussagen über sämtliche im Fahrzeug sitzende Personen treffen, bspw., ob diese angeschnallt sind, wie hoch die Achslast ist oder wie laut Musik gehört wird. Je nach der Art der erhobenen Daten können diese auch Aussagen über andere Verkehrsteilnehmer bzw. den Halter des Kfz beinhalten. Eine eindeutige Zuordnung zu einem Berechtigten sei aufgrund der Mannigfaltigkeit der Aussagemöglichkeiten eines Datums nicht gewährleistet²⁷⁹.

Zur Lösung dieser Problematik schlägt *Specht* hinsichtlich der Zuweisung mehrrelationaler Daten einen Rückgriff auf das zivilrechtliche **Institut des Gesamthand Eigentums** vor²⁸⁰. Bei einer Übertragung dieses Rechtsgedankens auf personenbezogene Daten könnten die Betroffenen ausschließlich gemeinschaftlich über das Datum disponieren. Die Betroffenheit mehrerer Personen ist auch kein Phänomen, das erst durch *Big Data* oder Industrie 4.0 aufgekommen ist. Bereits im geltenden Datenschutzrecht sind bei mehrrelationalen Daten Einwilligungen aller betroffenen Personen einzuholen²⁸¹. Wie noch aufzuzeigen sein wird, können sich auch nach anderen Zuweisungskriterien mehrere potenzielle Berechtigte als Inhaber eines Ausschließlichkeitsrechts anbieten. Hierfür sind geeignete Lösungen zu entwickeln, jedoch steht die Mehrrelationalität von Daten der Zuweisung eines eigentumsähnlichen Rechts an Daten nicht von vornherein entgegen.

Demgegenüber ist eine Zuweisung zum Betroffenen i. S. d. Datenschutzrechts nicht zwangsläufig zum Schutz von Persönlichkeitsrechten erforderlich. Wählt man anstelle des Personenbezuges eines der anderen Zuweisungskriterien, so würde das Datenschutzrecht das Ausschließlichkeitsrecht an Daten begrenzen – der Berechtigte wäre zur Nutzung eines personenbezogenen Datums stets auf die Einwilligung des Betroffenen bzw. das Eingreifen eines Er-

273 Siehe dazu Kapitel 4.3.3.

274 Siehe hierzu ausführlich *Jöns*, Daten als Handelsware, S. 23 ff.

275 *Schwartmann/Hentsch*, PinG 2016, 117 (121 f.).

276 Ausführlich zum Streitstand *Bergt*, ZD 2015, 365 ff.; EuGH, Urt. v. 19.10.2016, Rs. C-582/14, Breyer/Deutschland.

277 *Roßnagel/Pfützmann/Gerstka*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Inneren, S. 37 ff.; *Kilian*, CR 2002, 921 (924).

278 Dieser Begriff bezeichnet die prognostizierte vierte industrielle Revolution durch flächendeckende Vernetzung intelligenter Gegenstände, siehe <http://www.hightech-strategie.de/de/Industrie-4-0-59.php>.

279 *Specht/Rohmer*, PinG 2016, 127 (130 f.).

280 *Specht*, CR 2016, 288 (295); siehe auch *Ensthaler*, NJW 2016, 3473 (3477).

281 *Specht*, CR 2016, 288 (295).

laubnistatbestands angewiesen. Derartige Begrenzungen eines Ausschließlichkeitsrechts durch entgegenstehende Rechte Dritter sind in etlichen Bereichen feststellbar, ohne dass sie dessen Einführung entgegengestanden haben. Datenschutzrechtliche Probleme würden durch ein eigentumsähnliches Recht eines anderen als dem Betroffenen zwar nicht gelöst, jedoch auch nicht vertieft²⁸².

Insgesamt ist der Personenbezug als Zuweisungskriterium eines Ausschließlichkeitsrechts an Daten zwar aus rechtlicher Perspektive ein mögliches Zuweisungskriterium. Es sprechen jedoch gewichtige Gründe gegen diesen Ansatz. So führt das Datenschutzrecht vielfach nicht zu eindeutigen Ergebnissen, was unter ökonomischen Aspekten als nachteilig gesehen wird. Hinzu kommt, dass mangels **Eigenleistung** des Betroffenen im Zusammenhang mit der Datenerzeugung die Wahl eines anderen Ansatzes, der dieses Kriterium berücksichtigt, naheliegender ist. Schließlich bietet dieser Zuordnungsansatz keine Lösung für nicht-personenbezogene Daten. Er wird nachfolgend daher nicht weiter verfolgt.

Siehe zu den Konsequenzen dieser Ansicht in den Fallstudien: Tabellarische Übersichten im **Anhang**.

Unternehmensbezogene Zuordnung von Betriebs- und Geschäftsgeheimnissen

Daten genießen als Geschäfts- oder Betriebsgeheimnis den Schutz nach § 17 UWG, sofern sie einen Unternehmensbezug haben, nicht offenkundig sind, nach dem bekundeten Willen des Betriebsinhabers geheim gehalten werden sollen und ein berechtigtes Interesse an der Geheimhaltung besteht²⁸³. Dieser Geheimnisschutz sichert eine faktisch bestehende Ausschließlichkeit (straf-)rechtlich ab und gewährt dessen Inhaber Abwehrrechte gegenüber Dritten. Daher kann schon der geltenden Rechtslage eine gewisse Zuordnungsentscheidung an denjenigen entnommen wer-

den, der faktisch einen exklusiven Zugang zu den entsprechenden Daten hat²⁸⁴.

Im Rahmen der Schaffung von Dateneigentum wäre die Zuordnung eines Ausschließlichkeitsrechts zum Betriebsinhaber wie bei unternehmensbezogenen Daten denkbar²⁸⁵. Auch im Bereich des *Know-how*-Schutzes wird derzeit darüber nachgedacht, diesen aus dem Geheimnisschutz der §§ 17, 18 UWG herauszulösen und als eigenes Immaterialgüterrecht auszugestalten²⁸⁶. Der *Know-how*-Schutz bilde dann einen Teilbereich eines umfassenderen Ausschließlichkeitsschutzes an Daten. Auch ein mögliches Dateneigentum solle nur das Interesse von Unternehmen an der Vertraulichkeit wertvoller Daten schützen. Sollte dem so sein, könnte mit einem eigentumsähnlichen Ausschließlichkeitsrecht des Betriebsinhabers der gewünschte Schutz erzielt werden²⁸⁷. Alle unternehmensbezogenen Daten würden in der Folge über den Geheimnisschutz hinaus dem Unternehmensinhaber zur positiven Nutzung zugeordnet werden. Geschützt würden allerdings ausschließlich Daten, die der Dateninhaber geheim hält und die nicht offenkundig werden. Die Überlassung an einen in Bezug auf den konkreten Datenbestand zur Geheimhaltung verpflichteten Dritten würde die Geheimheit dabei nicht entfallen lassen.

Bei vielen Daten, die vernetzte Fahrzeuge generieren, fehlt jedoch der nötige Unternehmensbezug. Sie können oft nicht sicher einem bestimmten Unternehmen zugeordnet werden, weil sie etwa die Sphäre der Nutzer betreffen.²⁸⁸

Daher ist dieser Zuweisungsmechanismus nicht zur Zuweisung eines Ausschließlichkeitsrechts bezogen auf die zugrundeliegenden Fallstudien geeignet. Anstelle der Unternehmensbezogenheit möchte *Specht* daher die **Datenerzeugung** als relevantes Zuweisungsinstrument wählen, dennoch aber nur geheime Daten schützen. Das Merkmal der Geheimhaltung würde zu einer klaren Abgrenzbarkeit der geschützten Datenbestände führen. Zusätzlich zu einem Abwehrrecht gegen Geheimnisbruch umfasse eine güterrechtliche Zuordnung auch die positive Nutzung durch entsprechende Lizenzierung²⁸⁹.

282 *Specht*, CR 2016, 288 (294); *Specht/Rohmer*, PinG 2016, 127 (132).

283 *Diemer*, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, UWG, § 17 Rn. 9, siehe dazu auch bereits unter 3.2.4.

284 *Zech*, CR 2015, 137 (141).

285 Vgl. *Dorner*, CR 2014, 617 (622 f.).

286 *Specht*, CR 2016, 288 (289); McGuire, GRUR 2015, 424 (427).

287 *Specht*, CR 2016, 288 (290).

288 Siehe dazu Kapitel 3.2.4.

289 *Specht*, CR 2016, 288 (291, 294).

Die ausschließliche Anerkennung von Ausschließlichkeitsrechten im gewerblichen Bereich, die sich aufgrund des Erfordernisses der Unternehmensbezogenheit ergeben würde, scheint nicht gerechtfertigt. Auch *Specht* resümiert, dass ein Ausschließlichkeitsrecht an Daten auch Privaten zustehen müsse, weshalb sich *Know-how*-Schutz lediglich als Teilbereich eines Dateneigentums darstellen ließe²⁹⁰. Verzichtet man auf das Erfordernis der Betriebsbezogenheit, erscheint es dennoch nicht sachgerecht, ausschließlich geheime Daten zu schützen. Betrachtet man das Gut „Datum“, kommt diversen, auch offenkundigen Daten erheblicher Wert zu. Gerade die positive Nutzung könnte dazu führen, dass Daten offenbart werden und somit der Schutz entfallen würde. Insgesamt ist dieser Ansatz daher aus den voranstehenden Gründen abzulehnen.

Siehe zu den Konsequenzen dieser Ansicht in den Fallstudien: Tabellarische Übersichten im **Anhang**.

Datenverwertungsrecht für personenbezogene Daten in Anlehnung an das Urheberrecht

Möglicherweise könnte das Urheberrecht als neuer Ansatz für die Schaffung eines Datenverwertungsrechts dienen. Datenverwertungsrechte könnten die Verkehrsfähigkeit von Daten ermöglichen und mittels des Instruments der Lizenz einräumung zur Datennutzung könnte ein effektiver Datenschutz gewährleistet werden. Das Urheberrecht bietet insoweit einen gesetzlich abgewogenen Interessensausgleich zwischen dem Ausschließlichkeitsrechten der Schöpfer und dem Verwertungsinteresse der Allgemeinheit. Diesbezüglich wird argumentiert, dass gerade das Wechselspiel zwischen Ausschließlichkeit und Nicht-Ausschließlichkeit sich im Urheberrecht bewährt habe und auch auf das Datenschutzrecht zu übertragen sei. Hierzu trügen u. a. die Schrankenregelungen (§§ 44a ff UrhG) bei²⁹¹. Die datenschutzrechtliche Einwilligung sei durch Lizenzierungen zu ersetzen.

Das Urheberrecht ermöglicht nach §§ 31 ff. UrhG auf der Grundlage von Privatautonomie und Vertragsfreiheit die Einräumung einfacher oder ausschließlicher Rechte, deren Übertragung sowie zeitliche, räumliche oder inhaltliche Beschränkungen dieser Rechte. Hierfür spricht, dass die privatautonome Ausgestaltung von Nutzungsrechten mittels eines Lizenzvertrags (vgl. § 31 Abs. 5 S. 1 UrhG) zum einen flexiblere Gestaltungsmöglichkeiten als die datenschutzrechtliche Einwilligung zulässt und zum anderen durch die Übertragbarkeit die Verkehrsfähigkeit dieser Rechte sichert. Allerdings ist durch gesetzliche Regelungen sicherzustellen, dass Verbraucher von marktmächtigen Dienstleistern nicht übervorteilt werden und keine untolerierbaren Abhängigkeitsverhältnisse entstehen²⁹².

Diesem Vorschlag in Bezug auf ein Datenverwertungsrecht ist grundsätzlich zuzustimmen. Genau genommen handelt es sich jedoch nicht um einen Ansatz für die Zuweisung eines Ausschließlichkeitsrechts, sondern nur auf die **Ausgestaltung eines erwogenen Ausschließlichkeitsrechts an Daten**²⁹³. Das Urheberrecht ist nicht geeignet, eine Antwort auf die Frage zu geben, wer der Dateninhaber sein soll. Es bedarf bei dem hier vorgeschlagenen Datenverwertungsrecht des Rückgriffs auf einen der anderen Ansätze für dessen Zuordnung zu einem Berechtigten. Auch *Schwartmann* und *Hentsch* wollen dieses Recht nicht dem Schöpfer eines Werkes zuweisen, sondern dieses nach dem Personenbezug zuordnen²⁹⁴. Mangels persönlicher geistiger Schöpfung kann hier nicht auf den Schöpfer abgestellt werden, sondern die positive Nutzung eines personenbezogenen Datums gebührt dem Betroffenen i. S. d. Datenschutzrechts.

Siehe zu den Konsequenzen dieser Ansicht in den Fallstudien: **Anhang**.

290 *Specht*, CR 2016, 288 (291).

291 *Schwartmann/Hentsch*, PinG 2016, 117 (125).

292 *Schwartmann/Hentsch*, PinG 2016, 117 (122, 124); *Jöns*, Daten als Handelsware, S. 71 ff.

293 Zur Ausgestaltung des „Dateneigentums“ nach dem Vorbild der Vorschriften des Urheberrechts ausführlich unter Kapitel 5.1.2.

294 *Schwartmann/Hentsch*, PinG 2016, 117 (120 ff.); Zu den Schwächen einer Zuweisung nach dem Personenbezug siehe unter Kapitel 5.1.4.1.

5.1.2.3.2 Gegenständliche (sachenrechtliche) Ansätze

Grundsätzlich kann der Eigentümer einer Sache nach seinem Belieben mit dieser verfahren. Aufgrund der ausdifferenzierten **Regelungen zum Eigentum** im sachenrechtlichen Teil des BGB könnte es sich anbieten, zur Schaffung eines Dateneigentums auf diese zurückzugreifen und Daten körperlichen Gegenständen gleichzustellen. Eine weitere denkbare Ausgestaltungsmöglichkeit bestünde darin, das Dateneigentum den Berechtigungen an körperlichen Gegenständen folgen zu lassen. Aus dem Sacheigentum folgen Handlungsbefugnisse; die Zuweisung ist grundsätzlich weit, d. h. alle denkbaren Formen des Umgangs mit einer körperlichen Sache umfassend, zu verstehen. Das Sacheigentum schützt die Integrität von Gegenständen und reflexartig auch die Integrität der darauf gespeicherten Daten. Ferner hat der Eigentümer eines Gegenstands grundsätzlich auch das Recht zum Besitz und somit Zugang zu den auf dem körperlichen Datenträger befindlichen Daten²⁹⁵.

Daher könnte es sich anbieten, in einem nächsten Schritt an das Sacheigentum an einem körperlichen Gegenstand anzuknüpfen und daraus auch die Befugnis zur positiven Nutzung der auf diesem gespeicherten Daten herzuleiten. Grundsätzlich ist es allerdings aufgrund der immateriellen Natur von Daten problematisch, Regelungen zur Zuweisung der Handlungsbefugnisse an körperlichen Gegenständen zu übertragen.

§ 903 BGB

Während zur Begründung von Dateneigentum *de lege lata* eine Analogie zu § 903 BGB vorgeschlagen wird²⁹⁶, wird – soweit ersichtlich – eine explizite Normierung im BGB nach dem Vorbild des zivilrechtlichen Eigentums in der Literatur *de lege ferenda* nicht in Erwägung gezogen. Man könnte bspw. in den allgemeinen Teil des Gesetzes einen **§ 90b BGB** einfügen, der festlegt, dass Daten wie Sachen zu behandeln sind und die sachenrechtlichen Vorschriften entsprechend anzuwenden sind.

Eine Regelung des „Dateneigentums“ in Anlehnung an zivilrechtliches Eigentum nach § 903 BGB überzeugt jedoch nicht. Wie bereits dargelegt²⁹⁷, regelt § 903 BGB nicht die Voraussetzungen für die Entstehung von Eigentum, sondern lediglich dessen Rechtswirkungen. Diverse sachenrechtliche Vorschriften regeln konkret die Voraussetzungen

für einen originären (z. B. §§ 946 ff. BGB) oder derivativen (z. B. §§ 929 ff. BGB) Erwerb von Eigentum. Eine entsprechende Anwendung auf Daten erweist sich allerdings aufgrund der mangelnden Körperlichkeit von Daten teilweise als schwierig und nicht eindeutig. Folglich ist nach diesem Ansatz unklar, welche Tatbestandsvoraussetzungen zur Entstehung eines Ausschließlichkeitsrechts an Daten erfüllt sein müssten. Daher lässt sich auch keine exemplarische Zuordnung nach diesem Ansatz bezogen auf die Fallstudien vornehmen.

Aufgrund der Spezifika der zu betrachtenden Daten – fehlende Körperlichkeit – ist es sachlich naheliegender, hinsichtlich einer Normierung des Dateneigentums auf bewährte **Instrumente des Immaterialgüterrechts** zurückzugreifen. Immaterialgüterrechte entstehen durch Erfüllung der Tatbestandsvoraussetzungen des jeweiligen Spezialgesetzes, etwa Eintragung in das Markenregister (z. B. § 4 Nr. 1 MarkenG), Veröffentlichung im Patentblatt (§ 58 Abs. 1 S. 3 PatG), Entstehung des Werks durch einen schöpferischen Akt (§ 2 Abs. 2 UrhG) oder Herstellung einer Datenbank (§ 87a UrhG)²⁹⁸. All diese Entstehungstatbestände lassen sich jedoch nicht für Daten fruchtbar machen. Gerade in der Regelung der Voraussetzung für die Entstehung eigentumsähnlicher Ausschließlichkeitsrechte ist der hauptsächliche Mehrwert der speziellen Rechtsregime zu sehen. Hinsichtlich der Ausgestaltung des Dateneigentums sowie dessen Beschränkungen kann hingegen auf Vorschriften des Immaterialgüterrechts bspw. das Urheberrecht zurückgegriffen werden²⁹⁹. Das Sacheigentum bietet sich jedoch aufgrund der grundsätzlichen Unterschiedlichkeit materieller und immaterieller Güter nicht als Leitbild für Dateneigentum an.

Dateneigentum folgt dem Eigentum an körperlichen Gegenständen

Nach § 903 BGB kann der Eigentümer einer Sache nach Belieben mit dieser verfahren und andere von jeglicher Einwirkung ausschließen. Folglich umschreibt diese Vorschrift die dem Eigentümer im Umgang mit der Sache zustehenden Befugnisse, die sehr weit zu verstehen sind. Fraglich ist, ob sich die zugewiesenen Handlungsbefugnisse auch auf die mithilfe eines Gegenstands generierten Daten bzw. auf einem körperlichen Gegenstand gespeicherten Daten erstreckt. Wie bereits dargestellt, muss dies *de lege lata* verneint werden, da das Sachenrecht als Regime der rivalen Nutzungen zu verstehen ist und daher dem Eigentümer

295 Zech, CR 2015, 137 (141 f.).

296 Hoeren, MMR 2013, 486 (487).

297 Siehe Kapitel 3.2.5.1.

298 Bräutigam/Klindt, Digitalisierte Wirtschaft/ Industrie 4.0, S. 23.

299 Siehe hierzu ausführlich in Kapitel 5.1.2.

lediglich solche Befugnisse zugewiesen sind, die **Besitz** voraussetzen oder zumindest nach dem Vorbild des Besitzes rival sind. Der historische Gesetzgeber hatte nicht die heutigen technischen Möglichkeiten im Blick, die mittels des Kopierens von auf einem Datenträger gespeicherten Daten deren Loslösung von einem spezifischen Gegenstand und deren unbegrenzte Vervielfältigung ermöglichen³⁰⁰. In Betracht käme jedoch eine Ausgestaltung des Dateneigentums durch den Gesetzgeber, bei der Berechtigter an den Daten der Eigentümer des datengenerierenden Gegenstands bzw. des Trägermediums ist.

Eine Anknüpfung an das **Eigentum am datengenerierenden Gegenstand** wird bislang lediglich als Unterfall des Ansatzes nach dem Skripturakt vertreten³⁰¹. Rechtsinhaber eines Ausschließlichkeitsrechts solle derjenige sein, der den für die Entstehung von Daten erforderlichen Schaffensprozess bewirkt habe. Dies sei der wirtschaftlich verantwortliche Datenerzeuger, der die erforderlichen Produktionsmittel, bspw. den datengenerierenden Gegenstand, zur Verfügung stellt.

Wieck-Noodt schlägt hingegen vor, in Bezug auf die im Rahmen des § 303a StGB schwer zu bestimmende „Fremdheit“ der betreffenden Daten, ein Verfügungs- und Nutzungsrecht zugunsten der Person anzuerkennen, die **Eigentum am Datenträger** innehat. Der Eigentümer solle an den von ihm auf seinem Datenträger gespeicherten Daten Verfügungsrechte aus dinglichem Recht haben. Der am Datenträger Nutzungsberechtigte könne in der Folge einer anderen Person die Nutzung der auf seinem Datenträger gespeicherten Daten gestatten. Auch Welp hält die Beherrschung des Speicher- oder Übermittlungsmediums aufgrund der Notwendigkeit der „Verkörperung“ von Daten für ein geeignetes Zuweisungskriterium³⁰². Jedoch sind viele Ausgestaltungsfragen unklar. Über Daten, die unerlaubt auf einem fremden Datenträger gespeichert wurden, könnte nach Wieck-Noodt sowohl der Speichernde als auch der Eigentümer des Datenträgers verfassungsbefugt sein³⁰³. Folgt man streng dem Ansatz einer Zuordnung nach dem Eigentum am Datenträger, müsste eine Zuordnung zu Letztgenanntem erfolgen, die im Falle der Inanspruchnahme von Cloud-Dienstleistungen jedoch nicht sachgerecht erscheint.

Die Zuweisung eines eigentumsähnlichen Rechts an Daten an den Eigentümer des datengenerierenden Gegenstands bzw. an den Eigentümer des Speichermediums kann im Ergebnis **nicht überzeugen**. Das Eigentum an einer Sache gibt nicht unbedingt wieder, wer wirtschaftlich im Sinne von Eigenleistung die Datenerstellung veranlasst; es handelt sich vielmehr eher um eine zufällige Zuordnung, die nicht alle betroffenen Interessen sachgerecht in Ausgleich bringen kann. Bezogen auf Kraftfahrzeuge können Eigentum und wirtschaftlicher Betrieb (durch den Halter) bspw. im Fall des *Leasings* auseinanderfallen und die Zuordnung nach dem Eigentum vernachlässigt in gravierender Weise den Anteil des Fahrzeughalters an der Datenerzeugung. Doch auch außerhalb des vernetzten Fahrzeugs kann dieser Zuweisungsmechanismus bspw. im Falle der Datengenerierung mit Gegenständen in Unternehmen, bei denen aufgrund eines Eigentumsvorbehalts oder einer Sicherungsübereignung wirtschaftlicher Betreiber und Eigentümer auseinanderfallen, nicht überzeugen. Der Ansatz nach dem Eigentum am datengenerierenden Gegenstand erfasst ferner nicht alle Arten von Daten, da Daten auch mittels Eingabe generiert werden können. In diesen Fällen könnte das Eigentum an der jeweils genutzten Datenverarbeitungsanlage maßgeblich sein. Jedoch hat in vielen Fällen der Nutzung eines *Personal Computers* der Eigentümer eines solchen keinen Bezug zu den eingegebenen Daten bspw. bei dem Gebrauch eines Geräts durch vielfach wechselnde Nutzer.

Noch widersinniger scheint die Zuordnung nach dem Eigentum am Speichermedium. Insbesondere im Rahmen von **Cloud-Dienstleistungen** steht der Eigentümer des betreffenden Servers – abgesehen von der entgeltlichen Überlassung des Speicherplatzes – in keiner Beziehung zu den darauf gespeicherten Daten³⁰⁴. In gewissen operativen Leistungsmodellen (z. B. *Cloud Computing* oder *Leasingmodellen* für IT-Infrastruktur) fallen Datennutzer und Eigentümer des Datenmediums auseinander. Damit wäre die Verfügungsgewalt in der Hand eines Akteurs, der gerade nicht das spezifische wirtschaftliche Interesse an den Daten hat.

Ein scheinbarer Vorteil dieser beiden Ansätze, die an das Eigentum an körperlichen Gegenständen anknüpfen, liegt in

300 Zech, CR 2015, 137 (141 f.)

301 Specht befürwortet innerhalb der Zuweisung nach dem Skripturakt ein Abstellen auf das Zurverfügungstellen der zur Datengenerierung notwendigen Produktionsmittel, vgl. CR 2016, 288 (294); Zech, CR 2015, 137 (144).

302 Welp, iur 1988, 443 (447).

303 Wieck-Noodt, in: MüKo, StGB, 2. Aufl. 2014, § 303a Rn. 10.

304 Zech, CR 2015, 137 (138).

der Rechtssicherheit durch einen eindeutigen Zuweisungsmechanismus und der Publizität. Jedoch lässt sich durch den Besitz an einem körperlichen Gegenstand auf das Eigentum des Besitzers schließen (§ 1006 BGB), allerdings kann der Eigentümer und somit der Datenberechtigte in der Praxis nicht stets von allen Rechtssubjekten zweifelsfrei bestimmt werden. Die grundsätzliche Eindeutigkeit dieser Zuweisung sorgt aus ökonomischer Sicht zwar für geringe Transaktionskosten. Im Fall personenbezogener Daten wäre allerdings in einigen Szenarien zusätzlicher Aushandlungsaufwand mit den Betroffenen notwendig, was die Transaktionskosten wiederum erhöht.

Dieses Zuweisungskriterium könnte daher lediglich als eines mehrerer Kriterien zur Bestimmung des Inhabers des zu normierenden Ausschließlichkeitsrechts an Daten herangezogen werden. Aufgrund des Umstandes, dass Daten als „flüchtige Elemente“³⁰⁵ keiner dauerhaften Bindung an einen körperlichen Gegenstand bspw. an das zur erstmaligen Speicherung verwendete Trägermedium unterliegen, sind diese Ansätze als Zuweisungsmechanismen insgesamt eher ungeeignet.

5.1.2.3.3 Handlungsbezogene Ansätze

Abschließend kommen für die Zuweisung eines Ausschließlichkeitsrechts noch die Ansätze in Betracht, die an den **Akt der Datenerzeugung** anknüpfen. Diese Ansätze stellen auf die „erbrachte Eigenleistung“ bzw. die getätigte Investition in Bezug auf die Datenerzeugung und somit die Schaffung wirtschaftlicher Werte ab und sehen dies als Rechtfertigung für eine vermögensrechtliche Zuweisung an. Betrachtet man die erläuterten Gründe für die Schaffung von Immaterialgüterrechten (siehe Kapitel 5.1.2.2), sind die handlungsbezogenen Ansätze vorzugswürdig.

Abstellen auf die geistige Schöpfung

Das Zuweisungskriterium könnte sich auf den Prozess der Entstehung von Daten beziehen – insoweit kommt neben der technischen auch die geistige „Urheberschaft“ als Anknüpfungspunkt in Betracht³⁰⁶. Hierbei wird sich auf den Inhalt eines Datums und dessen Entstehung im menschlichen Geist bezogen, d. h. die Erzeugung des durch die Daten kodierten Informationsgehaltes. Anders als im geltenden Urheberrecht, das nach § 2 UrhG erst ab einer gewissen Schöpfungshöhe Werken urheberrechtlichen Schutz ver-

leiht, könnte jedweder Gedanke einem Ausschließlichkeitsrecht unterliegen.

Bei der Anwendung dieses Kriteriums würde der Urheberrechtsschutz jedoch in unangemessener Weise erweitert werden, da kein Recht am Datum, sondern ein Recht am Inhalt statuiert würde. Dieser Ansatz ist bezogen auf die Fallstudien zudem nicht praktikabel, da es sich bei den im Zusammenhang mit vernetzten Fahrzeugen erzeugten Daten vornehmlich um maschinengenerierte Daten handelt. Bei dieser Datenart ist der menschliche Einfluss auf die Datenerstellung gering, eine Entstehung im menschlichen Geist ist nicht gegeben. Es lässt sich daher keine exemplarische Zuordnung bezogen auf die Fallstudien nach diesem Ansatz vornehmen.

Es gilt daher, einen Zuweisungsansatz zu entwickeln, der sich allgemein auf alle Arten von Daten anwenden lässt. Die geistige Urheberschaft scheint dabei nicht praktisch operabel, da vollständig auf ein Publizitätsmoment verzichtet würde sowie jede Eingabe eines neuen Datums dem ursprünglichen Urheber des Inhalts zufallen würde³⁰⁷. Daher ist das Kriterium der geistigen Schöpfung als Zuweisungskriterium für ein Ausschließlichkeitsrecht an Daten ungeeignet.

Abstellen auf die Investition

Denkbar wäre ebenso, ein Ausschließlichkeitsrecht auf die Investition in die Datenerzeugung zu stützen. Auch bei der Einfügung des § 87b UrhG, der ein Leistungsschutzrecht sui generis des Datenbankherstellers normiert, war trager der Gedanke der Schutz der Investition in die Beschaffung, Prüfung und Darstellung der Daten³⁰⁸. Bei der Übertragung auf einfache Daten sollen weder Schutzvoraussetzungen noch Schutzzumfang der §§ 87a ff. UrhG entsprechende Anwendung finden, sondern es ist lediglich das Grundprinzip der §§ 87a ff. UrhG, das in dem Anreiz zu Investitionsleistungen liegt, fruchtbar zu machen³⁰⁹. Inhaber der Rechte aus den §§ 87a ff. UrhG ist der Datenbankhersteller, d. h. derjenige, der die Initiative zur Herstellung ergreift, sie organisatorisch betreut und mit der Investition das wirtschaftliche Risiko trägt³¹⁰. Zur Bestimmung des Rechteinhabers wird folglich im Rahmen des Datenbankschutzes nicht allein auf die Investition, sondern auch auf andere Faktoren im Zusammenhang mit der Erstellung der Datenbank abgestellt. Ob die Investition daher als alleiniges

305 Kraus, in: Big Data, Tagungsband der Herbstakademie 2014, S. 381.

306 Hoeren, MMR 2013, 486 (487); Hilgendorf, JuS 1996, 890 (892).

307 Hoeren, MMR 2013, 486 (487); Hilgendorf, JuS 1996, 890 (893).

308 Dreier, in: Dreier/Schulze (Hrsg.), UrhG, 5. Aufl. 2015, § 87b Rn. 7; Koch, in: Ahlberg/Götting (Hrsg.), BeckOK UrhG, § 87b Rn. 13.

309 Specht/Rohmer, PinG 2016, 127 (131); siehe auch Ensthaler, NJW 2016, 3473 (3477).

310 Koch, in: Ahlberg/Götting (Hrsg.), BeckOK UrhG, § 87a Rn. 30; Erwägungsgrund 41 der Datenbank-RL; siehe dazu unter Kapitel 3.2.2.

Kriterium zur Bestimmung des Inhabers eines Rechts am Datum dienen kann, erscheint fraglich. In der folgenden Tabelle wird der Ansatz der Zuweisung nach der Investiti-

on in die Datenerzeugung auf die Fallstudien angewendet (Abbildung 25).

Fallstudie 1: Kfz-Instandhaltung und -Wartung	Zuordnung nach Investition
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen	Eigentümer des Kfz, falls Investition des Fahrzeugherstellers in Entwicklung und Produktion des Fahrzeugsystems vollständig mit Kaufpreis abgegolten
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller	Schwierig zu beurteilen im Falle laufender Dienstleistungen wie der hier beschriebenen Ferndiagnose; Eigentümer hat Fahrzeugsystem erworben und betreibt das Kfz, hingegen erbringt der Hersteller (eventuell auch im Eigeninteresse) die Auswertung der übertragenen Sensordaten und eventuell die Vorbereitung des Werkstattbesuchs
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten	[entspricht 1b]
Fallstudie 2: Carsharing	Zuordnung nach Investition
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters	Fraglich, ob kalkulierter Preis für Carsharing-Nutzung auch Kosten der Datenerstellung (bspw. Integration technischer Systeme ins Fahrzeug) abdeckt; im Falle der Bejahung Zuordnung zum Carsharing-Nutzer, ansonsten Zuordnung zum Carsharing-Anbieter
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters	Entweder Eigentümer des Kfz, falls Investition des Fahrzeugherstellers in Entwicklung und Produktion des Fahrzeugsystems vollständig mit Kaufpreis abgegolten oder Carsharing-Anbieter durch Investition in sein lokales System bzw. Carsharing-Nutzer bei Umlegung der Kosten durch den Carsharing-Anbieter
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter	[entspricht 2b]
Fallstudie 3: Mobilitätsdienstplattform	Zuordnung nach Investition
3a) Eingabe von Daten in die Mobilitätsdienstplattform und Transfer zum MDP-Anbieter	Entweder Eigentümer des Kfz (vorausgesetzt die Investition des Fahrzeugherstellers in Entwicklung und Produktion der Hardware der Mobilitätsdienstplattform ist vollständig durch den Kaufpreis abgegolten) oder MDP-Anbieter durch laufende Erbringung von Dienstleistungen
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstplattform und zum MDP-Anbieter	[entspricht 1b]
3c) Transfer von Daten aus der Mobilitätsdienstplattform zum Fahrzeugsystem	[entspricht 1b]
Fallstudie 4: Mobilitätsdienste	Zuordnung nach Investition
4a) Eingabe von Daten in den Mobilitätsdienst (App) und Transfer zum MD-Anbieter	Entweder Eigentümer des Kfz (vorausgesetzt die Investition des Fahrzeugherstellers in Entwicklung und Produktion der Hardware der Mobilitätsdienstplattform ist vollständig durch den Kaufpreis abgegolten) oder MD-Anbieter durch laufende Erbringung von Dienstleistungen oder Nutzer aufgrund des Aufwands der Eingabe der Daten

4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter	[entspricht 1b]
Fallstudie 5: Car-2-X-Kommunikation	Zuordnung nach Investition
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug	[entspricht 1a]
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber	Eigentümer des Fahrzeugs, falls Investition des Fahrzeugherstellers in Entwicklung und Produktion des Fahrzeugsystems vollständig mit Kaufpreis abgegolten oder Infrastrukturbetreiber durch Kosten für Anschaffung und Betrieb der RSU bzw. Kosten für Aufbereitung der Daten
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer	Eigentümer des Fahrzeugs, falls Investition des Fahrzeugherstellers in Entwicklung und Produktion des Fahrzeugsystems vollständig mit Kaufpreis abgegolten oder Empfänger durch Kosten für Anschaffung und Betrieb des technischen Empfängers
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte	[entspricht 5b]

Abbildung 25: Zuweisung nach der Investition in die Datenerzeugung (Anwendung auf die Fallstudien)

Die getätigte Investition in die Datenerzeugung als Zuweiskriterium entspricht dem Grundprinzip von Leistungsschutzrechten, wonach demjenigen der Wert eines Gutes zugewiesen wird, der für dessen Erzeugung in wirtschaftlicher Hinsicht verantwortlich ist. Diese Form der Zuweisung wirtschaftlicher Werte dürfte auch dem überwiegenden Rechtsempfinden in der Bevölkerung entsprechen und ist Laien plausibel zu transportieren. Daher ist dieser Ansatz grundsätzlich sachgerecht und aufgrund des Vorliegens irgendeiner „Leistung“ in Bezug auf dessen Entstehung auf nahezu jedes Datum anzuwenden. Die Koppelung von Investition mit der Verfügungsgewalt an Daten ist auch wirtschaftlich sinnvoll, da derart Investitionsanreize geschaffen werden. In der Praxis ist bei personenbezogenen Daten der wirtschaftlich Berechtigte (derjenige, der eine Investition vornimmt) identisch mit dem Akteur, der Anspruch auf Datenschutz hat (ohne dass dieser Personenbezug allein als „Leistung“ angesehen werden kann³¹¹). Dieser Ansatz ermöglicht einen fairen Ausgleich zwischen den beteiligten Akteuren, da eine monetäre Abfindung aller Beteiligten ermöglicht wird. So ist bspw. die Investitionstätigkeit durch den Hersteller schon im Vorfeld der Datenerstellung durch den Eigentümer des Kfz mittels des Kaufpreises abzugelten, wenn dieser die Datenverfügungsbefugnis erlangen möchte.

Dennoch kann die Investition nicht als alleiniges Kriterium zur Bestimmung des Inhabers eines Ausschließlichkeitsrechts an Daten dienen. Die Investitionstätigkeit ist ein sehr unbestimmtes Kriterium, das keine hinreichende Rechtssicherheit für die beteiligten Akteure bieten kann. Die getätigten Investitionsleistungen verteilen sich unter Umständen auf mehrere Akteure und das Gewicht der einzelnen Beiträge lässt sich häufig schwerlich ermitteln. Beispielsweise verkaufen Hersteller eventuell ihre Fahrzeuge günstiger, wenn der Käufer in die kontinuierliche Übermittlung von Sensordaten aus dem Fahrzeug einwilligt. In dieser Konstellation kann das Argument, die Entwicklung und Herstellung der Sensorik sei mit dem Kaufpreis abgegolten, nicht überzeugen, da der Hersteller die Daten als diesbezügliche monetäre Gegenleistung betrachtet. Ferner würde vollständig auf ein Publizitätsmoment verzichtet. Unter Umständen steht der hinter der Datenerzeugung stehende Investor – abgesehen von der wirtschaftlichen Beteiligung – in keiner Beziehung zu den betreffenden Daten und hat eventuell nicht einmal faktischen Zugang zu diesen. Daher wird auch vertreten, grundsätzlich das Prinzip des Investitionsschutzes allgemein auf Daten zu übertragen, den Datenersteller jedoch auch nach dem Skripturakt zu bestimmen³¹². Im Ergebnis erscheint das Abstellen auf die Investition allenfalls als eines von mehreren Kriterien zur Bestimmung des Datenberechtigten geeignet.

311 Siehe dazu Kapitel 5.1.4.1.

312 Specht/Rohmer, PinG 2016, 127 (131).

Abstellen auf den Skripturakt

Als weiterer handlungsbezogener Ansatz kommt die Zuweisung nach dem Skripturakt in Betracht. Die Zuordnung von Daten an einen Berechtigten wird im Bereich des Strafrechts grundsätzlich nach diesem durch die Rechtsprechung entwickelten und manifestierten Ansatz beurteilt, der darauf abstellt, wer die Speicherung der Daten initiiert hat³¹³. Welp prägte bereits 1988 wesentlich den Begriff des Skripturakts, den er als Akt der Datenerzeugung, also die Eingabe der zu speichernden oder zu übermittelnden Daten in eine Datenverarbeitungsanlage, definierte. Diese Eingabe könne unmittelbar über die Konsole eines Geräts, automatisch durch programmierte Funktionen des Rechners oder durch die selbsttätige Einspeisung anderweitig erzeugter Messwerte oder sonstiger Daten erfolgen³¹⁴. Dieser Begriff bezeichnet folglich die **technische Erstellung von Daten**. Daten entstehen durch Übersetzen von Bedeutung in Zeichen, also das Codieren semantischer Information als syntaktische Information³¹⁵. Skribent sei derjenige, der die Daten erzeugt, also ihre Speicherung oder Übermittlung selbst unmittelbar bewirkt hat.

Jedoch ist nach dieser Definition des Skribenten offen, ob eher auf die Speicherung oder Übermittlung abzustellen ist. Keinesfalls kann nach dieser abstrakten Definition in der Praxis bezogen auf einen konkreten Fall der Datenerzeuger zweifelsfrei bestimmt werden. In diesem Sinne stellt auch Zech fest, dass bei einem Recht an Daten *de lege ferenda* unklar sei, ob auf das einfache Abspeichern von Daten oder die darüber hinausgehende Erzeugung bzw. Schaffung durch Aufnahmen, Rechenvorgänge etc. abgestellt werden sollte³¹⁶.

Hoeren vertritt letztere Ansicht und definiert die Person des Datenerzeugers als denjenigen, der durch Eingabe oder Ausführung eines Programms Daten selbst erstellt³¹⁷. In diesem Zusammenhang problematisch ist jedoch, dass bei maschinengenerierten Daten die Programmautomatik in vielen Fällen zwar von Menschen generiert und in Gang ge-

setzt wurde, anschließend die Maschinen aber über längere Zeiträume automatisch Daten produzieren und eine dauerhafte menschliche Beherrschung nicht notwendig ist.

Von den Befürwortern eines Dateneigentums wird hinsichtlich dessen Zuordnung zu einem Berechtigten überwiegend auf den Skripturakt, als den Moment der Datenerzeugung abgestellt³¹⁸. Dieser Ansatz lässt jedoch die Frage unbeantwortet, wem der Skripturakt rechtlich zugerechnet werden soll, wer mithin als der „Datenerzeuger“ gilt. Daher wird vorgeschlagen die Person des Erstellers zwar vorrangig nach dem Skripturakt zu bestimmen, jedoch weitere wertende Kriterien ergänzend zur Betrachtung hinzuzuziehen³¹⁹. Hierbei seien **vorwiegend wirtschaftliche Faktoren**, wie das Zurverfügungstellen der notwendigen Produktionsmittel oder das Tragen des wirtschaftlich-organisatorischen Aufwands für die Datenerzeugung maßgeblich³²⁰. Nach anderer Ansicht sei streng auf die technische Urheberschaft abzustellen³²¹. Insbesondere im Rahmen von Auftragsverhältnissen gelangt man nach den verschiedenen Verständnissen zu unterschiedlichen Zuordnungsergebnissen. Innerhalb von Arbeits- oder Dienstverhältnissen, in denen Daten im Auftrag erstellt werden, solle nach einer Ansicht zunächst der Auftragnehmer bis zur Aushändigung der Daten Berechtigter sein. Zum einen sei bei dem Abstellen allein auf die technische Urheberschaft eine eindeutige Zuweisung gewährleistet und zum anderen solle § 303a StGB nicht zu einer weiten Kriminalisierung von Vertragsbrüchen führen³²². Nach anderer Ansicht sei im Rahmen von Auftragsverhältnissen aufgrund der Weisungsgebundenheit des Skribenten auf den Auftraggeber abzustellen³²³. So sei bezogen auf komplexe Maschinen nicht auf den jeweiligen Nutzer, sondern auf den wirtschaftlichen Betreiber, etwa den Halter eines Fahrzeugs, abzustellen. Dieser Sorge schließlich dafür, dass die Aufnahme- bzw. Messvorrichtung unterhalten sowie effizient eingesetzt werde und trage die erforderlichen Aufwendungen³²⁴. Nach Hoeren ist der Skripturakt dogmatisch und praktisch brauchbar, da er sich auf die spezifische Dateneigenschaft beziehe³²⁵.

313 BayObLG, Urt. v. 24. Juni 1993, Az. 5 St RR 5/93; siehe zum Skripturakt auch bereits unter 3.2.3.

314 Welp, iur 1988, 443 (447).

315 Zech, CR 2015, 137 (144).

316 Zech, CR 2015, 137 (144).

317 Hoeren, MMR 2013, 486 (487).

318 Zech, CR 2015, 137 (144); Hoeren, MMR 2013, 486 (487).

319 Specht, CR 2016, 288 (294); Zech, CR 2015, 137 (144).

320 Specht, CR 2016, 288 (294).

321 Hoeren, MMR 2013, 486 (487).

322 Hoeren, MMR 2013, 486 (487).

323 Welp, iur 1988, 443 (448); Lenckner/Winkelbauer, CR 1986, 824 (829); Hilgendorf, JR 1994, 478 (479); Zech, CR 2015, 137 (143 f.).

324 Zech, CR 2015, 137 (144).

325 Hoeren, MMR 2013, 486 (487).

Grundsätzlich ist ein Anknüpfen an die Erzeugung von Daten auch sachgerecht, insbesondere da dies einen klaren Anknüpfungspunkt bildet. Wird das Entstehen von Daten als der erste Schritt der Wertschöpfung verstanden, dann ist der Skribent aus ökonomischer Sicht grundsätzlich ein interessanter Akteur mit Verfügungsgewalt. Der Personenbezug ist hier abgesehen von daraus folgenden Beschränkungen des Dateninhabers in der Nutzung seines Datums durch das Datenschutzrecht gänzlich unbeachtlich.

Problematisch an einer ausschließlich technischen Betrachtungsweise, die auf die Codierung bzw. Erstabspeicherung von Daten abstellt, ist indes, dass sie keine zweifelsfreie Bestimmung der Person des Erstellers gewährt. Zudem dürfte die technische Betrachtungsweise aus ökonomischer Sicht zu „fehlerhaften“ Ergebnissen führen, da der technische Ersteller nicht immer wirtschaftlich für die Datenerstellung verantwortlich ist und deren Kosten trägt. Der Skripturakt bezieht sich zu stark auf die technischen Aspekte der Datenerzeugung und zu wenig auf den menschlichen Einfluss, um einen Verfügungsberechtigten ermitteln zu können. Selbst bei ausschließlich technischer Betrachtung ist es bei maschinengenerierten Daten schwierig, einer Person die Verantwortlichkeit für den Schaffensprozess von Daten zuzuweisen. An der Datenerzeugung können auch mehrere Personen wesentlichen Anteil geleistet haben. Im Falle der Datengenerierung im Kfz kommen bspw. sowohl Eigentümer und Nutzer des Fahrzeugs als auch der Hersteller der Sensorik/Software bzw. der Anbieter von Mobilitätsdiensten und Mobilitätsdienstplattformen in Betracht. *Specht* schlägt daher eine güterrechtliche Mitinhaberschaft bezüglich des entstehenden Rechts in Anlehnung an die datenschutzrechtliche Mitverantwortlichkeit nach Art. 26 DSGVO bzw. entsprechend der Miturheberschaft nach § 8 UrhG vor³²⁶.

Zusammenfassend betrachtet erscheint der Ansatz des Skripturaktes am überzeugendsten. Er wirkt jedoch noch nicht ausgereift und bedarf daher der Weiterentwicklung. So muss zwischen den unterschiedlichen Datenarten unterschieden werden und sich genau ermitteln lassen, wer für den jeweiligen Skripturakt die Verantwortung trägt³²⁷. Zum Teil wird eine Weiterentwicklung dahingehend vorgeschlagen, dass auf die **wirtschaftliche Verantwortlichkeit hinsichtlich der Datenerzeugung** abzustellen sei³²⁸. Uneinigkeit herrscht jedoch darüber, welche wirtschaftlichen Gesichtspunkte konkret angewendet werden sollten. Während *Specht* darauf abstellt, wer die Produktionsmittel zur Verfügung gestellt habe³²⁹, ist *Zech* der Ansicht, es solle allgemein auf die wirtschaftliche Erzeugung von Daten abgestellt werden. Bei komplexen Maschinen wäre der Datenerzeuger regelmäßig der wirtschaftliche Betreiber, bspw. der Halter eines Fahrzeugs oder der Unternehmensinhaber, der Produktionsmaschinen einsetzt³³⁰. Nach erstgenannter Präzisierung ergeben sich Überschneidungen zu dem Ansatz, Dateneigentum nach dem Eigentum am datengenerierenden Gegenstand zuzuordnen. Bei der wirtschaftlichen Verantwortlichkeit nach *Zech* hingegen werden Gedanken des Ansatzes, der auf die Investition in die Datenerzeugung abstellt, übertragen.

Dem Ansatz des Skripturaktes ist daher nur in der weiterentwickelten Variante zuzustimmen. Als alleiniges Kriterium vermag dieser Ansatz nicht zu überzeugen. Es bietet sich jedoch an, den Skripturakt mit dem Ansatz der Zuweisung nach dem Investitionsakt zu verbinden. Im Rahmen einer Weiterentwicklung erscheint der Oberbegriff des Ansatzes allerdings nicht passend, da der Begriff Skripturakt ein sehr technischer ist und allein die Codierung von Daten bezeichnet.

In der nachfolgenden Tabelle werden die vorgestellten Ansätze zur Ermittlung des Datenberechtigten zusammengefasst:

326 *Specht*, CR 2016, 288 (295).

327 *Boesche/Rataj*, Zivil- und datenschutzrechtliche Zuordnung von Daten vernetzter Kraftfahrzeuge, abrufbar unter: http://schaufenster-elektromobilitaet.org/media/media/documents/dokumente_der_begleit_und_wirkungsforschung/EP21_Zivil-_und_datenschutzrechtliche_Zuordnung.pdf, S. 43.

328 *Zech*, CR 2015, 137 (144).

329 *Specht*, CR 2016, 288 (294).

330 *Zech*, CR 2015, 137 (144).

Ansatz	Rechtliche Bewertung	Ökonomische Bewertung
Personenbezug	Keine Zuordnung von nicht personenbezogenen Daten; Datenschutzrecht hat primär immaterielle Schutzgüter zum Gegenstand; keine ausreichende Eigenleistung der Betroffenen im Rahmen der Datenerstellung; zur Stärkung der Betroffenenrechte nicht notwendig, da andere Mechanismen denkbar; Kriterium des Personenbezugs teilweise uneindeutig	Bei einem einheitlichen Akt der „Datenerzeugung“ gibt es ggf. eine unterschiedliche Zuordnung der Verfügungsgewalt zu Akteuren in Abhängigkeit davon, welche Daten personenbezogen sind. Da Daten oft in Kombination von personen- und nichtpersonenbezogenen Daten entstehen und werthaltig sind, erschwert dies die wirtschaftliche Nutzung.
Gegenstand	Vorteil einer eindeutigen Zuordnung (Rechtssicherheit); Ansatz betrifft allerdings nicht alle Datenkategorien; Eigentum als formale Rechtsposition als Zuordnungskriterium nicht in allen Fällen interessengerecht und führt teilweise zu zufälliger Zuordnung; Eigentum am Gegenstand und Eigentum am Datum sind getrennt zu betrachten; Regelungen zu zivilrechtlichem Eigentum lassen sich mangels Körperlichkeit von Daten schwerlich übertragen	Rechtliche Eindeutigkeit sorgt grundsätzlich für geringe Transaktionskosten. Im Fall personenbezogener Daten wäre allerdings in einigen Szenarien zusätzlicher Aushandlungsaufwand notwendig, was die Transaktionskosten erhöht.
Speichermedium	Unterschiedliche Zuordnung von Inhalt und Trägermedium anerkannt; Vorteil einer eindeutigen primären Zuordnung (Rechtssicherheit); fraglich bei Datentransfers und erneuten Speichervorgängen	In gewissen operativen Leistungsmodellen (z. B. Cloud Computing oder Leasingmodellen für IT-Infrastruktur) fallen Datennutzer und Eigentümer des Datenmediums auseinander. Damit wäre die Verfügungsgewalt in der Hand eines Akteurs, der gerade nicht das spezifische wirtschaftliche Interesse an den Daten hat.
Investition	Investitionsschutz als Grundgedanke des Urheberrechts und diverser Leistungsschutzrechte; Investition als einziges Kriterium jedoch zu unbestimmt; mangels eindeutiger Erkennbarkeit des Investors keine Rechtssicherheit im Rechtsverkehr	Kopplung von Investition bzw. wirtschaftlicher Berechtigung mit Verfügungsgewalt ist sinnvoll, da so Investitionsanreize geschaffen werden.
Skripturakt	Anerkannt im Strafrecht (Einheit der Rechtsordnung); Nachteil der praktisch schwierigen Bestimmung der Person des Skribenten	Wird das Entstehen von Daten als der erste Schritt von Wertschöpfung verstanden, dann ist der Skribent aus ökonomischer Sicht grundsätzlich ein interessanter Akteur mit Verfügungsgewalt. Problematisch ist, dass der Skribent nicht immer einfach eindeutig zu identifizieren ist.

Abbildung 26: Rechtliche und ökonomische Bewertung der Zuordnungsansätze

5.1.2.4 Abschließende Bewertung: Zuordnung zum wirtschaftlich Berechtigten als überzeugendste Handlungsoption

Die Argumente, die für und gegen die genannten Zuordnungsansätze sprechen, zeigen, dass derzeit **kein Ansatz vollständig überzeugen kann**, aber zahlreiche erwägenswerte Indizien für eine sachgerechte Zuordnung benannt werden. Daher erscheint eine **Weiterentwicklung** einzelner Ansätze bzw. eine Kombination von Elementen verschiedener Ansätze zielführend und vor allem in Übereinstimmung mit den Ergebnissen der ökonomischen Analyse

geeignet, den wirtschaftlich Berechtigten am konkreten Datum in den Mittelpunkt zu rücken.

Im Vordergrund eines etwaigen, zu entwickelnden, eigentumsähnlichen Rechts an Daten stehen hinsichtlich der Zuordnungsentscheidung daher die handlungsbezogenen Ansätze, da demjenigen die Verwertung gebühren sollte, der die Daten geschaffen hat³³¹. Während der Ansatz nach der geistigen Schöpfung nicht praktikabel ist, sind der Investitionsschutzgedanke und die Bestimmung des Datenerzeugers mittels Abstellen auf den Skripturakt die wesentlichen Grundpfeiler zur Ermittlung des Berechtigten (Abbildung 27).

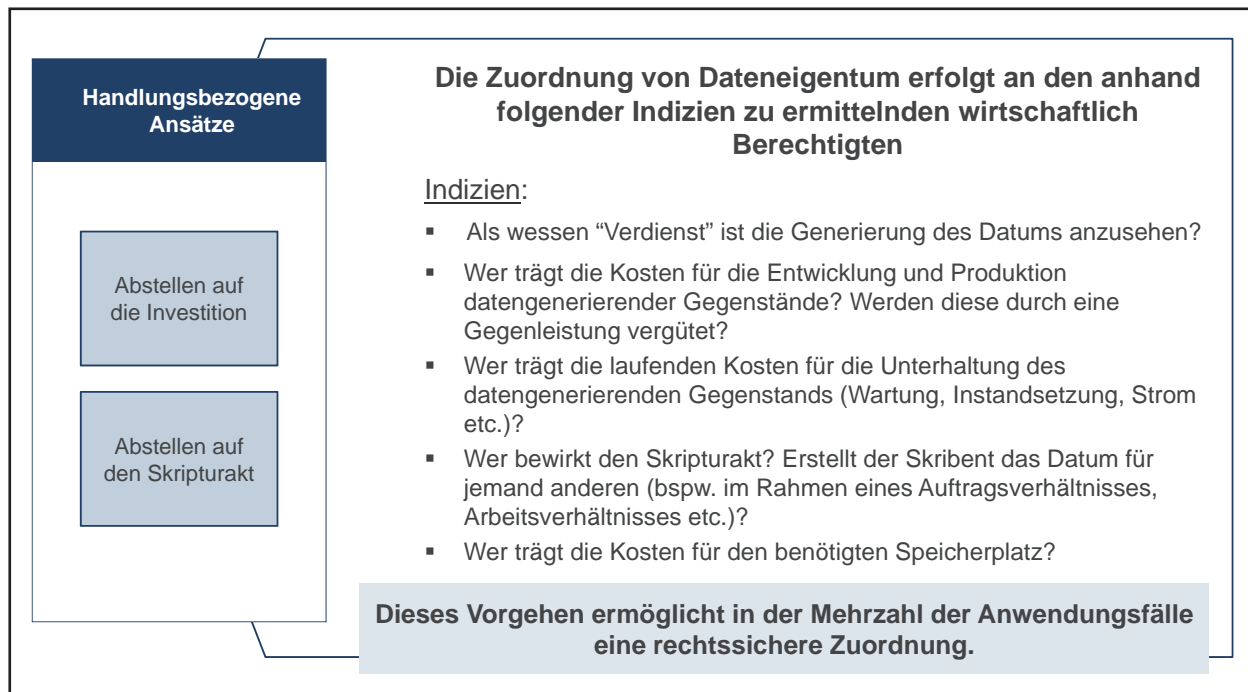


Abbildung 27: Indizien zur Ermittlung des Dateneigentümers gemäß des entwickelten Zuordnungsansatzes

331 Für eine ausführliche Bewertung der Zuordnungsansätze siehe Kapitel 5.1.2.3.

Eine Zuordnung zum **wirtschaftlich verantwortlichen Datenerzeuger** erfüllt alle an einen Zuweisungsmechanismus zu stellenden Anforderungen. Er weist ein in der Wirtschaft als wertvoll bewertetes Gut demjenigen zu, der erheblichen Anteil an der Schaffung desselben hat und rechtfertigt somit die dem Inhaber des Rechts zustehenden Befugnisse gegenüber jedermann. Dieser Ansatz ist eng angelehnt an den von Zech³³² entwickelten Ansatz, unterscheidet sich jedoch in der Bestimmung der Person des Datenerzeugers. Während Zech den Datenerzeuger als denjenigen definiert, der wirtschaftlich die Erzeugung veranlasst und bei maschinengenerierten Daten ausschließlich auf die wirtschaftliche Betreiberschaft abstellt³³³, soll hier eine differenziertere Betrachtungsweise eingenommen und mehrere Kriterien der verschiedenen Ansätze in Einklang gebracht werden.

Folgende **Indizien** dienen der Bestimmung des wirtschaftlichen Datenerzeugers:

- Als wessen Verdienst ist die Generierung eines Datums anzusehen?
- Wer bewirkt den Skripturakt? Erstellt der Skribent das Datum für jemand anderen (bspw. im Rahmen eines Arbeitsverhältnisses, Auftragsverhältnisses, etc.)?
- In Bezug auf maschinengenerierte Daten ist zu ermitteln, wer die Entwicklungs- und Produktionskosten trägt und ob diese gegebenenfalls im Rahmen der Anschaffung durch Dritte mittels einer Gegenleistung vergütet werden.
- Ebenfalls in Bezug auf den datengenerierenden Gegenstand ist zu ermitteln, wer die laufenden Kosten für die Unterhaltung des datengenerierenden Gegenstands trägt (Wartung, Instandsetzung, etc.).
- Wer trägt die Kosten für den benötigten Speicherplatz?

Hierbei stellt der Begriff „Datenerzeuger“ einen Rechtsbegriff dar, der je nach gewählten Kriterien und deren Rangverhältnis auf mehrere Arten auszulegen ist – er enthält nicht nur einen Bedeutungsinhalt, sondern mehrere. Dadurch ist in der Praxis die Möglichkeit einer im Einzelfall passenden Lösung und einer Weiterentwicklung und Anpassung durch die Rechtsprechung gegeben. Das Gesetz trifft keine eindeutige Aussage, sondern überlässt es den

mit dem Normvollzug betrauten Stellen und Personen, in Zweifelsfällen die konkrete Anwendung im Einzelfall vorzunehmen. In der Mehrzahl der Fälle wird sich der wirtschaftliche Datenersteller unter Zugrundelegung der genannten Kriterien jedoch zweifelsfrei bestimmen lassen. Bei Beherrschung des Datenerstellungsvorgangs durch mehr als einen Akteur bspw. im Falle von Miteigentum an dem datengenerierenden Gegenstand ließe sich eine güterrechtliche Mitinhaberschaft zugunsten mehrerer Rechtssubjekte bezüglich des Rechts am Datum normieren³³⁴.

Zusammenfassend lässt sich feststellen, dass die diversen Ansätze zur Bestimmung des „Datenerzeugers“ miteinander zu kombinieren sind, um eine im Einzelfall interessengerechte und flexible Bestimmung des Rechtsinhabers zu ermöglichen. Dennoch müssen die Kriterien derart bestimmt sein, dass keine Rechtsunsicherheit besteht. Die Praktikabilität des Ansatzes und seine grundsätzliche Eignung sollen nachfolgend einerseits durch die Anwendung auf die Fallstudien, andererseits durch die exemplarische Überführung in einen Normtext überprüft werden.

5.1.2.4.1 Anwendung des kombinierten Ansatzes auf die Fallstudien

Der Ansatz, demjenigen ein Ausschließlichkeitsrecht an einem Datum zuzuweisen, als dessen **Verdienst** die Generierung desselben anzusehen ist, ermöglicht in der Praxis flexible und sachgerechte Ergebnisse. Bezogen auf Daten, die im vernetzten Automobil autonom erzeugt und gespeichert werden, ist regelmäßig der Eigentümer des betreffenden Fahrzeugs der Verfügungsberechtigte.

Bei Daten, die durch die Sensorik im Fahrzeug erstellt werden, ist nach wirtschaftlicher Betrachtungsweise die Anschaffung des datengenerierenden Gegenstands (des Fahrzeugs) sowie die wirtschaftliche Unterhaltung desselben für die Datenerstellung maßgeblich. Bezogen auf das *Carsharing* gebühren die erstellten Daten daher eindeutig dem *Carsharing*-Anbieter, da dieser das Fahrzeug angeschafft und in die lokalen Systeme zur Generierung und Speicherung von Daten investiert hat. Die jeweilige konkrete Nutzung tritt demgegenüber zurück, da die Datenerzeugung lediglich als Nebenprodukt derselben anzusehen ist. Die Investition in die datengenerierende Technik durch den Hersteller des Fahrzeugs ist regelmäßig mit der Zahlung des Kaufpreises durch den Eigentümer abgegolten. Ein anderes Ergebnis ergibt sich bei Mobilitätsdiensten, wenn auf Basis

³³² Zech, CR 2015, 137 (144 ff.).

³³³ Zech, CR 2015, 137 (144).

³³⁴ So auch Specht, CR 2016, 288 (295).

der durch das Fahrzeug erzeugten Daten als Dienstleistung des Mobilitätsdienst-Anbieters neue Daten bspw. mittels automatisierter Datenanalyse generiert werden – diese sind dem Mobilitätsdienst-Anbieter nach wirtschaftlicher Betrachtungsweise zuzuordnen. Noch eine andere Zuordnung gilt in Fällen, in denen ein Mobilitätsdienst-Nutzer Daten preisgibt und diese in ein System eingibt – die Erstellung des Datums ist dann alleiniger Verdienst des Nutzers.

Ein Fall von besonderem Interesse ergibt sich bei der Car-2-X-Kommunikation und der Frage der Nutzung der Daten nach Empfang *mittels Roadside-Units* durch Infrastrukturbetreiber und die öffentliche Hand. In der im Fall der Car-2-X-Kommunikation stattfindenden periodischen Aussendung von Daten kann die automatische Einwilligung in die Nutzung durch den Rechtsinhaber zu sehen sein. Obwohl diese Übermittlung durch den Dateninhaber nichts an der primären Zuweisungsentscheidung ändert, berechtigt

sie den Empfänger aufgrund ausdrücklichen oder konkludenten Einverständnisses zur Nutzung. Es könnte sich sozusagen um die Erteilung einer einfachen Nutzungslizenz an einen unbestimmten Personenkreis handeln. Jeder, der über die technischen Möglichkeiten des Auslesens der periodisch ausgesendeten Daten verfügt, ist dann zu deren Nutzung berechtigt. Somit ist die Nutzung der Daten im Allgemeininteresse durch den Infrastrukturbetreiber bzw. den Staat – unabhängig von der originären Zuordnung zum Eigentümer des Fahrzeugs – sichergestellt.

Es lässt sich nach dem hier vorgeschlagenen Ansatz bezogen auf alle Fallstudien ein konkreter Dateninhaber bestimmen, dessen Berechtigung ferner sach- und interessen-gerecht ist. Im Folgenden wird nochmal zusammenfassend eine tabellarische Zuweisung nach dem vorgestellten kombinierten Ansatz bezogen auf die Fallstudien vorgenommen (Abbildung 28):

Fallstudie 1: Kfz-Instandhaltung und -Wartung	Zuordnung an den wirtschaftlich berechtigten Datenersteller
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen	Eigentümer des Kfz, da Aufwand des jeweiligen Fahrers bei maschinengenerierten Daten zu vernachlässigen und Investition des Herstellers typischerweise mit Kaufpreis abgegolten
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller	Entspricht 1a
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten	Entspricht 1a
Fallstudie 2: Carsharing	Zuordnung an den wirtschaftlich berechtigten Datenersteller
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters	Carsharing-Anbieter
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters	Entspricht 1a
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter	Entspricht 2a
Fallstudie 3: Mobilitätsdienstplattform	Zuordnung an den wirtschaftlich berechtigten Datenersteller
3a) Eingabe von Daten in die Mobilitätsdienstplattform und Transfer zum MDP-Anbieter	Nutzer, da er durch die Eingabe die unmittelbare datengenerierende Handlung vornimmt
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstplattform und zum MDP-Anbieter	Entspricht 1a
3c) Transfer von Daten aus der Mobilitätsdienstplattform zum Fahrzeugsystem	Entspricht 1a

Fallstudie 4: Mobilitätsdienste	Zuordnung an den wirtschaftlich berechtigten Datenersteller
4a) Eingabe von Daten in den Mobilitätsdienst (App) und Transfer zum MD-Anbieter	Entspricht 3a
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter	Entspricht 1a
Fallstudie 5: Car-2-X-Kommunikation	Zuordnung an den wirtschaftlich berechtigten Datenersteller
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug	Eigentümer des Kfz (Nutzungsberechtigte sind auf Basis des konkludenten Einverständnisses des originär Verfügungsberechtigten jedoch der Infrastrukturbetreiber bzw. der Staat)
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber	Entspricht 5a
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer	Entspricht 5a
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte	Entspricht 5a

Abbildung 28: Anwendung des kombinierten Ansatzes auf die Fallstudie

5.1.2.4.2 Überführung des neuentwickelten Ansatzes in einen Normtext

Abschließend kann die Praktikabilität des formulierten Zuordnungsansatzes daran exemplifiziert werden, ob es gelingt, diesen in einen Normtext zu überführen. In diesem Kontext ist darauf hinzuweisen, dass nachfolgende Formulierungen nur der Veranschaulichung dienen – als Element einer bereichsspezifischen Regelung, die eine Zuordnung erfordert oder als Ausgangspunkt eines übergreifenden Ausschließlichkeitsrechts wären zahlreiche Kon-

kretisierungen und Anpassungen an die Ausgestaltung im jeweiligen Gesetz vorzunehmen. Neben der eigentlichen Zuordnungsnorm kommt auch den Begriffsbestimmungen erhebliche Relevanz zu; gerade diesbezüglich ist auf eine Kohärenz mit anderen Regelungsmaterien zu achten, die bspw. schon heute auf dem Begriff der Daten aufbauen.

Der vorgeschlagene Entwurf besteht aus **zwei Vorschriften**, aufgeteilt in **Begriffsdefinitionen** und in die Bestimmung des **Verfügungsberechtigten** an den Daten.

Normtext: Begriffsdefinitionen	Erläuterungen des Entwurf
(1) Daten sind beobachtbare Unterschiede, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.	Um die Einheitlichkeit der Rechtsordnung sicher zu stellen, wurde die Begriffsdefinition von Daten zum Teil aus § 202a StGB übernommen, kombiniert mit einer Definition aus dem Bereich der Informatik.
(2) Erstellen ist das erstmalige technische Erzeugen von Daten. Die Replikation von Daten ohne Veränderung ist kein Erstellen in diesem Sinne. Ein Erstellen liegt auch in der Verarbeitung von Daten, dem Zusammenführen von Daten und ähnlichen Handlungen, soweit dieser Vorgang zu einem von den verwendeten Ausgangsdaten abweichendem Datum führt.	Der Begriff des Erstellens soll klarstellen, wann Daten erstmals im technischen Sinne entstehen. Mit Abs. 2 S. 3 wurde zudem ein Satz aufgenommen, der klarstellen soll, wann ein neues Datum und damit ein neuer Lebenszyklus von Daten beginnt. Dies ist jedenfalls dann der Fall, wenn der Vorgang zu einem von den verwendeten Ausgangsdaten abweichendem Datum führt.
(3) Speichern ist das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.	Der Begriff des Speicherns stammt aus dem BDSG (dort § 3 Abs. 4 Nr. 1).
(4) Datengenerierender Gegenstand ist der Gegenstand, der die Daten erstellt. Die Speicherung der Daten muss dabei nicht zwingend auf dem datengenerierenden Gegenstand erfolgen.	Die Begriffsdefinitionen des datengenerierenden Gegenstands, wesentliche Investition und datengenerierende Handlung sind erforderlich, da sie in der Verfügungsberechtigung vorausgesetzt werden. Als datengenerierender Gegenstand kann bspw. ein informationstechnisches System angesehen werden. Eine klassische Investition ist der Erwerb eines Gegenstandes. Aber auch die Entwicklung eines Produktes kann eine Investition darstellen. Eine datengenerierende Handlung ist bspw. das klassische Bedienen eines informationstechnischen Gerätes, kann aber bspw. auch lediglich das Steuern eines Fahrzeuges sein, soweit dadurch die Datengenerierung ausgelöst wird.
(5) Eine Investition in die Datenerstellung ist die Schaffung von Voraussetzungen für die Erstellung und Speicherung von Daten durch Einsatz von Kapital.	
(6) Datengenerierende Handlung ist der Akt, der die unmittelbare Erstellung und Speicherung der Daten auslöst. Er kann sowohl in menschlicher Aktivität als auch in einem autonomen, maschinengesteuerten Vorgang liegen. Bei maschinengesteuerten datengenerierenden Handlungen ist auf die Initiierung des automatisierten Vorgangs abzustellen.	
Normtext: Bestimmung des Verfügungsberechtigten	Erläuterungen des Entwurf
Verfügungsberechtigter der Daten ist, wer bei wirtschaftlicher Betrachtungsweise für die Erstellung und Speicherung des Datums verantwortlich ist. Dies ist derjenige, der bei einer wirtschaftlichen Gesamtwürdigung des Erstellungsvorgangs die wesentliche Investition in die Datenerstellung vornimmt. Von einer wesentlichen Investition kann in der Regel ausgegangen werden, wenn eine unmittelbare Investition in die Datenerstellung vorgenommen wird, die Investition für den Vorgang der Datenerstellung von entscheidender Bedeutung ist und die getätigte Investition nicht schon anderweitig kompensiert worden ist. Indizien für eine Investition in diesem Sinne sind die wirtschaftliche Unterhaltung des datengenerierenden Gegenstandes, die Vornahme oder Initiierung der datengenerierenden Handlung sowie das Sacheigentum am datengenerierenden oder datenspeichernden Gegenstand.	Wie zuvor erläutert, wird der Verfügungsberechtigte der Daten anhand seines Anteils an der Schaffung des Datums (handlungsbezogen) nach einer wirtschaftlichen Betrachtungsweise bestimmt. Dieser Ansatz ermöglicht eine hinreichend offene Formulierung, so dass im Einzelfall unter Zugrundelegung der zusätzlich genannten Indizien eine sachgerechte Zuordnung zum wirtschaftlich Verantwortlichen erfolgen kann.

Abbildung 29: Übertragbarkeit des Zuordnungsansatzes in einen Normtext

Wie die Anwendung des formulierten Ansatzes auf die Fallstudien gezeigt hat, führt die gewählte Formulierung bei nahezu allen Fällen zu eindeutigen Ergebnissen, bspw. weil alle genannten Indizien auf denselben Akteur hindeuten. In den Fällen, in denen die Indizien dagegen widersprüchlich sind (bspw. bei Cloud-Lösungen, bei denen die wirtschaftliche Unterhaltung und das Eigentum am Speichermedium gegen die Vornahme und Initiierung der datengenerierenden Handlung streiten), ermöglicht der Ansatz dennoch genügend Spielraum, um eine anlassbezogene Gewichtung vorzunehmen.

5.1.3 Gründe für und gegen ein Ausschließlichkeitsrecht an Daten

Trotz des vorgestellten denkbaren Ansatzes für eine Zuordnung von Dateneigentum, die den ökonomischen Anforderungen gerecht wird und rechtlich handhabbar sein könnte, kann derzeit – und auf Basis der Ergebnisse dieser Studie – nicht abschließend bewertet werden, ob es sich empfiehlt, ein Ausschließlichkeitsrecht zu normieren. Nicht von der Hand zu weisen ist insoweit, dass einige **Gründe gegen die Schaffung eines derartigen Ausschließlichkeitsrechts** an Daten sprechen:

So könnte zunächst eingewendet werden, dass in Daten verkörperte Informationen frei von exklusiven rechtlichen Zuordnungen bleiben müssten³³⁵. Ein Umgang mit Information könne nicht exklusiv bei einzelnen Personen liegen – insoweit müsse sichergestellt sein, dass die Allgemeinheit zu gewissen sozialadäquaten Nutzungen von Daten im Allgemeininteresse berechtigt sei.

Diesbezüglich ist festzuhalten, dass mit dem Eigentum zwar Rechte verbunden sind, diese jedoch – schon wegen der Sozialbindung des Eigentums (Art. 14 Abs. 2 GG) – nicht zwingend exklusiver Natur sein müssen³³⁶. Insoweit ließe sich die starke Rechtsposition des Eigentümers zugunsten der Allgemeinheit beschränken, wie dies in der Studie zugrundeliegenden Differenzierung der Betrachtungsebenen (2. Ebene als „Belastung“ des Dateneigentums) angelegt ist³³⁷. So ist auch bei der Schaffung des Urheberrechts verfahren worden; im Urhebergesetz existieren zahlreiche Schrankenbestimmungen (vgl. etwa §§ 44a ff. UrhG).

Jedoch ist weiter zu bedenken, dass die Formulierung eines Ausschließlichkeitsrechts auf **nationaler Ebene** möglicher-

weise **wenig zielführend** wäre. Vielmehr erscheint eine Einpassung in den europäischen Rechtsrahmen erforderlich. Insoweit wäre zum einen weiter auszuloten, ob auf europäischer Ebene ein Erfordernis der Regelung gesehen wird und zum anderen, in welchem Rechtsrahmen die Materie integriert werden könnte³³⁸. Die Regelung einer allgemeinen Verfügungsbefugnis an Daten stünde unabhängig neben datenschutzrechtlichen Vorschriften und wäre losgelöst von der DSGVO, die ausschließlich dem Schutz der Persönlichkeit der von Datenverarbeitung Betroffenen dient.

Hinzu kommt, dass zahlreiche **Abhängigkeiten** zu den bereichsspezifischen Rechtsgebieten existieren. Um Wertungswidersprüche zu vermeiden, müsste die (gesetzliche) Zuordnungsentscheidung daher in Einklang mit den verschiedenen Rechtsgebieten gebracht werden. Die Auswirkungen auf die anderen Rechtsgebiete und die erforderlichen Folgeregelungen sind dabei vor allem von der jeweiligen konkreten Ausgestaltung abhängig.

Zudem besteht die Gefahr, dass durch die Schaffung eines Ausschließlichkeitsrechts ein **unscharfes Recht entsteht**, welches möglicherweise weiteren Innovationen und Geschäftsmodellen – auch über den Automobilbereich hinaus – im Wege stehen könnte, anstatt das Ziel einer erhöhten Rechtsicherheit zu erreichen. Dies gilt umso mehr, als dass sich der Technologiesektor sehr schnell verändert und daher die Möglichkeit besteht, dass eine rechtliche Erfassung des Dateneigentums innerhalb kurzer Zeit angepasst werden müsste.

Schließlich ist stets zu bedenken, dass das Ausschließlichkeitsrecht zum Schutz von Persönlichkeitsrechten zwingend durch ein umfassendes **Schrankensystem** zu begrenzen wäre (2. Ebene). Insbesondere das Datenschutzrecht beansprucht bei personenbezogenen Daten stets Geltung und würde als Schranke des Ausschließlichkeitsrechts fungieren. Das Ausschließlichkeitsrecht wäre daher mit zahlreichen „Belastungen“ behaftet³³⁹.

Nicht zu verkennen ist auf der anderen Seite jedoch, dass weitere gute Argumente für die Einführung eines gesetzlichen Ausschließlichkeitsrechts an Daten sprechen. Ein wesentlicher Grund ist zunächst, dass eine durch das Ausschließlichkeitsrecht vermittelte **umfassende Ausschluss- und Nutzungsfunktion (erga omnes)** im Gegensatz zur

335 Dorner, CR 2014, 617 (622, 626); Hoeren, GRUR 1997, 866 (867); Druery, Information als Gegenstand des Rechts, 1995.

336 Hornung/Goebel, CR 2015, 265 (273).

337 Dazu bereits unter 3.

338 Thematisch könnte dies bspw. in die Datenschutz-Grundverordnung integriert werden (etwa in Kapitel III „Rechte der Betroffenen“).

339 Siehe dazu bereits unter 3.; sowie Handlungsempfehlung 7.6.2.

relativen Wirkung derzeitiger vertraglicher Regelungen gegenüber jedermann wirkt und eine derartige Zuweisung als Ausgangslage vertraglicher Absprachen mehr Rechtssicherheit verspricht³⁴⁰.

Zudem wurde gezeigt, dass derzeit vor allem die faktische Zugriffsmöglichkeit auf die Daten über die Einräumung von Rechten entscheidet³⁴¹. Ein umfassendes Ausschließlichkeitsrecht verspricht hier für **mehr Ausgewogenheit** der Akteure zu sorgen.

Wie noch zu zeigen sein wird, bestehen darüber hinaus in gewissen Situationen **Lücken** in Bezug auf den deliktischen Schutz von Daten, die auch durch ein bloßes Ausschließlichkeitsrecht nicht geschlossen werden können, sondern andere Maßnahmen erfordern³⁴². Es gilt daher im Folgenden zu prüfen, ob sich die mit dem Dateneigentum verbundenen Eigenschaften nicht auch durch andere Maßnahmen erreichen ließen.

5.2 Handlungsalternativen

Neben der Schaffung eines umfassenden Ausschließlichkeitsrechts existieren **weitere Möglichkeiten**, wie die derzeitige gesetzliche Ausgestaltung mit der Zielsetzung angepasst werden könnte, einige Vorteile eines Dateneigentums zu realisieren ohne aber ein vollumfassendes Ausschließlichkeitsrecht zu schaffen. Zu fragen ist, ob ein Markt für (Mobilitäts-)Daten und eine ökonomisch begründbare Datensouveränität auch unterhalb eines Eigentumsrechts realisiert werden können und ob es Handlungsinstrumente gibt, die eine verbesserte Wertschöpfung in diesem Bereich sichern können. Ausgewählte Varianten sollen nachfolgend näher betrachtet werden, ohne dabei einen Anspruch auf Vollständigkeit zu erheben. Zudem sind die dargestellten Handlungsalternativen nicht in der Weise zu verstehen, dass diese zwingend anstatt einem Ausschließlichkeitsrecht an Daten umgesetzt werden können. Vielmehr ergänzen einige Alternativen das denkbare Ausschließlichkeitsrecht oder können zum Teil auch unabhängig davon umgesetzt werden. Auf Basis dieser Darstellung werden abschließend im 7. Kapitel konkrete Handlungsempfehlungen gegeben.

5.2.1 Vollständiger Verzicht auf gesetzliche Änderungen

Die erste denkbare Alternative zur Schaffung eines umfangreichen Ausschließlichkeitsrechts an Daten könnte der vollständige Verzicht auf gesetzliche Änderungen sein.

Als Argument könnte insoweit angeführt werden, dass der Markt auch bei derzeitiger Rechtslage in gewisser Weise als funktionsfähig anzusehen ist. Zudem entginge man so der Gefahr, dass ein möglicherweise konturenloses Ausschließlichkeitsrecht an Daten entstünde, welches im schlechtesten Fall innovative Geschäftsmodelle durch Zuordnung der Daten zu bestimmten Akteuren eher verhindern als fördern könnte. Zudem verbliebe es bei der bestehenden Flexibilität, da die beteiligten Akteure sämtliche Inhalte vertraglich ausgestalten können. Auch die Gefahr, durch eine weitere Zuordnungsentscheidung die schon derzeit inkonsistente Situation weiter auszudifferenzieren (vgl. Abbildung 16), wäre begrenzt.

Gegen das Unterlassen sämtlicher gesetzlicher Anpassungen spricht indes, dass die dargestellte bereichsspezifische und vor allem lückenhafte Zuordnung von Daten auch weiterhin bestehen bliebe. Zudem führt die beschriebene Vertragsfreiheit dazu, dass weniger starke Marktteilnehmer den vertraglichen Vorgaben stärkerer Akteure „ausgeliefert“ sind. Wie gezeigt, entscheidet derzeit vor allem die faktische/technische Zugriffsmöglichkeit auf die Daten darüber, wer die Vertragsbedingungen vorgeben kann, ohne dass dies immer den berechtigten Interessen der Beteiligten entspricht³⁴³. Eine angemessene Gewinnallokation zwischen allen Marktteilnehmern ist in der momentanen monopolistischen Marktstruktur, in der häufig sektorfremde Unternehmen die Rendite besonders profitabler Wertschöpfungsschritte abschöpfen, schwierig herzustellen. Langfristig ist zu befürchten, dass der fehlende Interessenausgleich und steigende Bedenken über den Schutz von Privatheit, die Bereitschaft der Nutzer zur Datenfreigabe beeinträchtigen, was auch aus wirtschaftlicher Sicht bedenklich ist. Der vollständige Verzicht auf gesetzliche Änderungen erscheint vor diesem Hintergrund daher nicht empfehlenswert.

340 *Ensthaler*, NJW 2016, 3473 (3474).

341 Siehe dazu Kapitel 3.3.

342 Siehe dazu Kapitel 5.2.5.

343 Siehe dazu Kapitel 3.3.

5.2.2 Bereichsspezifische Anpassungen, insbesondere Schaffung eines effektiven Vertragskontrollrechts

Insbesondere aufgrund dieser aus der faktischen Situation folgenden „Gefahren“ ist es denkbar, anstelle eines umfassenden Dateneigentums sich auf zwei Bereiche zu konzentrieren, die jeweils nur eine bereichsspezifische Anpassung der Rechtsordnung erforderlich machen. Erstens wäre dies die Stärkung des Verbrauchers durch die **Schaffung eines effektiven Vertragskontrollrechts im Bereich der Mobilität**. Zweitens könnte eine Stärkung der Beteiligten, die zwar keine Verbraucher, aber dennoch gegenüber großen Konzernen unterlegen sind, durch das **Wettbewerbs- und Kartellrecht** erfolgen. Beide Anpassungen zielen auf einen gegenseitigen Interessensausgleich ab, indem sie den tendenziell schwächeren Gegner stützen.

Die Stärkung des schwächeren Vertragspartners (dies muss freilich nicht zwingend ein Verbraucher sein) könnte durch ein **effektives Vertragskontrollrecht** erfolgen. Ein solches ist bereits aus den §§ 305 ff. BGB in Form der AGB-Kontrolle bekannt. Die vorhandene Normierung im BGB könnte folglich erweitert werden, um datenspezifische Problemlagen zu erfassen. Ziel der AGB-Kontrolle ist es, den typischerweise schwächeren Vertragspartner zu stärken, allerdings nur in den Fällen, in denen dies gerechtfertigt ist, also vor allem bei einer einseitigen Vermachtung von Verhandlungspositionen. Der schwächere Vertragspartner, der in der Regel der Verbraucher ist, soll damit seine schwächere Verhandlungspositionen bestmöglich kompensieren können, um so Vertragsverhandlungen auf Augenhöhe führen zu können und nicht einer Situation ausgeliefert zu sein, in der er entweder alles akzeptieren muss oder keine Gegenleistung erhält.

Dafür wäre eine gesetzliche oder **interpretatorische Typisierung** der zugrundeliegenden Verträge erforderlich. Des Weiteren müsste dezidiert untersucht werden, in welchen Fällen eine unangemessene Benachteiligung gegeben ist. Dies wäre bspw. der Fall, wenn die Hersteller bzw. die Anbieter von Plattformen sich qua Vertrag unbegrenzte Rechte an den Daten ausbedingen und diese dann ökonomisch ausbeuten würden, ohne denjenigen, der die Daten bereitgestellt hat, in irgendeiner Weise am Gewinn zu beteiligen. Wo die datenschutzrechtlichen Grenzen für derartige umfassende Rechteeinräumungen liegen, ist bislang ungeklärt und unter der Datenschutz-Grundverordnung völlig offen. Eine zivilrechtliche Regelung oder Rechtsfortbildung könnte dementsprechend für Rechtssicherheit sorgen.

Dabei ist jedoch zu beachten, dass die Vertragskontrolle in Form der bisherigen **AGB-Kontrolle** nur für Nebenleistungs-, aber nicht für Hauptleistungspflichten greift. Damit würde eine Vertragskontrolle in Form der AGB-Kontrolle leer laufen, wenn die Einräumung einer Datenerhebung, -verarbeitung bzw. -nutzung als Hauptleistungspflicht angesehen würde. Dies wäre bspw. der Fall, wenn die Einwilligung im Gegenzug zu einer Reduzierung des Kaufpreises bzw. Mietzinses erfolgen, also quasi mit dem wirtschaftlichen Wert der Daten bezahlt werden würde.

Wie schon dargestellt muss der jeweils schwächere Vertragspartner nicht zwingend ein Verbraucher sein, weil substantielle Machtgefälle auch zwischen Unternehmern vorkommen können. Dabei ist insbesondere an das vertragliche Verhältnis zwischen marktmächtigen Herstellern einerseits, kleineren Plattformanbietern und Diensteanbietern andererseits zu denken sowie zwischen diesen Parteien mit großen Informationsdienstleistern. Hier könnte zwar auch eine AGB-Kontrolle greifen, jedoch ist dies meist nicht zweckdienlich. Die Zielrichtung ist vielmehr eine **Stärkung des Wettbewerbs**, die **Förderung von Innovation** und die **Verhinderung von Monopolen**, was den Anwendungsbereich des **Wettbewerbs- und Kartellrechts** eröffnet. Schutzgüter sind dabei primär die Schaffung einer wirtschaftlichen Fairness sowie die Sicherung des freien Wettbewerbs. Wirtschaftliche Fairness und freier Wettbewerb werden z. B. durch einheitliche Schnittstellen sowie gesetzliche Regulierung bzw. Schaffung der Zugriffsrechte ermöglicht. Des Weiteren müssten faktische Aneignungen und damit einhergehend der faktische Ausschluss von Wettbewerbern verhindert werden, so dass der Zugang für innovative Wettbewerber offen und möglich bleibt, um neue Produkte und Dienstleistungen am Markt zu etablieren. Dies kann auch eine Pflicht zu einer Zurverfügungstellung der Daten in einem bestimmten Format sowie die Öffnung bzw. Offenlegung von Software und Hardware, insb. Plattformen, umfassen, um die Anbindung eigener Produkte zu ermöglichen. Folglich ist das primäre Ziel die Schaffung und der Schutz eines innovationsfreudigen Marktes und nicht nur der Schutz der eigenen Verhandlungsposition. Folglich können Ansatzpunkte z. B. in der Förderung der Kompatibilität durch genormte Schnittstellen liegen und bis in den Bereich *Open Innovation*³⁴⁴ reichen.

Vorteil einer solchen **bereichsspezifischen Anpassung** wäre, dass keine Gefahr von einem konturenlosen Dateneigentumsrecht ausgeht. Eine solche Regelung könnte individueller an die Bedürfnisse des Mobilitätssektors angepasst werden. Des Weiteren besteht auch keine Gefahr, dass

344 Siehe dazu unter 4.3.5. sowie 5.2.6.

durch eine vermeintliche Zuordnung künftige innovative Geschäftsmodelle verhindert werden. Eine bereichsspezifische Anpassung belässt den beteiligten Akteuren eine große Flexibilität, so dass diese im Rahmen der Vertragsfreiheit, flankiert durch die korrigierenden Schranken, Daten weiterhin nutzen können.

Demgegenüber gehen mit einer solchen Anpassung auch **Nachteile** einher. Wie dargelegt ist eine bereichsspezifische Regelung zwar flexibel, aber sie zieht gleichzeitig die Gefahr der Schaffung eines komplizierten Regelungssystems mit sich. Erstens wird eine Bestandsaufnahme der bestehenden Benachteiligungen nur schwer möglich sein und zweitens bringt jede technische Entwicklung das Risiko mit sich, dass neue Schutzlücken entstehen. Folglich wäre der Gesetzgeber gehalten, die Kontrollmechanismen und Schutzinstrumente weiter nachzubessern, sodass eine übersichtliche und praktikable rechtliche Lösung nicht unbedingt wahrscheinlich erscheint. Die damit einhergehende Rechtsunsicherheit würde tendenziell vielmehr innovationshemmend wirken. Dies führt des Weiteren zu Einzelfallentscheidungen über die Angemessenheit von Vergütungen, was im Rahmen eines Massengeschäfts nicht praktikabel ist. Zwar können unbillige Klauseln *per se* durch Generalklauseln ausgeschlossen werden, aber eine vorübergehende Rechtsunsicherheit ist dennoch nicht von der Hand zu weisen. Darüber hinaus haben solche Regelungen, die im Rahmen von Verträgen greifen, nur eine relative Wirkung zwischen den beteiligten Akteuren, d. h. sie entfalten ihre Rechtswirkung lediglich *inter partes*. Aufgrund der Vielzahl an beteiligten Subjekten, die Interesse an fahrzeugbezogenen Daten geltend machen, könnten sich in der Praxis Schwierigkeiten bei divergierenden Vereinbarungen zwischen unterschiedlichen Parteien ergeben. Interessenten an der Datennutzung im Zusammenhang mit vernetzten Fahrzeugen sind bspw. Hersteller, Lieferanten, Plattform-Betreiber, Dienstleister (*Cloud*), Telekommunikationsunternehmen, Versicherer, Fahrzeugeigentümer, -halter, -nutzer, *Leasing*geber und -nehmer sowie staatliche Stellen³⁴⁵.

Des Weiteren würde eine solche Anpassung auch nur für den dann geregelten Bereich der Mobilitätsdaten gelten und nicht für alle wirtschaftlichen Bereiche, die mit Da-

ten arbeiten. Eine einheitliche Regelung für die gesamte Rechtsordnung, insbesondere auf Grund der rasanten Entwicklung von innovativen Geschäftsmodellen auf diesem Gebiet, auch außerhalb des Mobilitätssektors, wäre mehr als begrüßenswert. So wird in Bezug auf die geltende Rechtslage angemerkt, dass im Zusammenhang mit von *Smart Devices* erzeugten Daten auf gesetzlicher Ebene eine Vielzahl von Rechtsbeziehungen durch bereichsspezifische Regelungen bestehen, die ungenügend aufeinander abgestimmt sind. Dies spiegele sich in der Folge dann auch bei vertraglichen Absprachen wider³⁴⁶. Insoweit bestünde bei der Beibehaltung ausschließlich bereichsspezifischer Regelungen Bedarf einer (permanenten) Nachjustierung. Folglich wäre eine reine bereichsspezifische Anpassung, insbesondere durch die Schaffung eines Vertragskontrollrechts, alleine nicht wünschenswert.

5.2.3 Ausschließliche Fokussierung auf das Datenschutzrecht

Anstatt ein Ausschließlichkeitsrecht zu normieren, welches mit zahlreichen Rechten anderer belastet wäre, könnte des Weiteren in Betracht gezogen werden, die vorhandenen bereichsspezifischen Regelungen, die den Schutz von Daten zum Gegenstand haben, beizubehalten aber anzupassen³⁴⁷. Dies bietet sich insbesondere vor dem Hintergrund an, dass ein Großteil der Anwendungsfälle ohnehin personenbezogene Daten betrifft. So liegt eine Fokussierung auf den Bereich des Datenschutzrechts nahe, welches bereits einen umfassenden Schutzmechanismus und weitreichende Verfügungsbefugnisse (bspw. kein Datenumgang ohne Einwilligung) bietet³⁴⁸. Des Weiteren würde damit der großen Bedeutung des Datenschutzrechts, die insbesondere auch europarechtlich determiniert ist, Rechnung getragen.

Um die wirtschaftlichen Zusammenhänge der Datenflüsse transparenter zu machen und Akteure an der Wertschöpfung ihrer Daten zu beteiligen, könnte insbesondere eine Spezifizierung allgemeiner datenschutzrechtlicher Prinzipien erfolgen, wie bereits teilweise durch moderne Datenschutzinstrumente wie *privacy by design*, *privacy by default* oder Datenschutzaudit bzw. -siegel geschehen (diese werden künftig deutlich präzisiert, s. Art. 25, 42, 43 DSGVO)³⁴⁹. Bei gewissen Vorgaben auf einer allgemeinen Gestaltungs-

345 http://schaufenster-elektromobilitaet.org/media/media/documents/dokumente_der_begleit_und_wirkungsforschung/EP21_Zivil-_und_datenschutzrechtliche_Zuordnung.pdf, S. 33.

346 Heun/Assion, Internetrecht der Dinge, Vortrag im Rahmen der Telemedicus Sommerkonferenz 2015, Präsentation abrufbar unter: https://www.telemedicus.info/uploads/Heun_Assion_InternetrechtderDinge.pdf.

347 Siehe in diesem Zusammenhang bereits Kapitel 3.3, das auf die Einhaltung von datenschutzrechtlichen Standards im Rahmen des Kartell- und Lauterbarkeitsrecht eingeht.

348 Siehe dazu ausführlich Kap. 3.2.1.

349 Krüger, ZRP 2016, 190 (191).

ebene, die Voraussetzung, Inhalt und Form näher bestimmen, könnten die konkreten Rechtsbeziehungen und Datenflüsse weiterhin auf vertraglicher Basis geregelt werden. Auf diese Weise könnten auf den Einzelfall zugeschnittene Regelungen zwischen Eigentümer, Halter, Fahrer und Beifahrer eines Kfz sowie den beteiligten Unternehmen geschaffen werden³⁵⁰.

Für diesen Ansatz könnte sprechen, dass zum Teil bezweifelt wird, dass das gegenwärtig vorhandene gesetzliche Instrumentarium die Akteure nur unzureichend schützt.³⁵¹ Insbesondere der weite Anwendungsbereich des Datenschutzes, der viele Betroffenenrechte und Informationspflichten enthält und durch die DSGVO europarechtlich gestärkt wurde, unterstreicht dies³⁵².

Schwächen dieses Ansatzes liegen jedoch darin, dass das **Datenschutzrecht zum Schutz der Persönlichkeitsrechte der Betroffenen** geschaffen wurde und sich daher ggf. einige Prinzipien und allgemeine Grundsätze nicht auf den wirtschaftlichen Umgang mit Daten übertragen lassen. Aus diesem Grund könnten sich Regelungen zur wirtschaftlichen Verwendung von Daten auch konzeptionell **kaum in das Datenschutzrecht integrieren lassen**, zumal nur der Bereich der personenbezogenen Daten vom BDSG bzw. der DSGVO erfasst ist. Dies führt insbesondere dazu, dass durch eine Anonymisierung von Daten der Anwendungsbereich des Datenschutzes vollständig abgeschnitten wird, der ökonomische Wert der Daten aber (weithin) erhalten bleibt. Insgesamt scheint dieser Ansatz daher nicht empfehlenswert.

5.2.4 Spezifische Nutzungsrechte und Nutzungslizenzen

Eine abgeschwächte, flexiblere Form eines Ausschließlichkeitsrechts könnte die gesetzliche Regelung einzelner, spezifischer Nutzungsrechte an den erzeugten Daten sein. Dies würde einen schwächeren Schutz als ein Ausschließlichkeitsrecht gewähren und könnte dazu führen, dass mehrere Personen und Stellen – gleichermaßen, oder abgestuft – berechtigt sind, die Daten wirtschaftlich zu verwenden, um somit möglichst viel vom wirtschaftlichen Wert der Daten zu erhalten. Dabei kann eine wirtschaftliche Verwendung der Daten erfasst sein, die nur einzelne Bestandteile für eine kurze Zeitspanne vorsieht, über die Aufbereitung ein-

zelner Daten bzw. ihrer Bestandteile bis hin zu langfristigen Nutzungslizenzen.

Ein solches Vorgehen könnte einige der Probleme eines vollwertigen Dateneigentums als Ausschließlichkeitsrecht vermeiden. Während bei letzterem unter mehreren denkbaren Ansätzen für eine Zuordnung³⁵³ einer ausgewählt wird, wäre es ohne weiteres möglich, mehrere Nutzungsinteressen als legitim anzuerkennen. Des Weiteren können einzelne Nutzungsrechte zielgenauer eingeräumt werden bzw. auf mehrere Beteiligte gestreut werden. Dies führt einerseits zu einer angemesseneren Gewinnallokation auf der Unternehmensseite und schützt andererseits den Fahrzeugeigentümer, Halter bzw. Fahrer, denn dieser kann seine Einwilligung zur Datennutzung spezifischer aufschlüsseln. Der Betroffene kann individueller und einfacher seine Entscheidung nach wirtschaftlichen Interessen steuern, also auch zum Schutz seiner Privatsphäre, und dabei zwischen Nutzungsberechtigten differenzieren: quasi eine Verbindung aus informationeller und ökonomischer Selbstbestimmung. So kann er bspw. die Daten verschiedenen Unternehmen, die jeweils eigene Schwerpunkte haben, zur Verfügung stellen oder nur die Nutzung mancher Daten oder nur für eine bestimmte Zeitspanne einräumen oder unterschiedliche Gegenleistungen aus-handeln (oder auf sie verzichten)³⁵⁴. Umgekehrt kann dem Risiko begegnet werden, dass der umgekehrte Ansatz der Schaffung eines *Open-Data-Systems*³⁵⁵ zu weit geht und ökonomische Potentiale jedermann auch dort bereitstellt, wo einzelne Akteure ein legitimes Interesse an einer prioritären Nutzung haben. Insgesamt wäre ein solches System somit erheblich flexibler, weil einzelne Rollen (z. B. die in den Fallstudien genannten), aber auch einzelne Interessen abgestuft reguliert werden könnten. Dies würde durch einen besseren Interessenausgleich die Feingliedrigkeit und damit die Akzeptanz einer gesetzlichen Normierung erhöhen. Eine Abstufung würde des Weiteren eine höhere Verwertung auf der dritten Ebene ermöglichen. Mit anderen Worten müsste jeweils nur über die Legitimität oder Illegitimität der Position eines Akteurs entschieden werden, ohne gleichzeitig alle anderen Akteure von der Nutzung auszuschließen. Im Ergebnis sollten die einzelnen Ausprägungen möglicher Nutzungsrechte und Nutzungslizenzen aber nicht *a priori* durch den Gesetzgeber determiniert werden, sondern müssten die Folge einer Entscheidung des Marktes sein. Ansonsten würde die Gefahr bestehen, dass

350 Hornung/Gooble, CR 2015, 265 (273).

351 Dorner, CR 2014, 617 (626).

352 Dorner, CR 2014, 617 (626).

353 Siehe dazu unter Kapitel 5.1.3.

354 Siehe dazu unter Kapitel 4.3.1.

355 Siehe dazu unter Kapitel 5.2.6.

der Gesetzgeber bestimmte Geschäftsmodelle von Anfang an ausschließt, was nicht im Interesse einer möglichst umfassenden Verwertung der Daten ist³⁵⁶.

Ein solches Modell hat allerdings auch **erhebliche Nachteile**. Zunächst ergibt sich ein erhebliches Konfliktpotential und damit ein erheblicher Abstimmungsbedarf zum Datenschutzrecht, also zur 2. Ebene (Schranken). Dieses enthält nämlich in vielen Bereichen Regelungen, in denen – für personenbezogene Daten – genau die vorgenannte Abwägung mit berechtigten Interessen Dritter erfolgt, die die Daten ökonomisch nutzen wollen. Auch in einer Beschränkung dieses Ansatzes auf nicht personenbezogene Daten verbleiben Probleme, wie z. B. kartell- und wettbewerbsrechtliche, aber auch IT-sicherheitsrechtliche Anknüpfungspunkte. Während ein Ausschließlichkeitsrecht die Gefahr einer überschießenden Regelung birgt, besteht hier das **Risiko einer Unterregulierung**, weil in einem System einzelner Nutzungslizenzen alle legitimen Nutzungs-

interessen erfasst werden müssen – andernfalls würde das System zugunsten einzelner Akteure in Schieflage geraten. Eine gesetzliche Regelung müsste also eine Vielzahl von Rollen und Akteuren bedenken. Dies ist insbesondere im Bereich des vernetzten Automobils **schwer zu erreichen**, weil dieser derzeit durch eine erhebliche Innovationsgeschwindigkeit und durch eine starke Volatilität der Marktstrukturen gekennzeichnet ist. In dieser Situation eine einheitliche Systematik zu erreichen, erscheint sehr schwierig.

5.2.5 Schaffung eines verbesserten Integritätsschutzes von Daten

Außerhalb von Vertragsbeziehungen³⁵⁷ schützt das Deliktsrecht die Integrität von Daten nicht ausreichend. Die nachfolgende Übersicht zeigt, welche Anspruchsgrundlagen bei einer Beeinträchtigung von Daten in Betracht kommen und woran ein Anspruch in der Regel scheitert:

Schutz über § 823 Abs. 1 BGB	Verletzung des Eigentums Geschützt wird lediglich das Eigentum (bzw. der Besitz) am Datenträger – Schutzlücke, wenn beides nicht vorliegt (insbesondere bei Cloud-Konstellationen)
	Recht am eingerichteten und ausgeübten Gewerbebetrieb Greift nur bei betrieblichen Daten, zudem muss Eingriff betriebsbezogen sein – Schutzlücke bei bloß mittelbaren Eingriffen
	Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme Integrität des Systems nur geschützt, um die Vertraulichkeit des Systems zu schützen – Schutzlücke, bei Schäden, durch die die Vertraulichkeit nicht verletzt wird
Schutz über § 823 Abs. 2 BGB	<ul style="list-style-type: none"> ▪ Schutz nur bei vorsätzlichen Eingriffen ▪ Daten müssen besonders gesichert sein ▪ bloßes Löschen oder Verändern von Daten nicht geschützt, da Schutzzweck Geheimhaltungsinteresse
Schutz über § 826 BGB	Greift nur bei vorsätzlichem und sittenwidrigen Verhalten

Abbildung 30: Schaffung eines Integritätsschutzes

356 Siehe dazu unter Kapitel 4.3.3.

357 Zum vertraglichen Schutz *Spindler*, in: Leible/Lehmann/Zech (Hrsg.), *Unkörperliche im Zivilrecht*, S. 261 (275 ff.); *Faust*, 71. DJT, Teil A S. 71.

Bei **vorsätzlichen** Zerstörungen des Datenträgers kann der Nutzungsberechtigte Ansprüche gem. §§ 823 Abs. 2 i. V. m. 303a StGB³⁵⁸ und § 826 BGB gegen den Schädiger geltend machen. Bei gezielten und betriebsbezogenen Eingriffen kommen zudem Ansprüche wegen Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb in Betracht³⁵⁹, das ein sonstiges Recht i. S. v § 823 Abs. 1 BGB ist. Vor **fahrlässigen** Beschädigungen der Daten bietet § 823 Abs. 1 BGB dem Eigentümer des betroffenen Speichermediums Schutz³⁶⁰, da gespeicherte Daten aufgrund ihrer Verkörperung auf dem Speicher als Sachen (§ 90 BGB) angesehen werden³⁶¹. Gleiches gilt zu Gunsten des berechtigten Besitzers des Servers, weil auch dessen Position als sonstiges Recht i. S. v. § 823 Abs. 1 BGB anerkannt wird³⁶². Demgegenüber sind weder die einzelnen elektronischen Daten als solche noch der Datenbestand einer Person als sonstiges Recht i. S. v. § 823 Abs. 1 BGB einzustufen, da sich der Schutzbereich eines solchen Rechts kaum definieren lässt³⁶³.

Dieser mittelbare Integritätsschutz von Daten über das Eigentum reicht heute jedoch nicht (mehr) aus³⁶⁴. **Schutzlücken** bestehen insbesondere bei modernen Datenverarbeitungsstrukturen in der *Cloud*. Löscht oder beeinträchtigt ein Dritter auf andere Weise fahrlässig die Integrität von Daten stehen dem Dateninhaber nämlich meist keine Ansprüche nach § 823 Abs. 1 BGB zu, da er kein Eigentümer des als *Cloud-Service* bezogenen Speicherplatzes ist. Im Gegensatz zum bislang verbreiteten *Application Service Providing* (ASP) treiben *Cloud*-Strukturen die Virtualisierung voran und lösen damit die Rechenprozesse von bestimmten Hardwareressourcen³⁶⁵. Daten werden in der *Cloud* da-

her oft auf unterschiedlichen Servern weltweit gleichzeitig verarbeitet, so dass dem *Cloud*-Nutzer typischerweise keine (berechtigte) Besitzposition mehr zugewiesen werden kann, die als sonstiges Recht Ansprüche nach § 823 Abs. 1 BGB stützen könnte. Um diese Schutzlücke zu schließen, hat sich der 71. Deutsche Juristentag jüngst dafür ausgesprochen, ein Schutzgesetz nach Vorbild von § 303a StGB zu schaffen, das über § 823 Abs. 2 BGB auch eine Haftung für fahrlässige Verletzungen begründet³⁶⁶. § 303a StGB bietet einen guten Ausgangspunkt für ein solches Schutzgesetz³⁶⁷, da die Norm bereits einen Katalog von Verletzungshandlungen enthält, die das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit seiner Daten schützen³⁶⁸. Um den geschützten Personenkreis rechtssicherer zu bestimmen, sollte die Norm darüber hinaus definieren, wer als „Verfügungsbefugter“ Anspruchsinhaber ist. Diese Definition sollte die bereits im Rahmen des Ausschließlichkeitsrechts entwickelten Kriterien für eine Zuordnung von Daten berücksichtigen.

Mit Blick auf die Strafandrohung sollte eine solche Norm außerdem nicht ins Straf-, sondern in das öffentliche oder **Zivilrecht** eingeordnet werden. Erwogen wird hierzu etwa das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)³⁶⁹. Da die zu schaffende Regelung aber nicht die Aufgaben des Bundesamtes verändern, sondern den deliktischen Schutz von Daten verbessern soll, liegt es näher, diese Norm in das Deliktsrecht zu integrieren. Die genannten Erwägungen führen unter Berücksichtigung der oben entwickelten Definition der Verfügungsbeziehung zu folgendem Entwurf:

358 Zum Antragsberechtigten i. S. v. § 303c StGB, Wieck-Noodt, in: MüKo StGB, 2. Aufl. 2014, § 303a Rn. 26.

359 Faust, 71. DJT, Teil A S. 74; Spickhoff, in: Leible/Lehmann/Zech (Hrsg.), Unkörperliche Güter im Zivilrecht, S. 233 (242 f.).

360 Sprau, in: Palandt (Hrsg.), 75. Aufl. 2016, § 823 Rn. 9.

361 Jickeli/Stieper, in: Staudinger (Hrsg.), BGB, 2011, § 90 Rn. 19.

362 Wagner, in: MüKo BGB, 6. Aufl. 2013, § 823 Rn. 220 f.; Sprau, in: Palandt (Hrsg.), 75. Aufl. 2016, § 823 Rn. 13.

363 Spickhoff, in: Leible/Lehmann/Zech (Hrsg.), Unkörperliche Güter im Zivilrecht, S. 233 (243 f.); Wagner, in: MüKo BGB, 6. Aufl. 2013, § 823 Rn. 165; Für den Schutz eines Rechts „am eigenen Datenbestand“ als sonstiges Recht dagegen Meier/Wehlau, NJW 1998, 1585 (1588 f.); Bartsch, in: Conrad/Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, § 22 Rn. 23; Spindler, JZ 2016, 805 (813 f.); Jickeli/Stieper, in: Staudinger (Hrsg.), BGB, 2011, § 90 Rn. 19.

364 Faust, 71. DJT, Teil A S. 74; Spindler, JZ 2016, 805 (812); Wendehorst, NJW 2016, 2609 (2612 f.); Vgl. auch Bartsch, in: Conrad/Grützmaker (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, § 22 Rn. 10 ff.

365 Jotzo, Der Schutz personenbezogener Daten in der Cloud, 2013, S. 20 f.

366 Beschlüsse des 71. DJT, B. Ziff. 28. Var. b.

367 Spindler möchte stattdessen ein „wesentlich komplexeres System“ schaffen, das den gesamten Bereich der Produkt- und IT-Sicherheit mit regelt, JZ 2016, 805 (814).

368 Zum Zweck von § 303a StGB Stree/Hecker, in: Schönke/Schröder (Hrsg.), StGB, 29. Aufl. 2014, § 303a Rn. 1.

369 Faust, 71. DJT, Teil A S. 87.

§ 823a BGB-Entwurf Schädigung von Daten

Wer vorsätzlich oder fahrlässig rechtswidrig Daten Dritter löscht, unterdrückt, unbrauchbar macht oder verändert ist dem Verfügungsberechtigten der Daten zum Ersatz des daraus entstehenden Schadens verpflichtet. **Verfügungsberechtigter der Daten** ist, wer bei wirtschaftlicher Betrachtungsweise für die Erstellung und Speicherung des Datums verantwortlich ist. Dies ist derjenige, der bei einer wirtschaftlichen Gesamtwürdigung des Erstellungsvorgangs die wesentliche Investition in die Datenerstellung vornimmt. Von einer wesentlichen Investition kann in der Regel ausgegangen werden, wenn eine unmittelbare Investition in die Datenerstellung vorgenommen wird, die Investition für den Vorgang der Datenerstellung von entscheidender Bedeutung ist und die getätigte Investition nicht schon anderweitig kompensiert worden ist. Indizien für eine Investition in diesem Sinne sind die wirtschaftliche Unterhaltung des datengenerierenden Gegenstandes, die Vornahme oder Initiierung der datengenerierenden Handlung sowie das Sacheigentum am datengenerierenden oder datenspeichernden Gegenstand.

Die entsprechende Regelung ist **geeignet**, die aufgezeigte Schutzlücke zu schließen. Der verbesserte Integritätsschutz von Daten ermöglicht insbesondere Unternehmen stärker als bisher Cloud-Dienste einzusetzen. Dadurch können sie zum einen ihre Geschäftsprozesse effektiver gestalten. Zum anderen sorgt die wachsende Nachfrage nach Cloud-Lösungen für neue Investitionsanreize auf Seiten der Anbieter solcher Anwendungen. Mit dem gezeigten Entwurf zum Integritätsschutz werden zudem Daten nicht ausschließlich einzelnen Personen zugeordnet oder gar zu deren Gunsten monopolisiert. Letztlich ist der Lösungsansatz daher auch kombinierbar mit der weitergehenden Zuordnung im Rahmen eines zu erwägenden Ausschließlichkeitsrechts für Daten. Gleiches gilt für weitergehende Normen, die es z. B.

Mobilitätsdiensteanbietern *de lege lata* untersagen, Daten aus den Fahrzeugen zu nutzen.

5.2.6 Schaffung eines Open-Data-Systems

Zuletzt ist zu betrachten, ob anstelle einer eigentumsähnlichen Zuordnung stattdessen ein konträrer Ansatz gewählt werden könnte: Daten als Allgemeingüter bzw. als (Mobilitäts-) Datenallmende³⁷⁰. Dadurch könnten wenigstens für nicht-personenbezogene Daten die Probleme umgangen werden, die mit der Schaffung eines Dateneigentums in Hinblick auf den Datenschutz bei personenbezogenen Daten bestehen (s. o.). Folglich könnte man aus diesem Grund schließlich vor allem für nicht-personenbezogene Daten ein Open-Data-System (**Open Data und Public Open Data**) schaffen, welches evtl. sogar bis hin zum Open-Source-Gedanken reicht.

Die Förderung von innovativen Diensten sowie die Schaffung von neuen und individuellen Wertschöpfungsmodellen im Bereich des vernetzten Automobils scheint im Rahmen der Leitlinien von *Open Data*³⁷¹ und *Open Innovation*³⁷² besonders vielversprechend zu sein. Die Übergänge von *Open Data* hin zu *Open Innovation* sind fließend, sodass eine sinnvolle Abgrenzung nicht möglich ist. Dazu sollen die durch Fahrzeuge produzierten Daten in ihrer Rohform der Allgemeinheit zur Verfügung gestellt werden. Diese Nachnutzung der Daten, nachdem sie schon bspw. im Bereich der *Public Open Data* von staatlicher Seite genutzt worden sind, ermöglicht die Schaffung einer Grundlage für eine wirtschaftliche Verwendung im Rahmen weiterer Wertschöpfungsmodelle. Für die Schaffung einer angemessenen Gewinnallokation sind Monopole auf die Nutzung bestimmter Daten wenig hilfreich³⁷³. Vielmehr sollen durch einen kooperativen Ansatz **Anreize für Innovationen** gesetzt werden. Insbesondere in Bezug auf staatliche Daten existiert mit dem Informationsfreiheitsgesetz (IFG) und diversen bereichsspezifischen Regelungen wie bspw. dem Umweltinformationsgesetz (UIG) und dem Geodatenzu-

370 Der Begriff beschreibt zutreffend in historischer Anlehnung einen allen weitgehend unbeschränkt zur Verfügung stehenden Informationsmarkt. Eine Allmende stellte im Mittelalter eine im weitesten Sinne öffentliche Institution dar. Sie stand im Eigentum einer Körperschaft und das von ihr umfasste Gebiet (Wald, Weide und Wasser) stand den Mitgliedern der Körperschaft zur gemeinsamen Nutzung zur Verfügung. Die Allmende stellte für die Dorfgemeinschaft eine Art öffentlichen Raum dar. Im Gegensatz zur Agora diente dieser primär der ökonomischen Versorgung mit Gütern des täglichen Bedarfs und war lediglich für einen bestimmten Personenkreis zugänglich und nutzbar; ausführlich zu Unterschieden und Parallelen Ernst, in: Schliesky/Ernst/Schulz (Hrsg.), *Die Freiheit des Menschen in Kommune, Staat und Europa*, Festschrift für Edzard Schmidt-Jortzig zum 70. Geburtstag, 2011, S. 79 (85 ff.) m. w. N. Der Begriff der Datenallmende lässt sich zurückführen auf Reiner mann, Beitrag des Seminars »Informationssysteme für den Bürger und für die Verwaltungsführung« zur International Design Competition for an Advanced Information City, 1986, S. 9; ders., in: Schulz (Hrsg.), *Die Zukunft der Informationssysteme*, 1986, S. 111 (115); vgl. Lenk/Meyerholt/Wengelowski, *Wissen managen in Staat und Verwaltung*, 2014, S. 34. Zum historischen Verständnis Carlen, in: Auty u. a. (Hrsg.), *Lexikon des Mittelalters*, Bd. 1, 1980, Sp. 439 f.; zur Verortung zwischen Markt und Staat (im Sinne des englischen Begriffs „commons“) Ostrom, *Governing the Commons*, 1990 (deutsch: *Die Verfassung der Allmende*, 1999).

371 Schulz, *VerwArch* 2013, 327 ff.; ausführlich Lederer, *Open Data. Informationsöffentlichkeit unter dem Grundgesetz*, 2014.

372 Blohm, *Open Innovation Communities*, 2013; *Hornung/Goeble*, CR 2015, 265 (272) m. w. N.

373 Hornung/Goeble, CR 2015, 265 (272).

gangsgesetz (GeoZG) bereits ein im Grundsatz voraussetzungsloser Zugang zu den in Daten verkörperten Informationen. Die Zurverfügungstellung erfährt ihre Grenzen nur dort, wo es bisher schon bestehende Schranken gibt. Zur Erfüllung staatlicher Aufgaben wie dem Ausbau und Erhalt der öffentlichen Infrastruktur könnte auch durch eine Pflicht zur Preisgabe von Daten gegenüber dem Staat Informationsbeschaffung betrieben werden. Diese Verpflichtung von Privaten kann alle solche Daten erfassen, die der reinen Verkehrssicherheit und dem sonstigen Gemeinwohl, wie z. B. Informationen über den Straßenzustand, dienen. Eine solche Verpflichtung wird wohl mit Gemeinwohlinteressen gerechtfertigt werden können. Ansonsten ist im Bereich *Public Open Data* insbesondere an die Daten zu denken, die der Staat im Rahmen von *Car-2-Infrastructure*-Anwendungen im öffentlichen Sektor gewinnt und auch wieder bereitstellt. Hierbei kann es sich um Rohdaten oder auch anonymisierte Daten handeln. Die Bereithaltung der Daten durch den Staat wäre am einfachsten auf einem sogenannten Daten-Marktplatz³⁷⁴, der diskriminierungsfrei zugänglich sein müsste. Erste Ansätze, die bereits existieren, müssten noch weiter ausgebaut werden. In einem Antrag der Regierungsfractionen vom 26. Januar 2016 heißt es in Bezug auf Verkehrsdaten: *Der „diskriminierungsfreie Zugang“ zu den öffentlichen Verkehrsdaten „ist zu gewährleisten, um Raum für weitere Innovationen zu schaffen bzw. zu erhalten. Nur durch die freie Verfügbarkeit der Daten (Open Data) und offene und standardisierte Schnittstellen sind Vehicle2x-Kommunikation (Vehicle2Vehicle und Vehicle2Infrastructure, d. h. Kommunikation von Fahrzeugen mit anderen Fahrzeugen bzw. Verkehrsteilnehmern und Infrastruktur) und somit eine funktionierende intelligente Mobilität möglich“. Es wird daher gefordert, dass „[ö]ffentliche Mobilitäts- und Infrastrukturdaten [...] allen Verkehrsteilnehmern gleichermaßen zur Verfügung stehen.“*³⁷⁵

Neben *Public Open Data* ist aber auch ein *Open-Data-System* außerhalb von staatlichen Datenströmen denkbar. Diese Daten, insbesondere von am Markt wirtschaftlich tätigen Akteuren, werden hingegen bereits heute faktisch geheim gehalten und lediglich gegen eine Gegenleistung preisgegeben. Da für den Handel mit Daten jedoch kein stabiler Rechtsrahmen besteht, wird befürchtet, dass Daten

nicht zu demjenigen gelangen, der mit ihrer Nutzung den größten Mehrwert erzielen könnte³⁷⁶. Deshalb wäre es im Interesse der Innovationsförderung, *Open Data* nicht nur im gemischt staatlich-privaten Umfeld zu fördern, sondern auch im ausschließlich privaten Kontext. Bisher ist es, insbesondere für kleinere Unternehmen, schwer mit innovativen Wertschöpfungsmodellen am Markt Fuß zu fassen, denn der Zugang zu Daten wird ihnen vielfach durch große Unternehmen erschwert, indem diese sich die Daten *de facto* aneignen und vorbehalten. Dies schwächt die Wirtschaft in ihrer Gesamtheit. Eine Stärkung der Innovation wäre jedoch durch einen kooperativen Ansatz auch hier möglich, indem die Interoperabilität ausgebaut und der Austausch von Daten vereinfacht würde. Der Vorteil liegt dabei nicht nur auf der Seite von kleineren Unternehmen, sondern auch größere könnten durch die Steigerung ihrer Kompatibilität die Funktionen ihrer Produkte vergrößern und flexibler am Markt reagieren.

Eine **Pflicht** für Automobilhersteller, Zulieferer sowie Plattform- und Diensteanbieter zur Bereitstellung ihrer Rohdaten bzw. Daten in ihrer Rohform, die durch Automobile produziert wurden, ist jedoch weder förderlich noch rechtlich erstrebenswert³⁷⁷. Eine solche Pflicht würde die jeweiligen Unternehmen unter Umständen in unverhältnismäßiger Weise in ihren verfassungsrechtlichen Grundrechten einschränken. Demgegenüber wäre es zielführender, ein **Anreizsystem** zu schaffen, auf deren Basis durch vertragliche Vereinbarungen, im Rahmen des bisherigen Rechtssystems, eine Austauschplattform etabliert werden könnte. Eine Austauschplattform könnte für die Automobilbranche sinnvoll sein, um durch eine Zusammenarbeit kosteneffizienter zu arbeiten, die jeweiligen Kompetenzen zu bündeln und somit gemeinsam wirtschaftlicher zu sein. Dies gilt insbesondere als Gegengewicht zu den großen Informationsdienstleistern³⁷⁸. Neben einer solchen Plattform zum Austausch der nicht-personenbezogenen Daten können des Weiteren durch offene und standardisierte Schnittstellen Anreize und Nischen für weitere innovative Wertschöpfungsmodelle geschaffen werden. Beispielsweise sei hier nur die Öffnung von Multimediaplattformen zu nennen. Anknüpfungspunkte zur Förderung eines solchen *Open-Ansatzes* im Bereich des Mobilitätssektors könnten

374 Siehe dazu bereits den „Mobilitäts Daten Marktplatz“ (www.mdm-portal.de) sowie die mCloud, (mcloud.de).

375 BT-Drs.18/7362 vom 26. 1. 2016, abrufbar unter: <http://dip21.bundestag.de/dip21/btd/18/073/1807362.pdf>, S. 3 f.

376 Dorner, CR 2014, 67 (625).

377 In spezifischen Situationen kann eine solche Pflicht natürlich legitimiert werden oder ergibt sich sogar schon aus geltendem Recht, wenn sich beispielsweise nach einem Verkehrsunfall nach den Datenerhebungsnormen der Strafprozessordnung für Hersteller oder sonstige Anbieter eine Pflicht zur Bereitstellung von Daten in einem konkreten Ermittlungsverfahren ergibt. Dies gilt freilich nur im Rahmen der üblichen Schranken, die insbesondere in strafprozessualer Hinsicht auch dem Schutz des Betroffenen dienen. S. dazu auch mit weiteren Nachweisen Hornung/Gooble, CR 2015, 265 (268).

378 Siehe hierzu beispielhaft den Kauf des Kartendienstes „Here“ durch Audi, BMW und Mercedes im Jahr 2015, der als offene Plattform betrieben werden soll.

sogar bis hin zum *Open-Source*-Gedanken reichen. In diesem Kontext zeigt die sog. „Linux-Klausel“³⁷⁹ in § 32 Abs. 3 S. 3 UrhG, die einen Verzicht auf eine Vergütung vorsieht, eine mögliche Handlungsalternative des Gesetzgebers auf, um neue Formen der Zusammenarbeit zu ermöglichen. Durch die unentgeltliche Einräumung von Nutzungsrechten wiederum besteht die Möglichkeit, neues wirtschaftliches Potential zu entwickeln sowie kreative Ideen auch außerhalb des eigenen Unternehmen zu nutzen. Daneben besteht jedoch auch eine Parallele zum Wettbewerbsrecht, namentlich in Form von Zwangslizenzen, so wie z. B. der Zugang für kleine Werkstätten gegenüber dem Hersteller im europäischen Recht³⁸⁰.

Gegen einen *Open-Data*- bzw. *Open-Innovation*-Ansatz spricht jedoch, dass der Wert von Daten vielfach darin besteht, dass diese nicht für jedermann zur Verfügung stehen, sondern eine exklusive Nutzung erlauben. Daher könnte aus ökonomischer Perspektive ein übertragbares Ausschließlichkeitsrecht an Daten einen größeren gesamtgesellschaftlichen Mehrwert mit sich bringen.

Unter Berücksichtigung des eher geringen gesetzgeberischen Aufwandes im Verhältnis zur Schaffung eines absoluten Zuordnungsrechts, wäre es jedoch insgesamt **begrüßenswert**, wenn die Anreizsysteme für ein *Open-Data*-System, die rechtlichen Voraussetzungen, z. B. für offene und standardisierte Schnittstellen, sowie Vorgaben für die Form und Portabilität der Daten und für einen einheitlichen Datenmarktplatz geschaffen werden würden. Eine solche Lösung soll jedoch nicht als alleiniges Regelungs-

instrument in Bezug auf den Handel mit Daten gesehen werden, sondern vielmehr als eine mögliche Option neben anderen. Vielmehr würde sie einen Ausgangspunkt darstellen, der der Wirtschaft Raum für eigene, freiwillig und vertraglich fixierte *Open-Data*- und *Open-Innovation*-Systeme geben würde; wie bspw. schon im Rahmen der Schutzrechte durch verschiedenen Lizenzen im Rahmen von *Creative Commons* geschehen.

5.2.7 Zwischenergebnis

Nach Abwägung des Für und Wider der verschiedenen Handlungsalternativen, werden verschiedene Maßnahmen als empfehlenswert betrachtet. Die Schaffung eines **verbesserten Integritätsschutzes** durch Schaffung der vorgeschlagenen Vorschrift erscheint empfehlenswert, da der Befund einer entsprechenden Schutzlücke weitestgehend anerkannt ist. Hier wird insoweit ein konkreter Lösungsvorschlag unterbreitet, um die Schutzlücke zu schließen. Deutlich wurde, dass auch für eine entsprechende Regelung die Bestimmung des Verfügungsberechtigten der Daten erforderlich ist und insoweit auf den bereits im Rahmen des Ausschließlichkeitsrechts entwickelten Ansatz zurückgegriffen werden kann. Als gangbarer Weg der genannten Handlungsalternativen erscheint es daher, neben anderen langfristig zu beobachtenden Möglichkeiten, als kurzfristige Maßnahme den Integritätsschutz unter Zugrundelegung des entwickelten Ansatzes zu verbessern. Für nicht-personenbezogene Daten sollte daneben die **Förderung von Open Data** gestärkt werden.

379 Die Linux-Klausel gibt dem Schöpfer eines Werkes das Recht, zugunsten der Allgemeinheit auf eine finanzielle Vergütung zu verzichten und soll so die Gültigkeit von Lizenzen freier Software und anderer Medien sicherstellen (siehe § 32 Abs. 3 S. 3 UrhG: „Der Urheber kann aber unentgeltlich ein einfaches Nutzungsrecht für jedermann einräumen.“).

380 Euro-5/6-Verordnungen, Kapitel III der Verordnung (EG) 715/2007 vom 20.06.2007; s. dazu bereits auch Roßnagel, Wem gehören die Daten im Fahrzeug? - Grundlegende Rechtsverhältnisse und Ansprüche, 52. Deutscher Verkehrsgerichtstag, Köln 2014, 257 (272 ff.).

6 Exkurs: Übertragbarkeit auf andere Gebiete: Beispiel Gesundheitsdaten

Die in der vorliegenden Studie entwickelten Konzepte sollen anhand eines anderen Datenbereichs hinsichtlich ihrer Übertragbarkeit validiert werden. Persönliche Gesundheitsdaten bieten sich dazu an, da diese in der Regel als personenbezogene Daten einen hohen Grad an Schutz erfordern, andererseits aber für verschiedene Marktakteure, z. B. aus der Gesundheitsindustrie, einen hohen Wert haben können.

Gesundheitsdaten können auf vielfältige Art entstehen, bspw. in Folge von ärztlichen Untersuchungen oder durch das Tragen eines **Fitnesstrackers**, einer **Smart Watch** oder einer **Pulsuhr** beim Sport. Die Daten können anschließend auf vielfältige Weise genutzt werden, sowohl im Rahmen der Verbesserung der persönlichen Fitness als auch, nach geeigneter Pseudonymisierung oder Anonymisierung, für wissenschaftliche Forschung oder zur Nutzung bei der Entwicklung von Medikamenten. Insbesondere im Fall des persönlichen *Trackings* gibt es Parallelen zum Fall der Mobilitätsdaten. Eine Investition in einen Gegenstand (hier bspw. in eine *Smart Watch*) und die Nutzung desselben führt dazu, dass ein kontinuierlicher Datenstrom entsteht, der entweder zwischengespeichert oder auf eine zentrale Plattform geleitet wird. In der Regel handelt es sich nicht um ein explizites *Opt-in*, sondern die Datennutzung wird im Rahmen von allgemeinen Geschäftsbedingungen ermöglicht. Für den Nutzer gibt es nur wenig Transparenz dazu, welche Daten übertragen werden – sofern er sich der Tatsache an sich überhaupt bewusst ist. Die Daten besitzen einen ausreichenden Wert (denn sonst würden sie nicht erfasst werden). Und der Kunde wird für die Bereitstellung nicht explizit kompensiert.

Die Konzepte bzw. Lösungsansätze, die im ökonomischen Kapitel vorgestellt worden sind, lassen sich auf den Fall der Gesundheitsdaten übertragen. Datensouveränität würde dazu führen, dass den Kunden der Wert ihrer Daten explizit bewusst würde und die erste Verfügungsgewalt über die Daten klar ihnen zugewiesen wäre. Ein **Markt für Gesundheitsdaten** würde wie im Fall der Mobilitätsdaten unter anderem dazu führen, dass die Daten, sofern bereitgestellt, einer breiten Nachnutzung zugänglich wären und über eine Kompensation eine verstärkte Bereitstellung erreicht werden könnte. Ein klares regulatives Umfeld schließlich würde durch vergrößerte Rechtssicherheit die wirtschaftliche Nachnutzung vereinfachen.

Eine Anwendung des hier entwickelten Zuordnungsansatzes kommt auch beim Beispiel der Gesundheitsdaten zu sachgerechten Ergebnissen. So führt die entworfene Zuordnungsentscheidung (Zuordnung an den wirtschaftlich Berechtigten) dazu, dass bspw. der **Nutzer** einer *Smart Watch* als **Verfügungsberechtigter** der entstehenden Daten

anzusehen ist. Er ist bei wirtschaftlicher Betrachtungsweise für die Erstellung der Daten verantwortlich. Ähnlich wie bei einem Fahrzeug ist die Investition des Herstellers in den datengenerierenden Gegenstand bereits mit Zahlung des Kaufpreises abgegolten. Zudem fallen nur dann überhaupt Daten an, wenn die Uhr tatsächlich genutzt wird, sodass der Nutzer die Datengenerierung hauptsächlich initiiert. Auch wenn der Aspekt der wirtschaftlichen Unterhaltungskosten bei einer *Smart Watch* nicht so stark ins Gewicht fällt wie bei Fahrzeugen, gilt auch hier, dass derjenige, der die Kosten für die wirtschaftliche Unterhaltung, wie bspw. Wartungs- und Reparaturkosten trägt, als Verfügungsberechtigter der Daten anzusehen ist. Dies wird in der Regel der Eigentümer der Uhr sein, wobei dies nicht zwingend ist.

Im Bereich von speziellen **Medizinprodukten** sind indes auch andere Ergebnisse denkbar. So existieren bspw. vermehrt Geräte, die Patienten kostenlos zur Verfügung gestellt werden und die bestimmte Gesundheitsdaten regelmäßig an den behandelnden Arzt übermitteln³⁸¹. Vorteil ist, dass der Patient den Arzt nicht persönlich aufsuchen muss. Die Daten werden bei diesen Modellen meist dezentral gesammelt, aber zentral, bspw. auf einem Server des Krankenhauses oder eines IT-Dienstleisters, gespeichert. Die Anwendung des oben entwickelten Zuordnungsansatzes führt dazu, dass in derartigen Fällen nicht der Patient als Verfügungsberechtigter der Daten anzusehen ist. Er hat aufgrund des kostenlosen Zurverfügungstellens keine Investition in den datengenerierenden Gegenstand getätigt und ist auch nicht der wirtschaftlich Verantwortliche für das Gerät. Dies wird vielmehr derjenige sein, der das jeweilige Gerät unterhält und an die Patienten verleiht.

Bei diesem Beispiel wird jedoch besonders deutlich, dass durch die reine Zuordnungsentscheidung noch keine Aussage über die damit verbundenen Befugnisse und Schranken getroffen ist. Vor allem Gesundheitsdaten gelten unter datenschutzrechtlichen Aspekten als besonders **sensibel**³⁸². Insoweit hat der Verfügungsberechtigte daher stets die durch das **Datenschutzrecht** aufgestellten „Belastungen“ bei der Weiterverwendung der erhobenen Daten zu beachten. Anders gestaltet sich dies nur dann, wenn der Personenbezug bei der Weiterverwendung durch entsprechende technische Maßnahmen – wie etwa der vollständigen Anonymisierung bzw. Pseudonymisierung – entfernt wird. Besonders an diesem Beispiel zeigt sich aber auch, dass eine Zuordnung der Daten zum datenschutzrechtlich Betroffenen zu keinem sachgerechten Ergebnis kommen würde, da der bloße Personenbezug nicht zwangsläufig dazu führt, den Betroffenen auch als wirtschaftlich Verantwortlichen anzusehen. Dies gilt insbesondere, wenn die Daten erst durch eine nachfolgende Weiterverarbeitung einen wirtschaftlichen Wert erhalten.

381 Siehe etwa: <http://www.golem.de/news/healthkit-immer-mehr-krankenhaeuser-nutzen-apples-gesundheits-app-1502-112175.html>.

382 Vgl. dazu etwa *Ortner/Daubenbüchel*, NJW 2016, 2918 ff.; *Wilmer*, K&R 2016, 382 ff.; *Becker/Schwab*, ZD 2015, 151 ff.; *Weichert*, DuD 2013, 251 ff.

7 Handlungsempfehlungen



Abbildung 31: Umsetzungshorizont der Handlungsempfehlungen

Vor dem Hintergrund, dass keine abschließende Abwägung der Vor- und Nachteile der Kodifizierung eines ausschließlichen Verfügungsrechts an Daten erfolgen kann (siehe Kapitel 5.1.3.), ist alternativ auch ein Vorgehen basierend auf verschiedenen rechtlichen und außerrechtlichen Maßnahmen mit **kurz-, mittel- und langfristigem Umsetzungshorizont** in Betracht zu ziehen (Abbildung 31). Diese Maßnahmen verfolgen das Ziel, bestehende Regelungen an die Anforderungen der Datenökonomie anzupassen und so geeignete Rahmenbedingungen für die Erschließung des ökonomischen Potenzials von Mobilitätsdaten zu schaffen.

Während einige Maßnahmen bereits kurzfristig die Erschließung weitergehender ökonomischer Potenziale und die Schließung offenkundiger Schutzlücken ermöglichen, sollten auch Maßnahmen mit naturgemäß längerfristigem Umsetzungshorizont – wie die Förderung von *Open Data* (Kapitel 7.4), die Sensibilisierung für Daten als marktfähiges Gut (Kapitel 7.5) und die Konsolidierung datenbezogener Regelungen (Kapitel 7.6) – frühzeitig angestoßen werden.

Die verschiedenen rechtlichen Empfehlungen (siehe Kapitel 7.1, 7.3) können für sich stehen, aber auch zusammen mit weiteren Regelungen in ein ganzheitliches Gesetzesvorhaben zur möglichen Schaffung eines „Datengesetzes“ einfließen (siehe Kapitel 7.6).

7.1 Gezielte Schließung von Schutzlücken

Wie gezeigt wurde ist der Integritätsschutz von Daten derzeit unzureichend und sollte daher zeitnah verbessert werden. Dies ist insbesondere bei in der Cloud gespeicherten Daten geboten, da das geltende allgemeine Deliktsrecht (§§ 823 ff. BGB) Daten unzureichend vor fahrlässigen Beeinträchtigungen durch Dritte schützt³⁸³. Ein **verbesserter Integritätsschutz** von Daten, die nicht auf eigenen Datenträgern gespeichert sind, würde das Vertrauen von Unternehmen stärken, künftig noch mehr Datenverarbeitungsvorgänge in die **Cloud** auszulagern. Unternehmen könnten durch entsprechende Outsourcing-Maßnahmen Geschäftsprozesse effektiver gestalten und damit ihre Wettbewerbsfähigkeit steigern. Zudem würde die Nachfrage nach *Cloud*-Lösungen wachsen, was neue Investitionsanreize auf Seiten der Anbieter dieser Zukunftstechnologie schaffen würde. Um den Schutz der Integrität von Daten zu verbessern, sollte die **Einführung einer eigenen Haftungs-norm** erwogen werden (siehe Kapitel 5.2.5 (Normvorschlag § 823a BGB-Entwurf)). Diese könnte in das allgemeine Deliktsrecht oder ein neu zu schaffendes „Datengesetz“³⁸⁴ eingefügt werden. Der geschützte Personenkreis sollte auf Grundlage der hier entwickelten Zuordnungsentscheidung³⁸⁵ definiert werden.

383 Siehe Kapitel 5.2.5.

384 Siehe Kapitel 7.6.

385 Siehe Kapitel 5.1.

7.2 Förderung eines einheitlichen Markts für Daten durch Standardisierung

Weiter sollte ein einheitlicher Markt für Daten durch eine Standardisierung gefördert werden. Standardisierung in einem Markt hat grundsätzlich zur Folge, dass Transaktionen erheblich vereinfacht werden, da der Aufwand für die Marktteilnehmer sinkt³⁸⁶. Aufbauend auf der vorangegangenen ökonomischen Analyse sind im Fall von Mobilitätsdaten zwei voneinander unabhängige und damit komplementäre Ansätze sinnvoll:

- **Schaffung standardisierter Informationen über die Datenerhebung und -weiterleitung bei der Fahrzeugnutzung:** Fahrzeugnutzer wissen oft nicht, welche Informationen aus dem Fahrzeug weitergegeben werden – es besteht zurzeit eine Informationsasymmetrie zwischen Nutzer und Fahrzeughersteller. Wird davon ausgegangen, dass Intransparenz einer der Gründe für die geringe Bereitschaft zur Datenweitergabe ist, kann eine verbesserte **Transparenz** Datenschutzbedenken verringern und so, auch im Interesse der Fahrzeughersteller, für eine höhere Bereitschaft zur Datenweitergabe sorgen. Die Form der Information sollte verbraucherfreundlich (d. h. so klar wie möglich) und insbesondere in der Form einheitlich über die Fahrzeughersteller sein. Das BMVI könnte einen Prozess zusammen mit der Automobilindustrie initiieren, in dem die Informationen für einen solchen „**Daten-Ausweis**“, d. h. Umfang und Ausprägung der Datenerhebung und -weiterleitung, strukturiert werden. Die Bereitstellung dieser Informationen könnte ggf. – unterstützt durch eine regulative bzw. gesetzliche Maßnahme – verpflichtend sein. Geeignete Elemente eines solchen Daten-Ausweises könnten sein: die Art der erhobenen Daten (z. B. Kategorien wie Motordaten, Positionsdaten, Daten des *Entertainment*-Systems, Umweltdaten), Erhebungs- und Speicherungsintervalle, Häufigkeit bzw. Anlass der Datenweitergabe (z. B. in Echtzeit oder bei Werkstattbesuch), bestehender oder nicht bestehender Personenbezug und ggf. der Name der Standardlizenz (siehe den nächsten Punkt), unter der die Weitergabe erfolgt.

- **Entwicklung von Standardlizenzen für Mobilitätsdaten:** Entscheidend für die wirtschaftliche Verwertung von Daten ist, in welcher Form diese erhoben, genutzt und weitergegeben werden dürfen. Es bietet sich an, für bestimmte Datenkategorien **Standardlizenzen und Standardnutzungsrechte** zu entwickeln, die den Austausch von Daten vereinfachen. Somit könnten nicht nur unter Umständen mehrere Personen oder Stellen die Daten nutzen, sondern auch eine abgestufte Berechtigung zur ihrer Nutzung ist denkbar. Leitidee ist dabei die optimale wirtschaftliche Ausnutzung unter Berücksichtigung der unterschiedlichen (wirtschaftlichen) Potentiale der Daten, die durch eine differenzierte Betrachtung, die insbesondere auch Dritte mit einbezieht, geprägt ist. Das BMVI könnte im ersten Schritt als Organisator eines runden Tisches mit Akteuren aus den relevanten Wirtschaftszweigen und Institutionen (z. B. Automobilhersteller, unternehmerische Datennachnutzer, Zivilgesellschaft) agieren. Die Teilnehmer würden zunächst **Eckpunkte** für standardisierte Nutzungslizenzen erarbeiten. Entscheidend ist hier, dass der Teilnehmerkreis deutlich über die Automobilindustrie hinausgeht, um das gesamte Wertschöpfungsnetzwerk zu erfassen. Standardlizenzen dürften auch den Effekt haben, dass die **Markterschließung vereinfacht** wird. Im zweiten Schritt sind mögliche Konflikte durch Schrankenregelungen, insbesondere aus dem Bereich des Datenschutzrechts, aufzulösen. Geeignete Dimensionen, die in derartigen Standardlizenzen berücksichtigt werden könnten, sind: Art der genutzten Daten (Datenkategorien) entlang eines einheitlichen Katalogs (siehe den vorhergehenden Punkt zu standardisierten Informationen), erlaubte/nicht erlaubte Sekundärnutzung, entgeltliche/nicht entgeltliche Weitergabe, Nutzung nur mit oder auch ohne Anonymisierung/Pseudonymisierung, maximale Dauer der Nutzung bzw. Möglichkeit oder Ausschluss des Widerrufs der Datennutzung, erlaubte/nicht erlaubte Nutzung in Kombination mit Daten aus anderen Quellen, ggf. Einschränkung der Domänen für die Nutzung (z. B. Produktverbesserungen, Produktangebote, Verbesserung der Verkehrssituation). Es ist denkbar, entlang ausgewählter Dimensionen ein „Baukastensystem“ mit geeigneten Kombinationsmöglichkeiten zu etablieren. Ein Vorbild für ein solches Vorgehen sind die Standard-Lizenzverträge der Organisation „Creative Commons“ für die Verbreitung kreativer Inhalte.

386 Siehe Kapitel 4.2.3.

7.3 Abbau von Schranken für Data-Mining- und Big Data-Anwendungen

Unabhängig von der Schaffung eines Ausschließlichkeitsrechts an Daten³⁸⁷, besteht der Befund, dass **Schutzrechte Dritter** heute die Nutzung von Daten im Rahmen innovativer datenverarbeitender Systeme **vor neuen Herausforderungen stellen**³⁸⁸. Dies betrifft derzeit exemplarisch *Big-Data*- und *Data-Mining*-Anwendungen. Daher sollten politische Initiativen unterstützt werden, die ausloten, welche bestehenden Schutzrechte künftig zu Gunsten von *Big-Data*- und *Data-Mining*-Anwendungen³⁸⁹ stärker beschränkt werden können. Solche Systeme bieten ein enormes wissenschaftliches und ökonomisches Potenzial, das bislang nicht vollständig ausgeschöpft werden kann.

Zu diesem Zweck sollten entsprechende politische Initiativen auf EU-Ebene unterstützt werden: Für das **Urheberrecht** hat z. B. die EU-Kommission jüngst mit Art. 3 ihres Entwurfes einer Richtlinie über das Urheberrecht im digitalen Binnenmarkt (COM(2016) 593 final) eine solche Schranke zu Gunsten von *Data-Mining*-Anwendungen vorgeschlagen. Auch bei der laufenden Reform der nationalen urheberrechtlichen Schranken für Bildung und Wissenschaft werden solche Schranken diskutiert. In seinem Referentenentwurf für ein Gesetz zur Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft³⁹⁰ hat das *Bundesministerium der Justiz und für Verbraucherschutz* mit § 60d einen konkreten Entwurf formuliert.³⁹¹

Beispielhafte Maßnahmen diesbezüglich könnten die **Formulierung politischer Forderungen** ausgehend vom Mobilitätssektor, die Einbringung in die weiteren Initiativen der Europäischen Kommission sowie in die Arbeitsgruppen des Rates und in die (federführenden) Ausschüsse des EU-Parlamentes sowie das **Monitoring** des europäischen Gesetzgebungsverfahrens sein (z. B. Fristen, Beteiligungsmöglichkeiten).

7.4 Public Open Data als Standard definieren und Private Open Data fördern

Ergänzend könnte mit verhältnismäßig geringem Aufwand ein *Open Data System* etabliert werden. Hierbei ist zwischen **Public Open Data** und **Private Open Data** zu unterscheiden.

Der Ansatz von **Public Open Data** könnte als Standard definiert werden, um so eine Zweitverwertung von staatlich gewonnenen Daten, insbesondere aus der *Car-2-Infrastructure*, zu ermöglichen und damit die Wirtschaft zu fördern. Dafür müssen zuerst geeignete *Car-2-Infrastructure*-Daten, die offen bereitgestellt würden, identifiziert werden. Danach müssen rechtliche, technische und organisatorische Voraussetzungen für die Datenbereitstellung geschaffen werden. Die rechtlichen Voraussetzungen für die Datenbereitstellung würden vordergründig durch die Pflicht zur Weitergabe begründet. Dies geht mit einer Einschränkung der exklusiven Nutzungsrechte einher und kann auch die Offenlegung weiterer Informationen und Prozesse, die zur Einordnung der Daten unerlässlich sind, mit einbeziehen, soweit dem keine anderweitigen Interessen entgegenstehen. Des Weiteren ist im Rahmen dessen die Festlegung eines einheitlichen Datenformates und eines diskriminierungsfreien Zugangs bzw. von Schnittstellen erforderlich. Dies kann auch die rechtliche Pflicht zur Schaffung weiterer technischer bzw. IT-Infrastruktur umfassen, die den Zugang erst ermöglicht. Die Möglichkeit der Nutzung bestehender Standards sollte in diesem Zusammenhang geprüft werden. Anschließend muss ein **Datenmarktplatz** geschaffen werden, der Plattform für die Zurverfügungstellung der Daten sein kann, wobei hier u. U. auf bestehenden Marktplatzansätzen (z. B. Mobilitäts Daten Marktplatz (MDM), mCloud) aufgebaut werden kann³⁹². Darüber hinaus können weitere Anknüpfungspunkte z. B. im **Informationsfreiheitsgesetz**, im **Umweltinformationsgesetz** und im **Geodatenzugangsgesetz** gefunden werden. Schlussendlich ist im Anschluss auch denkbar, dass für Daten, die im öffentlichen Interesse liegen, eine Verpflichtung zur Weitergabe an staatliche Stellen geschaffen wird, die freilich dann auch im Sinne von *Open Data* ausgestaltet werden könnte.

387 Siehe Kapitel 5.1 sowie Handlungsempfehlung 7.6.

388 Dazu, welche Schutzrechte *de lege lata* Mobilitätsdaten erfassen, siehe Kapitel 3.

389 *Data-Mining* bezeichnet die Analyse großer Datensätze mit dem Ziel, für Entscheidungsträger relevante Muster und Zusammenhänge aufzudecken. Durch die Filterung, Extraktion und Aggregation von Daten können aus der Untersuchung großer Datenbestände unternehmensrelevante Erkenntnisse gewonnen werden.

390 Abrufbar unter http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_UrhWissG.pdf.

391 In der Literatur lassen sich vergleichbare Entwürfe finden, so z. B. Schack, ZUM 2016, 266 (268 f.).

392 Siehe dazu bereits bestehende Ansätze, wie zum Beispiel den „Mobilitäts Daten Marktplatz“ (MDM) und die mCloud, <http://mcloud.de/>.

Im Bereich von **Private Open Data** hingegen ist keine verpflichtende Normierung anzustreben, sondern vielmehr die Etablierung eines **Anreiz- und Förderungssystems**, welches durch kooperative Elemente die Innovationskraft der Wirtschaft steigert. Anreize und Förderungen können durch die Schaffung von einheitlichen Standards und rechtlichen Marktbedingungen und -schränken geschaffen werden, die diesen Ansatz abbilden (Stichwort: Linux-Klausel). Im Rahmen dessen können Private (insbesondere Hersteller, Zulieferer, Plattform- sowie Diensteanbieter) Daten anderen Akteuren als *Open Data* zur Verfügung stellen. Voraussetzung ist jedoch stets, dass keine Schranken entgegenstehen. In Betracht kommt daher vor allem die Verwendung von anonymisierten und pseudonymisierten Daten. Hierbei handelt es sich insbesondere um Rohdaten, die durch Fahrzeuge „produziert“ wurden.

Aufgabe des Staates ist es dabei, die **rechtlichen Ausgangs- und Rahmenbedingungen** zu schaffen, damit die Wirtschaft im zweiten Schritt eigene, freiwillige und vertraglich fixierte Modelle entwickeln kann. Dafür müssten insbesondere Standards für offene und standardisierte Schnittstellen durch den Gesetzgeber gefunden werden, die die Zugangsvoraussetzungen und Nutzungsbedingungen normieren. In Betracht kommen insbesondere die Öffnung von Multimediaplattformen und die Etablierung von Lizenzierungsmodellen für das einzelne Datum, soweit eine Selbstverpflichtung der beteiligten Akteure nicht erreicht werden kann. Anknüpfungspunkte hierfür bestehen bereits im Wettbewerbsrecht sowie im Urhebergesetz, wobei der Übergang von *Open Data* zu *Open Innovation* als fließend betrachtet werden kann. Dies setzt als Ausgangsbasis zunächst einen **Dialog mit den involvierten Akteuren** voraus. Im Rahmen dessen soll einerseits der Bedarf nach einer Regelung herausgefiltert und andererseits die rechtlich wünschenswerten Bedingungen festgestellt werden. Dazu sollte eine **Sensibilisierung und Motivation** der Wirtschaft erfolgen.

7.5 Förderung des Bewusstseins für die Einordnung von Daten als marktfähiges Gut

Ferner sollte im allgemeinen Bewusstsein der Bevölkerung die Eigenschaft von Daten als ökonomisch handelbares Gut nachhaltig verankert werden. Dies ist eine langfristige, **generationenübergreifende Aufgabe**, die jedoch kurzfris-

tig angestoßen werden sollte. Sie ist zentral, da die Dienste der Informationstechnik immer tiefer in unsere Lebensbereiche eindringen und immer mehr Daten produzieren. Daten werden daher noch stärker in den Mittelpunkt zahlloser Geschäftsmodelle rücken und auch der „Austausch“ von Daten auf vertraglicher Grundlage wird zunehmen. Bislang begreifen jedoch vor allem Unternehmen Daten als werthaltiges Gut. Künftig sollten auch die Nutzer von Onlinediensten den ökonomischen Wert ihrer Daten besser verinnerlichen, damit sie privatautonom über deren Preisgabe entscheiden können. Dieses Bewusstsein ist einer der wesentlichen Schritte auf dem Weg hin zu einem **funktio-**
nierenden Markt für Daten, den alle Marktteilnehmer als fair akzeptieren.

Dieses Bewusstsein lässt sich vor allem durch die **Förderung transparenter Geschäftsmodelle** stärken. Die Datenschutz-Grundverordnung der EU leistet hierzu einen wertvollen Beitrag. Sie wird nicht verhindern, dass Nutzer als synallagmatische Gegenleistung ihre Daten für die Nutzung von Onlinediensten offenbaren. Anders als bisher müssen die Dienstleister diese Gegenleistung und deren Wert aber transparent machen. Sie können ihre Dienste daher nicht länger allgemein als „unentgeltlich“ oder gar „kostenlos“ offerieren. Das **Koppelungsverbot** wird sie stattdessen dazu zwingen, als Alternative zur Preisgabe von Daten, künftig ihre Dienste auch in einer Form anzubieten, bei der der Nutzer für den Dienst ein Entgelt zahlen kann, das dem Wert der Daten entspricht³⁹³. Das Verständnis von Daten als synallagmatische Gegenleistung hat auch vertragsrechtliche Konsequenzen. Die Einräumung von **„Rechten zur Datennutzung“** wäre nicht mehr nur die Nebenleistung eines – kostenlosen – Vertrages, sondern **Hauptleistungspflicht**. Damit würde die AGB-Kontrolle nicht mehr greifen und es würden andere, etablierte Mechanismen gelten (bspw. das Wucherverbot des § 138 Abs. 2 BGB). Hier ließen sich wiederum allgemeine **Leitlinien** formulieren, wann von einem angemessenen Entgelt in Form der „Übereignung“ von Daten ausgegangen werden könnte. Ein solcher Mechanismus könnte auch dem bisherigen „Alles-oder-nichts-Prinzip“ in vielen Bereichen entgegenwirken, da dabei vielfach – je nach Dienst – Leistung und Gegenleistung in keinem angemessenen Verhältnis mehr stehen dürften. Granulare Einwilligungen zur Datenerhebung und -verwendung würden sicherstellen, dass es nicht zu unbilligen Nachteilen eines Vertragspartners kommt.

Daneben können schulische und andere **Bildungs- und Aufklärungsinitiativen** einen wichtigen Beitrag zur Förderung dieses Bewusstseins leisten. So könnten Aufklärungs-

393 Dazu ausführlich Buchner, DuD 2016, 155 (158 f.); Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 3 Rn. 44.

maßnahmen zum Thema „Datenschutz durch Medienkompetenz“ dazu beitragen, dass Nutzer ein Verständnis des wirtschaftlichen Werts ihrer Daten entwickeln und den bewussten Umgang mit personenbezogenen Daten erlernen³⁹⁴. Das synallagmatische Verhältnis zwischen dem Recht zur Datennutzung und der Nutzung von bislang scheinbar kostenlosen Onlinediensten sollten diese Initiativen stärker in den Vordergrund rücken. Auch in der politischen Diskussion bestehen – offensichtlich geprägt durch die primär datenschutzrechtliche Sichtweise auf Daten – in Deutschland Hemmnisse, derartige Vorgänge als „normale“ Austauschvorgänge einzuordnen. Die strikte Trennung von ökonomischer Verwertung von (auch personenbezogenen) Daten und dem Persönlichkeitsschutz dürfte hier zielführend sein.

Letztlich muss die, jedenfalls aus der EU-Datenschutz-Grundverordnung folgende, Verpflichtung von Unternehmen, alternative Bezahlung anstelle der Bezahlung mit Daten anzubieten, durch geeignete Maßnahmen durchgesetzt werden. **Anreizsysteme**, wie z. B. Bekanntmachungen sowie die Schaffung von Zertifikaten, die den Unternehmen datenschutzkonforme Verhaltensweisen bescheinigen und Wettbewerbsvorteile darstellen können, können diesbezüglich zielführend sein. Ziel solcher Maßnahmen ist es nicht nur, ein Alternativangebot zu schaffen – das ggf. ohnehin nicht viele Personen nutzen –, sondern die Förderung des allgemeinen Bewusstseins, dass auch Daten ein Handelsgut und ein Entgelt darstellen. Zudem kann es dazu dienen, Anhaltspunkte dafür zu erhalten, welchen Wert bestimmte Dienstleistungen (Speichern in der Cloud, Suchanfragen, Vernetzung im Privaten wie Beruflichen), die heute „kostenlos“ angeboten werden, und die zur Nutzung freigegebenen Daten haben. Dies ermöglicht Vergleichbarkeit und die Herausbildung von Angebot und Nachfrage im Sinne eines funktionierenden Marktes.

7.6 Konsolidierung datenbezogener Regelungen und Zusammenführung in einem „Datengesetz“

Die Analyse des geltenden Rechts hat gezeigt, dass Daten derzeit vor allem durch bereichsspezifische Regelungen

geschützt werden. Diese Regeln weisen jedoch unterschiedliche Voraussetzungen, Rechtsfolgen und Zuordnungsentscheidungen auf, sodass keine homogene Rechtsposition an Daten besteht (siehe Kapitel 3)³⁹⁵. Dieser „Flickenteppich“ hemmt die Verwertung von Mobilitätsdaten und verhindert, dass deren ökonomisches Potenzial vollständig ausgeschöpft wird. Hinzu kommt, dass an Stelle der rechtlichen Zuordnung derzeit die faktischen Zugriffsmöglichkeiten auf die Dateninfrastruktur darüber entscheiden, ob und von wem Daten genutzt werden können.³⁹⁶

Um diese Hürden zu beseitigen, sollte der Gesetzgeber die datenbezogenen Normen stärker aufeinander abstimmen. Dieser Prozess sollte kurzfristig durch ein **Normenscreening** angestoßen werden, um zu klären, welche Regelungsbereiche betroffen sind und welche Konflikte diese auslösen³⁹⁷. Ausgehend von den Ergebnissen des Normenscreenings sollte ein konsistenterer Rahmen für eine funktionierende Datenökonomie geschaffen werden. Langfristig könnte so ein „**Datengesetz**“ mit rechtsgebietsübergreifenden Normen geschaffen werden. Dieses wäre nach derzeitigem Erkenntnisstand als Artikelgesetz mit bereichsspezifischen Regelungen zu gestalten. Dieses Vorhaben sollte der Gesetzgeber zugleich zum Anlass nehmen und Maßnahmen umsetzen, die zwar nicht die Verwertung von Daten fördern, insgesamt aber den rechtlichen Rahmen der Datenökonomie verbessern (siehe z. B. Kapitel 7.1 und 7.3). Die in einem „Datengesetz“ zu behandelnden Elemente und Themenfelder werden im Folgenden exemplarisch herausgearbeitet. Hierzu zählen u. a. der Ausbau des deliktischen Integritätsschutzes von Daten³⁹⁸ und die Anpassungen der schuldrechtlichen Regeln, um die Vorgaben aus der kommenden „Digitale Inhalte-RL“ der EU umzusetzen³⁹⁹.

7.6.1 Festlegung eines Zuordnungsansatzes

Im Rahmen eines solchen Vorhabens sollte der Gesetzgeber erwägen, bei datenbezogenen Rechten für eine einheitliche Zuordnung zu sorgen. Durch eine homogene Zuordnungsentscheidung würden die jeweiligen Rechte in den Händen weniger Personen entstehen, sodass die Beteiligten einfacher und kostengünstiger die nötigen Nutzungsrechte erwerben könnten. Die Zuordnung **zum wirtschaftlichen Berechtigten** erweist sich jedenfalls für den Mobilitätssektor als zweckdienlich (siehe Kapitel 5.1.2.4). Der Gesetzgeber sollte einen einheitlichen Zuordnungsansatz wählen, den er bei künftigen Schutzrechten mit Datenbezug zu Grun-

394 Siehe hierzu m. w. Nachw. Jöns, Daten als Handelsware, S. 64.

395 Siehe Kapitel 3.2.6.

396 Siehe Kapitel 3.3.

397 Bezogen auf die in dieser Studie exemplarisch betrachteten Fallstudien (siehe Kapitel 3.2).

398 Siehe Kapitel 5.2.5 sowie 7.6.6.

399 Siehe Kapitel 7.6.5.

de legen kann, soweit deren Regelungszwecke mit dieser Zuordnung korrespondieren. Dies gilt etwa bei dem zu diskutierenden Leistungsschutzrecht für maschinen-generierte Daten⁴⁰⁰ oder einer neu zu schaffenden deliktischen Haftungsnorm für Schäden an Daten⁴⁰¹. Daneben könnte der Gesetzgeber mit Hilfe der einheitlichen Zuordnungsentscheidung direkt oder mittelbar das geltende Recht harmonisieren. Wo es bspw. an einer ausdrücklichen Normierung fehlt (z. B. im Strafrecht) könnte er eine Klarstellung erwägen.

7.6.2 Schaffung der nötigen Schrankenbestimmungen

Die Analyse hat gezeigt, dass zahlreiche Rechte Dritter bestehen (sog. 2. Ebene (siehe Kapitel 3)). Auch das vorgeschlagene Ausschließlichkeitsrecht an Daten wäre mit den gezeigten Rechten „belastet“. Aufgrund dieser verschiedenen Rechtspositionen können die beteiligten Akteure bereits heute im Einzelfall nur selten rechtssicher abschätzen, ob sie Daten verwerten dürfen. Diese Rechtsunsicherheit hemmt die Entwicklung neuer Angebote und lässt die Transaktionskosten von Innovatoren wachsen.

Um diese Situation bei Schaffung eines Ausschließlichkeitsrechts zu verbessern, sollte der Gesetzgeber prüfen, inwieweit er seinen Gestaltungsspielraum nutzen kann, um vorbestehende Rechte durch **Schrankenbestimmungen** zu begrenzen. Dies betrifft vor allem das Urheberrecht.⁴⁰²

Wie aufgezeigt⁴⁰³ kollidieren diverse bereichsspezifische Regelungen Daten betreffend derart miteinander, dass sie Zuordnungen zu Rechtssubjekten nach unterschiedlichen Mechanismen treffen (siehe Kapitel 3.2.6). Wünschenswert wäre die Schaffung von Normen, die das Verhältnis unterschiedlicher Rechte diverser Akteure an Daten regeln. § 28 Abs. 1 Nr. 2 BDSG stellt bspw. eine Norm dar, die eine Aussage hinsichtlich des Verhältnisses der datenschutzrechtlichen Ansprüche des Betroffenen zu dem Recht auf Erhebung, Speicherung und Nutzung personenbezogener Daten durch wirtschaftliche Akteure zu eigenen Geschäftszwecken trifft. In diesem Fall ist die Datenverarbeitung durch die verantwortliche Stelle grundsätzlich zulässig, sofern nicht schutzwürdige Interessen des Betroffenen überwie-

gen. Etliche Kollisionsregeln, die die Datennutzung betreffen, werden abwägungs offen ausgestaltet werden müssen, um eine flexible Handhabung in der Praxis und Einzelfall-gerechtigkeit zu ermöglichen. Zu beachten ist ferner, dass diverse Schutzrechte auf europäischer Ebene bspw. in der DSGVO verankert und nicht einschränkbar sind – daher ist ihnen zwingend Vorrang vor anderen Nutzungsrechten einzuräumen. Bezogen auf Smart Cars können diverse Akteure wie der Eigentümer, der Besitzer, der Hersteller sowie der jeweilige Betroffene unterschiedlichste Rechte aus dem Sachenrecht, dem Urheberrecht und dem Datenschutzrecht herleiten, die im Falle konfligierender Nutzungsinteressen in ein angemessenes Rangverhältnis zueinander zu setzen sind⁴⁰⁴. Der Gesetzgeber sollte die bestehende Rechtsunsicherheit bezüglich der möglichen Verletzung vorrangiger Rechte Dritter durch die eigene Datennutzung beseitigen. Hierfür ist allerdings zunächst ein belastbares, allgemeines Rangverhältnis zwischen den Rechten an Daten zu entwickeln.

7.6.3 Anpassung der schuldrechtlichen Regeln an die digitale Welt

Das Datengesetz bietet ferner die Gelegenheit, das Schuldrecht stärker an die digitalen Wirklichkeiten anzupassen.

Bei modernen smarten Geräten gehen die Nutzer typischerweise nicht nur eine vertragliche Beziehung zu den Verkäufern der Hardware ein, sondern müssen zugleich eine Reihe weiterer Verträge mit dem Hersteller oder externen Diensteanbieter schließen, um die vernetzten Funktionen der Geräte zu nutzen. Diese besonderen Vertragsbeziehungen bestehen immer öfter auch im Mobilitätsbereich, so etwa beim Erwerb eines PKW mit integrierter Mobilitätsdienstplattform eines Drittanbieters.⁴⁰⁵ Ob das bestehende Vertragsrecht die **Interdependenzen der verschiedenen Verträge** ausreichend abbildet, wird bezweifelt.⁴⁰⁶ Hier sollte zum einen näher betrachtet werden, auf welchen Wegen (Eigengeschäft, Stellvertretung) diese vielschichtigen Vertragsbeziehungen in der Praxis geschlossen werden und welchem Recht sie unterliegen. Des Weiteren wäre zu prüfen, ob die §§ 158, 313, 314, 358 ff. BGB die gegenseitigen Abhängigkeiten der unterschiedlichen Verträge ausreichend berücksichtigen. Letztlich sollte durch diesen

400 Siehe dazu unter Kapitel 5.1.2.3.

401 Siehe dazu unter Kapitel 5.2.5 sowie 7.6.6.

402 Zu konkreten Entwürfen für solche Schranken siehe oben Kapitel 7.3.

403 Siehe unter Kapitel 3.3.

404 Heun/Assion, Internetrecht der Dinge, Vortrag im Rahmen der Telemedicus Sommerkonferenz 2015, Präsentation abrufbar unter: https://www.telemedicus.info/uploads/Heun_Assion_InternetrechtderDinge.pdf.

405 Siehe oben Fallstudie 3.

406 Wendehorst, NJW 2016, 2609 (2610).

Evaluationsprozess ein detaillierter Überblick über die bestehende Vertragspraxis im Mobilitätssektor entstehen. Dieser Übersicht wäre auch für die effektivere Nutzbarkeit von Daten ein Fortschritt. Auf dieser Grundlage ließe sich besser beurteilen, ob die beteiligten Akteure im Rahmen der Verträge die entsprechenden Lizenzen für die Nutzung der Mobilitätsdaten tatsächlich privatautonom regeln können und damit über die aus ökonomischer Sicht angestrebte Datensouveränität⁴⁰⁷ verfügen.⁴⁰⁸

Mit Blick auf die Integration verschiedener Anwendungen im smarten PKW rückt daneben die **Haftung für Verhalten anderer Akteure** stärker in den Vordergrund. Diese Fragen werden bislang vor allem mit Zurechnungsnormen (§ 278 BGB), der Erweiterung der vertraglichen Haftung (§ 311 Abs. 3 BGB) und deliktischen Haftungsgrundlagen (§ 831 BGB) beantwortet. Ob diese Vorschriften insbesondere die Endnutzer smarter Automobile ausreichend schützen, sollte näher geprüft werden. Des Weiteren wird diskutiert, ob die Gewährleistungsrechte der besonderen Schuldverhältnisse für digitale Produkte überarbeitet werden sollten. Auf der EU-Ebene werden derzeit spezifische **Gewährleistungsregeln** für digitale Dienste entwickelt. Die EU-Kommission hat hierzu den Entwurf einer „Digitale Inhalte RL“ vorgestellt⁴⁰⁹. Diesen Prozess sollte der deutsche Gesetzgeber begleiten und auf Kohärenz der kommenden Regeln mit dem bestehenden europäischen und nationalen Schuldrecht drängen.

Weitere Anpassungen des Schuldrechts sollte der Gesetzgeber zur **Förderung der Interoperabilität** der unterschiedlichen Plattformen und **Datenportabilität** erwägen. Diese Maßnahmen können einen wichtigen Beitrag leisten, um *Lock-in*-Effekte, eine für Kunden aufgrund hoher Wechselbarrieren und -kosten unvorteilhafte Bindung an Produkte und Services eines Anbieters, und die gezeigte faktische Herrschaftsmacht⁴¹⁰ über die Daten abzubauen. Die europäische Datenschutz-Grundverordnung weist mit Blick auf personenbezogene Daten hier in die richtige Richtung, da deren Art. 20 dem Betroffenen ein Recht auf Datenportabilität gewähren wird. Für die Beendigung und (vorzeitige) **Rückabwicklung von datenbezogenen Schuldverhältnissen** fehlen heute indes Regeln, die den Nutzern klare An-

sprüche auf Herausgabe nicht personenbezogener Daten in interoperablen Formaten verschaffen⁴¹¹.

Darüber hinaus sollte der Gesetzgeber prüfen, ob auch über das Vertragsrecht die Sicherheit der IT-Infrastruktur verbessert werden kann. Unter anderem haben die zahlreichen großflächigen Bot-Netz-Angriffe⁴¹² der letzten Monate gezeigt, dass die IT-Sicherheit sich von einem individuellen zu einem kollektiven Interesse wandelt. Bislang können Nutzer von IT-Geräten aber vom Hersteller weder aus den vertraglichen Nebenpflichten (§ 241 Abs. 2 BGB) noch aus dem kaufrechtlichen Mängelgewährleistungsrecht (§§ 434 ff. BGB) oder der Produkt- bzw. Produzentenhaftung Ansprüche auf laufende Updates herleiten. Entsprechende Rechte würden insgesamt die Integrität und Vertraulichkeit der im Alltag eingesetzten smarten Geräte erhöhen.

7.6.4 Konkretisierung von AGB-Vorgaben (§§ 305 ff. BGB)

Der Gesetzgeber sollte ferner im Rahmen des Datengesetzes prüfen, ob er die Vertragsparität für Nebenleistungspflichten im digitalen Umfeld verbessern kann (**Vertragskontrolle**). Dazu müssten zunächst typische Vertragskonstellationen mit einem digitalen Bezug typisiert werden, um einschlägige Konstellationen herauszufiltern, die durch ein Ungleichgewicht geprägt sind. Hierzu drängen sich dann im zweiten Schritt spezifische **AGB-Vorgaben** – nach Vorbild der §§ 305 ff. BGB – für „Verträge über Daten“ auf, die den schwächeren Vertragspartner im Ergebnis stärken sowie eine einseitige Vermachtung der Verhandlungsposition verhindern. Auf diese Weise könnten insbesondere Vertragsklauseln untersagt werden, die die Datensouveränität des Verfügungsberechtigten schwächen⁴¹³.

7.6.5 Anpassung der Verbraucherschutzvorschriften (§§ 312 ff. BGB: Informationspflichten, Widerrufsrechte)

Mit Hilfe des Datengesetzes sollte der Gesetzgeber ferner die **Transparenz bei datenbasierten Geschäftsmodel-**

407 Siehe oben Kapitel 4.3.1.

408 Bestehende Hindernisse können u.a. durch entsprechende AGB-rechtliche Klauselverbote (vgl. §§ 308, 309 BGB) abgebaut werden, dazu unten Kapitel 7.6.4.

409 Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 2015/0287 (COD).

410 Siehe bereits unter 3.3.

411 Faust, 71. DJT, Teil A S. 40 f.

412 Als Bot-Netz wird ein großer Zusammenschluss von mit Malware infizierten Computern bezeichnet.

413 Siehe dazu unter Kapitel 4.3.

len verbessern, da sie die Grundlage der Datensouveränität des Verfügungsberechtigten ist⁴¹⁴. Hierzu kann der Gesetzgeber z. B. spezielle Informationspflichten regeln, die insbesondere die Kategorien der verarbeiteten Daten abdecken (für Beispiele möglicher Informationen siehe die Handlungsempfehlung 7.2 zu Standardisierungen). Bei deren Gestaltung sollte einbezogen werden, dass bereits aus anderen Regelungsbereichen entsprechende Pflichten folgen (z. B. §§ 312a, 312d, 312i Abs. 1 Nr. 2, 491a Abs. 1, 675a, 675d BGB, Art. 13, 14 DSGVO, § 93 TKG). Für den Nutzer von IT-Diensten droht daher durch weitere Informationspflichten zunächst eine Informationsflut, die den Regelungszweck der Pflichten gefährdet. Gerade für kleine und mittelständische Anbieter von IT-Diensten – die ebenfalls Adressaten der Informationspflichten sein können – muss zudem überschaubar bleiben, welche Pflichten sie im Alltag erfüllen müssen. Zunächst sollte daher ein Normenscreening durchgeführt werden, um einen Überblick über die verschiedenen Informationspflichten bei IT-Diensten zu erhalten. Anschließend ist zu prüfen, ob die gewünschten Verbesserungen durch Anpassung der bestehenden oder Schaffung neuer Pflichten zu erreichen sind. Dabei sollte erwogen werden, ob die Dienste-Anbieter ihre Informationspflichten künftig auch durch Symbole oder Piktogramme erfüllen können, um die Informationen für den Nutzer verständlicher aufzubereiten. Nach Vorbild der Art. 246 ff. EGBGB sollte der Gesetzgeber zudem Muster schaffen, damit die Verpflichteten möglichst einfach und kostengünstig den Informationspflichten genügen können. Eine solche Standardisierung würde den Nutzern helfen, die Informationen zu erfassen und könnte beispielsweise eine Ausprägung des in Handlungsempfehlung 2 beschriebenen Datenausweises sein.

7.6.6 Verbesserung des Integritätsschutzes von Daten durch Schaffung einer eigenen Rechtsgrundlage

Um die dargestellte Schutzlücke beim Integritätsschutz zu verbessern, wäre in ein Datengesetz eine entsprechende Rechtsgrundlage aufzunehmen, soweit dies nicht bereits zuvor durch eine Einzelfalllösung geschehen ist⁴¹⁵.

7.7 Fazit und Auswirkungen der Handlungsempfehlungen auf die Fallstudien

Die Handlungsempfehlungen verdeutlichen, dass vor dem Hintergrund der Herausforderungen bei der Schaffung eines Ausschließlichkeitsrechts an Daten grundsätzlich zwei Vorgehensweisen vorstellbar sind, um die rechtlichen und ökonomischen Rahmenbedingungen für die Etablierung von Daten als Wirtschaftsgut zu schaffen.

Zum einen besteht die Möglichkeit eines sukzessiven Vorgehens, bei dem die empfohlenen rechtlichen sowie außerrechtlichen Maßnahmen (siehe Kapitel 7.1 bis 7.5) schrittweise vorangetrieben würden. Diese Maßnahmen könnten langfristig in ein Datengesetz einfließen. Eine solche Vorgehensweise birgt weniger Komplexität. Einzelne Maßnahmen wären schneller und zeitnäher realisierbar. Allerdings wären die Fortschritte auch punktueller.

Zum anderen könnte ein umfassendes „Datengesetzesvorhaben“ mit vorangeschaltetem Normenscreening (siehe Kapitel 7.6) angestoßen werden. Ein solches „Datengesetz“ verspricht durch die ganzheitliche Vorgehensweise mehr Homogenität und könnte viele der genannten Handlungsempfehlungen vereinen. Ein weiterer Vorteil besteht in der Möglichkeit, den Handlungsspielraum für einzelne Kompromisse im Rahmen des Gesamtvorhabens zu erhöhen. Dieses ambitionierte Vorgehen könnte zudem von einem politischen Momentum profitieren. Gleichzeitig wachsen die Komplexität dieses Ansatzes und die Heterogenität der in einem „Datengesetz“ behandelten Themen. Für eine zeitnahe Umsetzung der empfohlenen Maßnahmen stellen diese Gesichtspunkte eine besondere Herausforderung dar.

Zudem ist zu beachten, dass sowohl beim sukzessiven Vorgehen als auch im Rahmen eines umfassenden Datengesetzesvorhabens die normativen Fragestellungen einer Flankierung durch die in den außerrechtlichen Handlungsempfehlungen beschriebenen Maßnahmen bedarf (siehe Kapitel 7.2, 7.4, 7.5).

Vor diesem Hintergrund obliegt die Wahl zwischen einem sukzessiven Vorgehen oder dem Anstoßen eines ganzheitlichen „Datengesetzes“ letztendlich dem politischen Entscheidungsträger.

414 Siehe dazu unter 4.3.

415 Siehe dazu unter Kapitel 7.1.

Darüber hinaus führt die Kombination aus rechtlichen sowie außerrechtlichen Maßnahmen zu wesentlichen Verbesserungen bei der Nutzung von Mobilitätsdaten. So stellt die Einführung eines „Daten-Ausweises“ im Fahrzeug im Fall der Kfz-Instandhaltung (Fallstudie 1) eine wichtige Maßnahme dar, um bei dem – gemäß dem entwickelten Ansatz – wirtschaftlich Berechtigten (dem Eigentümer und Fahrer) Transparenz über die Art und den Umfang der Erhebung „seiner“ Daten zu schaffen. Die Entwicklung von Standardlizenzen für bestimmte Daten würde dem wirtschaftlichen Berechtigten die Möglichkeit verschaffen, anderen Marktspielern auf einfache Weise Standardnutzungsrechte für diese Daten zu erteilen und die Verwendung seiner Daten somit zu steuern. So könnte eine Situation geschaffen werden, in der der Nutzer bzw. Eigentümer/Fahrer die Verwendung seiner Daten souverän steuern und – je nach Ausgestaltung – an dem wirtschaftlichen Mehrwert partizipieren könnte, während der Hersteller die erhobenen Daten unter klaren rechtlichen Bedingungen für seine Zwecke nutzen dürfte. Ähnliche Möglichkeiten ergeben sich beispielsweise auch in Fallstudie 4 zwischen dem Nutzer des Mobilitätsdienstes (wirtschaftlich Berechtigter) und dem Mobilitätsdiensteanbieter. Die Ausgestaltung kann dabei von einer verpflichtenden Bereitstellung hin zu abgestuften Nutzungsberechtigungen reichen. In beiden Fällen ist die Stärkung des Bewusstseins, dass Daten

ein wirtschaftliches Gut sind, unabdinglich für die Etablierung des skizzierten Systems.

Auch in Hinblick auf die in Fallstudie 5 erhobenen *Car-2-Infrastructure*-Daten kann die Forcierung des empfohlenen *Open-Data*-Ansatzes zu wesentlichen Verbesserungen bei der Nutzung der erhobenen Daten führen. So sind neben der Optimierung der Verkehrssteuerung auf Basis eines größeren Datensatzes auch weitergehende ökonomische Potenziale durch eine bessere Zweitverwertung der Daten durch Private zu erwarten. Neben der Nutzung durch die öffentliche Hand eröffnen sich somit vielfältige Möglichkeiten für die Entwicklung neuer auf Verkehrsdaten basierender Geschäftsmodelle und innovativer Mobilitätsdienste. Um diese Potenziale zu erschließen, sind die Bereitstellung der Daten in einem einheitlichen Format und über standardisierte Schnittstellen sowie die Schaffung von Transparenz gegenüber dem Nutzer unabdinglich.

Die exemplarische Skizzierung anhand ausgewählter Fallstudien verdeutlicht, dass die Handlungsempfehlungen in ihrer Gesamtheit einen wertvollen Beitrag leisten, den bestehenden Rahmen für die Nutzung von Mobilitätsdaten so zu gestalten, dass ökonomische Potenziale bei gleichzeitiger Achtung von Persönlichkeitsrechten und Privatheitsanforderungen erschlossen werden können.

Anhang

I. Tabellarische Übersicht der Fallstudienanalyse aus technischer Sicht

i. Fallstudie 1: Kfz-Instandhaltung und -Wartung

<i>Herr Mustermann ist Eigentümer eines Autos. Während er fährt, meldet sein Auto eine Motorstörung, zeigt sie ihm an und sendet sie zugleich automatisiert an den Hersteller. Seine Werkstatt kontaktiert Herrn Mustermann nach der Fahrt, um einen Service-/Wartungstermin zu vereinbaren.</i>	
Allgemeine Situationsbeschreibung	<ul style="list-style-type: none"> Der Fahrzeughersteller bietet Online-Diagnose als zusätzliche Dienstleistung zu seinen Fahrzeugen mit dem Ziel, den Service für den Kunden zu optimieren Das Fahrzeug sendet Sensordaten und Diagnoseergebnisse automatisiert an den Hersteller
Akteure	<ul style="list-style-type: none"> Fahrer (zugleich auch Fahrzeugeigentümer/-halter) Fahrzeughersteller Weitere Akteure: Werkstatt, Zulieferer
Relevante Daten	<ul style="list-style-type: none"> Dynamische Fahrzeugdaten: im Fahrzeug erfasste Sensordaten und Diagnoseergebnisse Statische Nutzerdaten: persönliche Kundendaten
Datenbezogene Vorgänge	<ul style="list-style-type: none"> Lokale Erfassung von Sensordaten und Verarbeitung durch elektronische Steuergeräte im Fahrzeug Datenübertragung vom Fahrzeug zum Hersteller in periodischen Intervallen, beim Eintreten von Ereignissen (z. B. Motorschaden), ständige Übertragung aller Daten oder auf Initiative des Herstellers (z. B. vor Werkstattbesuch) Datenübertragung vom Hersteller zur Werkstatt zur Vorbereitung eines Werkstattbesuchs (z. B. Wartung oder Reparatur)
Eingesetzte Technologien	<ul style="list-style-type: none"> Elektronische Steuergeräte im Fahrzeug: lokale Datenerfassung und -auswertung Mobilfunkrouter im Fahrzeug: Datenübermittlung an den Hersteller über eine verschlüsselte Internet-Verbindung via Mobilfunk zwischen Fahrzeug und System des Herstellers Datenübermittlung an die Werkstatt: verschlüsselte Internet-Verbindung zwischen den Systemen des Herstellers und der Werkstatt
(Technische) Zugriffsmöglichkeiten	<ul style="list-style-type: none"> Hersteller hat Zugriff auf alle an ihn übertragenen Daten; optional: Hersteller kann aktiv jederzeit aktuelle Daten vom Fahrzeug anfordern Werkstatt hat Zugriff auf Daten eines Reparatur-/Wartungsauftrages (inkl. Kundendaten und relevante Sensor- und Diagnosedaten)
Zweck der Datenerstellung	<ul style="list-style-type: none"> Frühzeitige und automatisierte Erkennung von Fehlfunktionen (z. B. Motorschaden) Optimierung der Fahrzeugwartung (z. B. Planung von Serviceterminen) Optimierung des Werkstattbesuchs (z. B. Ersatzteilbestellung)

ii. Fallstudie 2: *Carsharing*

Frau Musterfrau öffnet das Fahrzeug eines Carsharing-Anbieters mit ihrer Zugangskarte und tritt die Fahrt an. Nach Abstellen des Fahrzeugs und Beendigung des Mietvorgangs erhält sie eine Rechnung über die gefahrene Strecke über ihr Kundenkonto bei dem Carsharing-Anbieter.

Allgemeine Situationsbeschreibung	<ul style="list-style-type: none"> ■ Carsharing-Anbieter vermietet Fahrzeuge an Carsharing-Nutzer, zur Reservierung und Nutzung werden eine Smartphone-Anwendung und Zugangskarten ausgegeben ■ In den Fahrzeugen laufen vom Carsharing-Anbieter betriebene Anwendungen, welche den Zugang zum Fahrzeug ermöglichen und die Nutzung protokollieren ■ Für das Auftanken der Fahrzeuge erhalten Nutzer Bonuspunkte
Akteure	<ul style="list-style-type: none"> ■ Fahrer (als Carsharing-Nutzer) ■ Carsharing-Anbieter (zugleich Fahrzeugeigentümer/-halter) ■ Weitere Akteure: Fahrzeughersteller, Tankstelle
Relevante Daten	<ul style="list-style-type: none"> ■ Dynamische Nutzerdaten: Mietvorgangsdaten (Position, Zeit und Kilometerstand zu Beginn und Ende der Miete) ■ Statische Nutzerdaten: Persönliche Daten des Carsharing-Nutzers ■ Dynamische Fahrzeugdaten: Echtzeitstatusinformationen des Fahrzeugs (z. B. aktuelle Position, Tankfüllstand)
Datenbezogene Vorgänge	<ul style="list-style-type: none"> ■ Prüfung der Zugangsberechtigung zu Beginn der Miete ■ Übertragung von Position, Zeit und Kilometerstand zu Beginn und Ende der Miete ■ Übertragung von Echtzeitstatusinformationen (aktuelle Position, etc.) während des Mietvorgangs ■ Auslesen des Tankfüllstandes und Übertragen an den Carsharing-Anbieter nach dem Tankvorgang ■ Regelmäßige Übertragung von Statusinformationen (z. B. Position, Batterieladestand) des abgestellten Fahrzeugs (außerhalb des Mietvorgangs) an den Carsharing-Anbieter
Eingesetzte Technologien	<ul style="list-style-type: none"> ■ Carsharing-Hardware und -Softwareplattform im Fahrzeug, bestehend aus Mobilfunkrouter, Kartenleser, Benutzerschnittstelle ■ Tankfüllstandmesssonde ■ Schnittstelle zu Fahrzeug (Sensoren) und Carsharing-System (via Fahrzeugbus)
(Technische) Zugriffsmöglichkeiten	<ul style="list-style-type: none"> ■ Carsharing-Anbieter hat Zugriff auf alle erhobenen Daten vom Carsharing-System und ausgewählten angebundenen Sensoren im Fahrzeug
Zweck der Datenerstellung	<ul style="list-style-type: none"> ■ Vermietung von Carsharing-Fahrzeugen ■ Abrechnung von Carsharing-Nutzung ■ Lokalisierung der Fahrzeuge erfolgt zum Zwecke der Fahrzeugvermittlung

iii. Fallstudie 3: Mobilitätsdienstesteplattform

Im Fahrzeug von Herrn Mustermann ist eine Mobilitätsdienstesteplattform eines Drittanbieters integriert. Auf dem Basisbildschirm wird das aktuelle Wetter an der Fahrzeugposition angezeigt. Herr Mustermann ist mit seinem persönlichen Account am System angemeldet und tätigt einen Telefonanruf aus der synchronisierten Kontaktliste.

Allgemeine Situationsbeschreibung	<ul style="list-style-type: none"> ■ Hersteller integriert Mobilitätsdienstesteplattform eines Drittanbieters in seine Fahrzeuge ■ Die Plattform ist mit dem Fahrzeug vernetzt und bietet Internetzugang
Akteure	<ul style="list-style-type: none"> ■ Fahrer (als Nutzer der Mobilitätsdienstesteplattform) ■ Anbieter der Mobilitätsdienstesteplattform (unabhängig vom Fahrzeughersteller) ■ Weitere Akteure: Fahrzeughersteller
Relevante Daten	<ul style="list-style-type: none"> ■ Statische Nutzerdaten: Persönliche Daten (inkl. Kontaktliste) des Nutzers ■ Positionsdaten: Positionsdaten des Fahrzeugs
Datenbezogene Vorgänge	<ul style="list-style-type: none"> ■ Synchronisierung der Kontaktliste in die (und aus der) <i>Cloud</i> des Anbieters der Mobilitätsdienstesteplattform ■ Abrufen der lokalen Wetterinformation von einem integrierten Dienst des Anbieters der Mobilitätsdienstesteplattform (inkl. Übertragung der Fahrzeugposition) ■ Initiierung eines Telefonanrufs (inkl. Übertragung der Rufnummer von der Plattform ans <i>Infotainment</i>-system des Fahrzeugs)
Eingesetzte Technologien	<ul style="list-style-type: none"> ■ Mobilitätsdienstesteplattform ■ Schnittstelle zu Fahrzeugdaten, vom Fahrzeughersteller zur Mobilitätsdienstesteplattform ■ Softwaresystem (<i>App Operating System</i>) zur Installation und Ausführung von Apps Dritter ■ Synchronisation über Internetverbindung per Mobilfunk
(Technische) Zugriffsmöglichkeiten	<ul style="list-style-type: none"> ■ Anbieter der Mobilitätsdienstesteplattform hat Zugriff auf in die <i>Cloud</i> synchronisierte Daten ■ Die lokale Mobilitätsdienstesteplattform hat Zugriff auf synchronisierte Daten aus der <i>Cloud</i> und ausgewählte Sensordaten aus dem Fahrzeug (je nach Plattform und Fahrzeughersteller) ■ Das Fahrzeug (<i>Infotainmentsystem</i>) hat keinen Zugriff auf die Mobilitätsdienstesteplattform, wird jedoch bei Bedarf mit benötigten Daten versorgt (z.B. Rufnummer bei Anrufinitiierung)
Zweck der Datenerstellung	<ul style="list-style-type: none"> ■ Bündelung von fahrzeug- und nutzerspezifischen Daten in der Mobilitätsdienstesteplattform, um darauf aufbauend Dienste anzubieten

iv. Fallstudie 4: Mobilitätsdienste

Herr Mustermann sucht über eine Parkplatzreservierungs-App eines unabhängigen Anbieters, die er auf seiner Mobilitätsdienstesteplattform installiert hat, einen freien Stellplatz in einem Parkhaus in seiner Umgebung.

Allgemeine Situationsbeschreibung	<ul style="list-style-type: none"> ■ Von Drittanbietern betriebene Mobilitätsdienste-Apps können auf der Mobilitätsdienstesteplattform laufen und ermöglichen dadurch die Nutzung von Drittanbieterdiensten im Fahrzeug ■ Der Nutzer kann selbstständig entsprechende Apps von Drittanbietern nachinstallieren
Akteure	<ul style="list-style-type: none"> ■ Fahrer (als Nutzer des Mobilitätsdienstes) ■ Anbieter des Mobilitätsdienstes ■ Nebenakteure: Anbieter der Mobilitätsdienstesteplattform, Fahrzeughersteller
Relevante Daten	<ul style="list-style-type: none"> ■ Positionsdaten: Positionsdaten des Fahrzeugs ■ Statische Nutzerdaten: Persönliche Daten des Nutzers ■ Dynamische Nutzerdaten: Anwendungsbezogene Daten (z. B. Anfrageparameter)
Datenbezogene Vorgänge	<ul style="list-style-type: none"> ■ Lokalisierte Suchanfrage des Nutzers an die Parkplatzvermittlungs-App ■ Abfrage der Positionsdaten durch die Parkplatzvermittlungs-App von der Mobilitätsdienstesteplattform ■ Weitergabe ausgewählter Sensordaten vom Fahrzeug an die Mobilitätsdienstesteplattform, hier Positionsdaten ■ Lokalisierte Suchanfrage der App an den Parkplatzvermittlungsdienst
Eingesetzte Technologien	<ul style="list-style-type: none"> ■ Internetverbindung per Mobilfunk zum Drittanbieter
(Technische) Zugriffsmöglichkeiten	<ul style="list-style-type: none"> ■ Die Mobilitätsdienstesteplattform hat (je nach angebundenen Sensoren) Zugriff auf ausgewählte Daten des Fahrzeugs, z. B. die aktuelle Position ■ Die Drittanbieter-App hat (je nach gewährten Rechten) Zugriff auf ausgewählte Daten der Mobilitätsdienstesteplattform (inkl. verfügbarer Fahrzeugdaten), z. B. die aktuelle Position ■ Mobilitätsdiensteanbieter hat Zugriff auf übermittelte Daten, z. B. Positionsdaten aus Suchanfragen
Zweck der Datenerstellung	<ul style="list-style-type: none"> ■ <i>Location-based Services</i>

v. Fallstudie 5: *Car-2-Infrastructure*-Kommunikation

Während der Fahrt mit ihrem LKW fährt Frau Musterfrau über eine Brücke und passiert dabei eine Roadside-Unit des Landesbetriebs Straßenbau, die alle Car-2-X-Nachrichten aufzeichnet und zur Verkehrszentrale des Landesbetriebs überträgt.

Allgemeine Situationsbeschreibung	<ul style="list-style-type: none"> ■ Statusinformation des Fahrzeugs werden periodisch per Car-2-X-Kommunikation ausgesendet ■ Andere Fahrzeuge, Verkehrsinfrastrukturen sowie -zentralen können sich daraus in Echtzeit ein Lagebild der näheren Umgebung erstellen
Akteure	<ul style="list-style-type: none"> ■ Fahrer (zugleich auch Fahrzeugeigentümer/-halter) ■ Infrastrukturbetreiber (z. B. Landesbetrieb Straßenbau oder Autobahnmeisterei) ■ Nebenakteure: Fahrzeughersteller, Verkehrszentrale
Relevante Daten	<ul style="list-style-type: none"> ■ Verkehrslagedaten: Verkehrslagebild ■ Dynamische Fahrzeugdaten: z. B. Geschwindigkeit, Richtung ■ Statische Fahrzeugdaten: z. B. Abmessungen, Fahrzeugtyp ■ Positionsdaten: Aktuelle Position
Datenbezogene Vorgänge	<ul style="list-style-type: none"> ■ Periodisches Aussenden von Sensordaten per Car-2-X an Fahrzeuge und Infrastruktur in der näheren Umgebung ■ Aufzeichnung empfangener Car-2-X-Nachrichten in der Roadside-Unit ■ Übermittlung aufgezeichneter Car-2-X-Nachrichten von der Roadside-Unit zur Verkehrszentrale
Eingesetzte Technologien	<ul style="list-style-type: none"> ■ Direkte Car-2-X-Kommunikation per 802.11p ■ Sensorik in Fahrzeugen und Roadside-Units ■ Datenverbindung zwischen Roadside-Units und Verkehrszentralen
(Technische) Zugriffsmöglichkeiten	<ul style="list-style-type: none"> ■ Car-2-X-Nachrichten werden unverschlüsselt im 5,9 GHz-Band versendet und sind für jeden Empfänger in der Umgebung frei zugänglich und nutzbar ■ Die Roadside-Unit verfügt über die gesammelten Car-2-X-Daten passierender Fahrzeuge ■ Die Verkehrszentrale hat Zugriff auf gesammelten Car-2-X-Nachrichten aller angeschlossenen Roadside-Units
Zweck der Datenerstellung	<ul style="list-style-type: none"> ■ Verkehrsoptimierung ■ Erhöhung der Verkehrssicherheit (weniger Unfälle) ■ Reduktion von Emissionen

II. Bereichsspezifische Zuordnung von Daten im geltenden Recht

i. Verfassungsrecht

Fallstudie 1 Kfz-Instandhaltung und -Wartung	Akteure	Grundrechtliche Zuordnung zu ...
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung ist nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung vor staatlichen Zugriffen geschützt. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems als solches.
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und damit Begrenzung des Transfers ist nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung erfasst. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems als solches. Der Transfer zu einem privaten Dritten (Hersteller) ist nicht unmittelbarer Regulationsgegenstand des Verfassungsrechts.
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller Dritter (z. B. Zulieferer)	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und daraus folgende Begrenzung des Transfers ist nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Eigentümer des Kfz = Fahrer = Halter Hersteller Dritter (z. B. Werkstatt)	Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung erfasst. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems als solches. Der Transfer zu einem weiteren privaten Dritten (Werkstatt) ist ebenfalls nicht unmittelbarer Regulationsgegenstand des Verfassungsrechts.

Fallstudie 2 Carsharing	Akteure	Grundrechtliche Zuordnung zu ...
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung dieser Daten ist nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung vor staatlichen Zugriffen geschützt. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems als solches. Daran ändert sich auch dadurch nichts, dass im Unterschied zur ersten Fallkonstellation die Daten auf Systemen gespeichert werden, die im Eigentum eines Dritten (hier des Carsharing-Anbieters) stehen.
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Hersteller (-system)	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer Hersteller (-system)	Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung erfasst. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems als solches. Der Transfer zu einem privaten Dritten (Carsharing-Anbieter) ist nicht unmittelbarer Regulationsgegenstand des Verfassungsrechts.
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung erfasst. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems als solches. Der Transfer zu einem privaten Dritten (Carsharing-Anbieter) ist nicht unmittelbarer Regulationsgegenstand des Verfassungsrechts.

Fallstudie 3 Mobilitätsdienstesteplattform	Akteure	Grundrechtliche Zuordnung zu ...
3a) Eingabe von Daten in die Mobilitätsdienstesteplattform und Transfer (Synchronisierung) zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz MDP-Anbieter	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung ist nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Fahrer = Eigentümer und Halter des Kfz MDP-Anbieter	Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung erfasst. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems (hier der Mobilitätsdienstesteplattform) als solches. Die Synchronisation ist nicht unmittelbarer Regulationsgegenstand des Verfassungsrechts; eine verfassungsrechtliche Zuordnung ist nicht möglich. Da es sich nicht um eine Individualkommunikation handelt, greift auch kein Schutz von Art. 10 GG.
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstesteplattform und zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz	[entspricht 3a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Hersteller (-system) MDP-Anbieter	[entspricht 3a]
3c) Transfer der Daten von Mobilitätsdienstesteplattform zu Fahrzeug (Anruftätigung)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz	[entspricht 3b]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	Hersteller (-system) MDP-Anbieter	Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen, werden vom Recht auf informationelle Selbstbestimmung erfasst. Im Sinne eines Vorfeldschutzes bezieht sich dieser Schutz auch auf die Vertraulichkeit und Integrität des informationstechnischen Systems (hier der Mobilitätsdienstesteplattform) als solches. Soweit es sich dabei um laufende Kommunikation handelt, ist ein Schutz über Art. 10 GG gegeben.

Fallstudie 4 Mobilitätsdienste	Akteure	Grundrechtliche Zuordnung zu ...
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz MD-Anbieter	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		[entspricht 3a]
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer des Kfz Hersteller(-system) MDP-Anbieter	[aufbauend auf 3b, deswegen wird das Herstellersystem nicht betrachtet; der Fall, dass der Mobilitätsdienst unmittelbar auf Fahrzeugsysteme zugreift, dürfte technisch nicht abgebildet sein]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	MD-Anbieter	[aufbauend auf 3b, deswegen wird das Herstellersystem nicht betrachtet; der Fall, dass der Mobilitätsdienst unmittelbar auf Fahrzeugsysteme zugreift, dürfte technisch nicht abgebildet sein]

Fallstudie 5 Car-2-X-Kommunikation	Akteure	Grundrechtliche Zuordnung zu ...
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Infrastrukturbetreiber	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Verkehrsteilnehmer	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer des Kfz Infrastrukturbetreiber Dritter (z. B. Anbieter von Navigationsdiensten)	Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen, werden nicht vom Recht auf informationelle Selbstbestimmung erfasst; eine verfassungsrechtliche Zuordnung und eine daraus folgende Begrenzung des Transfers sind nicht möglich.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	

ii. Datenschutzrecht

Fallstudie 1 Kfz-Instandhaltung und -Wartung		Akteure	Datenschutzrechtliche Zuordnung zu ...
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen			
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter	Keine Aussage des Datenschutzrechts.	
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		Keine Aussage des Datenschutzrechts, da Daten sich beim Betroffenen selbst befinden.	
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller			
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen ⁴¹⁶ (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller	Keine Aussage des Datenschutzrechts.	
Daten, die einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		Stellt eine Erhebung durch den Hersteller dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; regelmäßig Vertrag).	
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten			
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller Dritter (z. B. Zulieferer)	Keine Aussage des Datenschutzrechts.	
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Eigentümer des Kfz = Fahrer = Halter Hersteller Dritter (z. B. Werkstatt)	Stellt eine Übermittlung durch den Hersteller dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; regelmäßig Vertrag). Wenn der Dritte (z. B. als Werkstatt) rechtlich Teil des Herstellers ist, liegt keine Übermittlung vor.	

⁴¹⁶ Dies setzt voraus, dass die Daten anonymisiert werden, bevor der Hersteller sie erhält – entweder im Kfz selbst oder durch einen vertrauenswürdigen Dritten. Sofern – wie regelmäßig – der Hersteller die Daten in Verbindung mit einer eindeutigen Kennung des Kfz erhält und dessen Halter kennt (weil er z. B. in einer Kundendatenbank enthalten ist), sind die Daten personenbezogen.

Fallstudie 2 Carsharing	Akteure	Datenschutzrechtliche Zuordnung zu ...
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz	[vergleichbar mit 1a – aber Generierung auf Systemen, die im Eigentum eines Dritten stehen] Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer	Stellt eine Erhebung und Verarbeitung in Form von Speichern durch den Carsharing-Anbieter dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; hier: Vertrag).
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Hersteller(-system)	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer Hersteller(-system)	Stellt eine Übermittlung durch den Carsharing-Anbieter (unter Zuhilfenahme des Hersteller(-systems)) dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; hier: Vertrag oder separate Einwilligung bei optionalen Diensten).
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer	Stellt eine Nutzung sowie Speicherung durch den Carsharing-Anbieter dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; hier: Vertrag).

Fallstudie 3 Mobilitätsdienstesteplattform	Akteure	Datenschutzrechtliche Zuordnung zu ...
3a) Eingabe von Daten in die Mobilitätsdienstesteplattform und Transfer (Synchronisierung) zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Fahrer = Eigentümer = Halter des Kfz MDP- Anbieter	Stellt eine Erhebung und ggf. Speicherung durch den MDP-Anbieter dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; hier: Vertrag).
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstesteplattform und zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer = Halter des Kfz	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Hersteller (-system) MDP-Anbieter	Stellt eine Erhebung sowie Nutzung und ggf. Speicherung durch den MDP-Anbieter (unter Zuhilfenahme des Hersteller(systems)) dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; hier: Vertrag).
3c) Transfer der Daten von Mobilitätsdienstesteplattform zu Fahrzeug (Anruftätigung)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer = Halter des Kfz MDP-Anbieter	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		Stellt eine Nutzung durch den MDP-Anbieter dar und bedarf daher einer Legitimation (Erlaubnisnorm oder Einwilligung; hier: Vertrag).

Fallstudie 4 Mobilitätsdienste	Akteure	Datenschutzrechtliche Zuordnung zu ...
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz MD-Anbieter	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	[entspricht 3a]	
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer des Kfz Hersteller (-system) MDP- Anbieter MD-Anbieter	[aufbauend auf 3b, deswegen wird das Herstellersystem nicht betrachtet; der Fall, dass der Mobilitätsdienst unmittelbar auf Fahrzeugsysteme zugreift, dürfte technisch nicht abgebildet sein]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		[aufbauend auf 3b, deswegen wird das Herstellersystem nicht betrachtet; der Fall, dass der Mobilitätsdienst unmittelbar auf Fahrzeugsysteme zugreift, dürfte technisch nicht abgebildet sein]

Fallstudie 5 Car-2-X-Kommunikation	Akteure	Datenschutzrechtliche Zuordnung zu ...
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant] ⁴¹⁷	
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Infrastrukturbetreiber	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Verkehrsteilnehmer	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer des Kfz Infrastrukturbetreiber Dritter (z. B. Anbieter von Navigationsdiensten)	Keine Aussage des Datenschutzrechts.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	

⁴¹⁷ Durch die Aussendung der Daten mit dem CAM- bzw. DENM-Standard, ggf. in Verbindung mit weiteren technischen Maßnahmen, ist die Herstellung eines Personenbezuges nicht mehr ohne weiteres möglich. Der Austausch von Nachrichten per Funk erfolgt im 5.9 GHz-Bereich, der für die Fahrzeugkommunikation reserviert ist. Zwar werden alle Nachrichten digital signiert und mit einem gültigen Zugangszertifikat versehen, aber die Fahrzeuge besitzen eine große Menge an Zertifikaten mit einem jeweils kurzen Gültigkeitszeitraum, der in jeweils schneller Folge gewechselt wird, so dass keine eindeutige Zuordnung einer ID mit dem Zertifikat möglich ist.

iii. Urheberrecht

Fallstudie 1 Kfz-Instandhaltung und -Wartung	Akteure	Urheberrechtliche Zuordnung zu ...
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter	Mangels persönlicher schöpferischer Tätigkeit besteht kein urheberrechtlicher Werkschutz für die einzelnen maschinengenerierten Rohdaten. Die Daten wurden ferner nicht schöpferischer ausgewählt oder angeordnet, so dass deren Zusammenstellungen kein Sammelwerk ist. Da der Eigentümer keine wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung der Daten tätigt, entsteht in seinen Händen zudem kein Leistungsschutzrecht i. S. v. § 87a UrhG. Ein solches würde im Übrigen dem Datenbankhersteller auch kein Ausschließlichkeitsrecht an einzelnen Mobilitätsdaten zuweisen.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller	Es liegt keine vom Urheberrechtsgesetz geschützte Leistung vor (siehe oben 1a).
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer Hersteller Dritter (z. B. Zulieferer)	Es liegt keine vom Urheberrechtsgesetz geschützte Leistung vor (siehe oben 1a).
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		

Fallstudie 2 Carsharing	Akteure	Urheberrechtliche Zuordnung zu ...
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz	Die verarbeiteten Einzelinformationen (PIN, Standortinformationen, Tankfüllstand) sind mangels Individualität keine persönliche geistige Schöpfung i. S. v. § 2 Abs. 2 UrhG. Sie werden zudem für Abrechnungszwecke zusammengestellt, so dass auch deren Auswahl und Anordnung buchhalterischen bzw. mathematischen Zwängen folgt und damit kein Sammelwerk (§ 4 UrhG) ist. Da der Eigentümer keine wesentliche Investition in die Beschaffung, Überprüfung oder Darstellung der Daten tätigt entsteht in seinen Händen zudem kein Leistungsschutzrecht i. S. v. § 87a UrhG. Ein solches würde im Übrigen dem Datenbankhersteller auch kein Ausschließkeitsrecht an einzelnen Mobilitätsdaten zuweisen.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer	
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Hersteller (-system)	Es liegt keine vom Urheberrechtsgesetz geschützte Leistung vor (siehe oben 2a).
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer Hersteller (-system)	
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz	Es liegt keine vom Urheberrechtsgesetz geschützte Leistung vor (siehe oben 2a).
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer	

Fallstudie 3 Mobilitätsdienstplattform	Akteure	Urheberrechtliche Zuordnung zu ...
3a) Eingabe von Daten in die Mobilitätsdienstplattform und Synchronisierung mit der Cloud des MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Fahrer = Eigentümer und Halter des Kfz MDP- Anbieter	Die übertragenen Daten (Kalendereinträge, Telefonbücher, E-Mails) schützt das UrhG in aller Regel nicht. Diese weisen meist keine hinreichende Individualität auf und sind daher keine persönlichen geistigen Schöpfungen i. S. v. § 2 Abs. 2 UrhG. Der Fahrer tätigt auch keine wesentliche Investition in deren Beschaffung, Überprüfung oder Darstellung (vgl. § 87a UrhG).
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstplattform und zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP- Anbieter	[entspricht 3a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
3c) Transfer der Daten von Mobilitätsdienstplattform zu Fahrzeugsystem		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	[entspricht 3a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		

Fallstudie 4 Mobilitätsdienste	Akteure	Urheberrechtliche Zuordnung zu ...
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz MD-Anbieter	Es liegt keine vom Urheberrechtsgesetz geschützte Leistung vor.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer des Kfz Hersteller (-system) MDP-Anbieter MD-Anbieter	Es liegt keine vom Urheberrechtsgesetz geschützte Leistung vor.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		

Fallstudie 5 Car-2-X-Kommunikation	Akteure	Urheberrechtliche Zuordnung zu ...
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz	Die Rohdaten (Positionsdaten) sind keine vom Urheberrechtsgesetz geschützte Leistung.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Infrastrukturbetreiber	Die einzelnen Rohdaten sind keine vom Urheberrechtsgesetz geschützte Leistung. Deren Auswertung für die lokalen Umfelddaten erfolgt nach verkehrstechnischen und mathematischer Regeln, so dass keine schöpferische Auswahl oder Anordnung vorliegt und damit auch kein Sammelwerk (§ 4 UrhG). Möglicherweise genießt der Infrastrukturbetreiber aber den Schutz des Leistungsschutzrechts des Datenbankherstellers (§ 87a UrhG). Letztlich bietet dieser sui generis Schutz jedoch kein Ausschließlichkeitsrecht an einzelnen Mobilitätsdaten.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Verkehrsteilnehmer	[entspricht 5a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer des Kfz Infrastrukturbetreiber Dritter (z. B. Anbieter von Navigationsdiensten)	[entspricht 5a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	

iv. Strafrecht

Fallstudie 1 Kfz-Instandhaltung und -Wartung	Akteure	Strafrechtlicher Schutz zugunsten von ...
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter	Bei maschinengenerierten Daten sind unterschiedliche Zuordnungen denkbar: ■ Fahrer durch Betrieb des Fahrzeugs ■ Eigentümer des Kfz als Eigentümer der Sensorik im Ergebnis führen beide Ansichten in diesem Fall zur gleichen Zuordnungsentscheidung Skribent: Eigentümer des Kfz = Fahrer = Halter
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller	[entspricht 1a] ggf. bei automatisiertem Transfer und externer Steuerung der Sensorik und Datenerstellung: Hersteller als Betreiber der Programmautomatik
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer Hersteller Dritter (z. B. Zulieferer, Werkstatt)	[entspricht 1a und 1b: Transfer und Weiterleitung haben keine Auswirkungen auf die Festlegung des ursprünglichen Skribenten] ggf. bei Aufbereitung der Daten, Kombination mit weiteren Daten beim Hersteller: Hersteller als Verantwortlicher für die Erstellung „neuer Daten“
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		

Fallstudie 2 Carsharing	Akteure	Strafrechtlicher Schutz zugunsten von ...
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zu- zuordnenden Aussagegehalt auf- weisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz	[vergleichbar mit 1a – aber Generierung auf Systemen, die im Eigentum eines Dritten stehen] Bei maschinengenerierten Daten sind unterschiedliche Zu- ordnungen denkbar: ■ Fahrer durch Betrieb des Fahrzeugs ■ Eigentümer des Kfz (=Carsharing-Anbieter) als Eigentü- mer der Sensorik
Daten, die einen einer Person (Fah- rer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer	anders als bei 1a führen die Ansichten in diesem Fall zu un- terschiedlichen Zuordnungen: Vorzugswürdig ist eine Zu- ordnung zu demjenigen, dem die Erstellung des konkreten Datums nach wirtschaftlicher Betrachtungsweise zuzurech- nen ist. Da der Betrieb des Kfz durch den Carsharing-Nutzer vordergründig der eigenen Fortbewegung dient, scheint eine Zuordnung zum Eigentümer der Sensorik hier sachgerecht
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zu- zuordnenden Aussagegehalt auf- weisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Hersteller (-system)	[entspricht 2a] ggf. bei automatisiertem Transfer und externer Steuerung der Sensorik und Datenerstellung: Carsharing-Anbieter als Be- treiber der Programmatomatik
Daten, die einen einer Person (Fah- rer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer = Halter des Kfz Fahrer Hersteller (-system)	
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter		
Daten, die keinen einer Person zu- zuordnenden Aussagegehalt auf- weisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer = Halter des Kfz	[entspricht 1a und 1b: Transfer und Weiterleitung haben keine Auswirkungen auf die Festlegung des ursprünglichen Skri- benten]
Daten, die einen einer Person (Fah- rer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	

Fallstudie 3 Mobilitätsdienstesteplattform	Akteure	Strafrechtlicher Schutz zugunsten von ...
3a) Eingabe von Daten in die Mobilitätsdienstesteplattform und Transfer (Synchronisierung) zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Fahrer = Eigentümer und Halter des Kfz MDP-Anbieter	Skribent: Fahrer = Eigentümer und Halter des Kfz durch Eingabe der Daten in eine Datenverarbeitungsanlage
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstesteplattform und zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	Bei maschinengenerierten Daten sind unterschiedliche Ansichten denkbar: <ul style="list-style-type: none">■ Fahrer durch Betrieb des Fahrzeugs■ Eigentümer des Kfz als Eigentümer der Sensorik■ Hersteller des Kfz als Betreiber der Programmatematik■ MDP-Anbieter als Betreiber der Programmatematik Vorzugswürdig ist eine Zuordnung zu demjenigen, dem die Erstellung des konkreten Datums nach wirtschaftlicher Betrachtungsweise zuzurechnen ist – dies dürfte in der Regel der Eigentümer des Kfz als Eigentümer der Sensorik sein.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
3c) Transfer der Daten von Mobilitätsdienstesteplattform zu Fahrzeug (Anruftätigung)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	[entspricht 3b]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		

Fallstudie 4 Mobilitätsdienste	Akteure	Strafrechtlicher Schutz zugunsten von ...
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz MD-Anbieter	[entspricht 3a, da der Skripturakt sich auch auf Daten beziehen kann, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen] Skribent: Fahrer = Eigentümer und Halter des Kfz
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		[entspricht 3a] Skribent: Fahrer = Eigentümer und Halter des Kfz
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdiensteplattform) zum Mobilitätsdienst und zum MD-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer des Kfz Hersteller (-system) MDP-Anbieter MD-Anbieter	[aufbauend auf 3b, deswegen wird das Herstellersystem nicht betrachtet; der Fall, dass der Mobilitätsdienst unmittelbar auf Fahrzeugsysteme zugreift, dürfte technisch nicht abgebildet sein] Skribent: Eigentümer des Kfz als Eigentümer der Sensorik
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		[aufbauend auf 3b, deswegen wird das Herstellersystem nicht betrachtet; der Fall, dass der Mobilitätsdienst unmittelbar auf Fahrzeugsysteme zugreift dürfte technisch nicht abgebildet sein] Skribent: Eigentümer des Kfz als Eigentümer der Sensorik

Fallstudie 5 ⁴¹⁸ Car-2-X-Kommunikation	Akteure	Strafrechtlicher Schutz zugunsten von ...
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz	Bei maschinengenerierten Daten sind unterschiedliche Zuordnungen denkbar: <ul style="list-style-type: none">■ Fahrer durch Betrieb des Fahrzeugs■ Eigentümer des Kfz als Eigentümer der Sensorik im Ergebnis führen beide Ansichten in diesem Fall zur gleichen Zuordnungsentscheidung Skribent: Eigentümer des Kfz = Fahrer = Halter
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Infrastrukturbetreiber	[entspricht 5a: Transfer hat keine Auswirkung auf die Festlegung des ursprünglichen Skribenten] Skribent: Eigentümer des Kfz = Fahrer = Halter
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Verkehrsteilnehmer	[entspricht 5a: Transfer hat keine Auswirkung auf die Festlegung des ursprünglichen Skribenten] Skribent: Eigentümer des Kfz = Fahrer = Halter
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer des Kfz Infrastrukturbetreiber Dritter (z. B. Anbieter von Navigationsdiensten)	[entspricht 5a: Transfer hat keine Auswirkung auf die Festlegung des ursprünglichen Skribenten] Skribent: Eigentümer des Kfz = Fahrer = Halter ggf. bei Aufbereitung der Daten, Kombination mit weiteren Daten beim Infrastrukturbetreiber: Infrastrukturbetreiber als Verantwortlicher für die Erstellung „neuer Daten“
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	

418 Im Rahmen der Fallstudie 5 werden ausschließlich nicht-personenbezogene Daten betrachtet, da es sich bei den periodisch oder ereignisbezogen ausgesendeten (überwiegend technischen) Daten um solche zu Lagebild der Umgebung sowie zu Gefahrensituationen handelt, die der Verbesserung des Verkehrsflusses, der Erhöhung der Verkehrssicherheit oder der Reduktion von Emissionen dienen und daher naturgemäß regelmäßig keinen Personenbezug aufweisen.

v. (Lauterkeitsrechtlicher) Schutz von Betriebs- und Geschäftsgeheimnissen

Fallstudie 1 Kfz-Instandhaltung und -Wartung	Akteure	Lauterkeitsrechtliche Zuordnung zu ...
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter	Über Schnittstellen (OBD) können auch Dritte diese Daten auslesen, so dass sie keine Betriebsgeheimnisse bilden.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		Mangels Betriebsbezogenheit werden diese Daten nicht als Betriebsgeheimnis geschützt.
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller	[entspricht 1a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer Hersteller Dritter (z. B. Zulieferer)	[entspricht 1a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer Hersteller Dritter (z. B. Werkstatt)	

Fallstudie 2 Carsharing	Akteure	Lauterkeitsrechtliche Zuordnung zu ...
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz	Über Schnittstellen (OBD) können auch Dritte diese Daten auslesen, so dass sie keine Betriebsgeheimnisse bilden.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	Mangels Betriebsbezogenheit werden diese Daten nicht als Betriebsgeheimnis geschützt.
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Hersteller (-system)	[entspricht 2a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer Hersteller (-system)	
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz	[entspricht 2a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	

Fallstudie 3 Mobilitätsdienstesteplattform	Akteure	Lauterkeitsrechtliche Zuordnung zu ...
3a) Eingabe von Daten in die Mobilitätsdienstesteplattform und Synchronisierung mit der Cloud des MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)	Fahrer = Eigentümer und Halter des Kfz MDP-Anbieter	Die von privaten Fahrern übertragenen Kalendereinträge, Telefonbücher und E-Mails weisen keinen Bezug zu einem Unternehmen auf und werden daher nicht als Betriebsgeheimnis geschützt.
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstesteplattform und zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	[entspricht 3a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
3c) Transfer der Daten von Mobilitätsdienstesteplattform zu Fahrzeug (Anruftätigung)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	[entspricht 3a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		

Fallstudie 4 Mobilitätsdienste	Akteure	Lauterkeitsrechtliche Zuordnung zu ...
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz MD-Anbieter	Die Länge und Breite der Fahrzeuge ist offenkundig und damit kein Betriebsgeheimnis.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		Die von privaten Fahrern übertragenen Namen und Adressen weisen keinen Bezug zu einem Unternehmen auf und werden daher nicht als Betriebsgeheimnis geschützt.
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer des Kfz Hersteller (-system) MDP- Anbieter MD-Anbieter	[entspricht 4a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		

Fallstudie 5 Car-2-X-Kommunikation	Akteure	Lauterkeitsrechtliche Zuordnung zu ...
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz	Die einzelnen Car-2-X-Nachrichten betreffen die Sphären der Kfz-Fahrer und sind daher keine Betriebsgeheimnisse.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Infrastrukturbetreiber	Die einzelnen Car-2-X-Nachrichten betreffen die Sphären der LKW-Fahrer und sind daher keine Betriebsgeheimnisse. Die lokalen Umfelddaten können Betriebsgeheimnisse der Infrastrukturbetreiber sein, soweit diese geheim gehalten werden.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Verkehrsteilnehmer	[entspricht 5a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer des Kfz Infrastrukturbetreiber Dritter (z. B. Anbieter von Navigationsdiensten)	Gibt der Infrastrukturbetreiber die Umfelddaten an Open-Data-Plattformen weiter, sind diese nicht (mehr) geheim und werden nicht als Betriebsgeheimnis geschützt.
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen	[nicht relevant]	

vi. Allgemeines Zivilrecht

Fallstudie 1 Kfz-Instandhaltung und -Wartung	Akteure	Zivilrechtliche Zuordnung zu ...
1a) Lokale Generierung und Speicherung von Daten durch und in Fahrzeugsystemen		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter	Integritätsschutz über § 823 zugunsten des Eigentümers des Fahrzeugsystems
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1b) Transfer von Daten aus Fahrzeugsystemen zum Hersteller		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer = Halter Hersteller	Integritätsschutz über § 823 BGB zugunsten des Herstellers als Eigentümer des Speichermediums, auf dem sich die Daten nach dem Transfer befinden
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)		
1c) Transfer von Daten vom Hersteller zu einem weiteren Dritten		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer Hersteller Dritter (z. B. Zulieferer)	Integritätsschutz über § 823 BGB zugunsten des Dritten als Eigentümer des Speichermediums, auf dem sich die Daten nach dem Transfer befinden
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Eigentümer des Kfz = Fahrer Hersteller Dritter (z. B. Werkstatt)	

Fallstudie 2 Carsharing	Akteure	Zivilrechtliche Zuordnung zu ...
2a) Generierung und Speicherung von Daten durch und in lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz	Integritätsschutz über § 823 BGB zugunsten des Carsharing-Anbieters als Eigentümer des lokalen Systems
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	
2b) Lokaler Transfer von Daten aus Fahrzeugsystemen zu lokalen Systemen des Carsharing-Anbieters		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Hersteller (-system)	[entspricht 2a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer Hersteller (-system)	
2c) Transfer von Daten aus lokalen Systemen des Carsharing-Anbieters (unabhängig von der Quelle) an den Carsharing-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Temperaturdaten oder Verschleißanzeige der Bremsen)	Carsharing-Anbieter = Eigentümer und Halter des Kfz	[entspricht 2a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Standortdaten)	Carsharing-Anbieter = Eigentümer und Halter des Kfz Fahrer	

Fallstudie 3 Mobilitätsdienstplattform	Akteure	Zivilrechtliche Zuordnung zu ...
3a) Eingabe von Daten in die Mobilitätsdienstplattform und Synchronisierung mit der Cloud des MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz MDP-Anbieter	Integritätsschutz über § 823 BGB zugunsten des MDP-Anbieters als Eigentümer des Speichermediums bzw. zugunsten des Cloud-Anbieters als Eigentümer des Speichermediums
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
3b) Transfer von Daten aus Fahrzeugsystemen zur Mobilitätsdienstplattform und zum MDP-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	[entspricht 3a]
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
3c) Transfer der Daten von Mobilitätsdienstplattform zu Fahrzeug (Anruftätigung)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer und Halter des Kfz Hersteller (-system) MDP-Anbieter	Integritätsschutz über § 823 BGB zugunsten des Fahrzeugeigentümers als Eigentümer des im Kfz verbauten Speichermediums
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		

Fallstudie 4 Mobilitätsdienste	Akteure	Zivilrechtliche Zuordnung zu ...
4a) Eingabe von Daten in den Mobilitätsdienst (App), Transfer zum MD-Anbieter und zurück zum Mobilitätsdienst (App)		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz MD-Anbieter	Integritätsschutz über § 823 BGB zugunsten des Fahrzeugeigentümers als Eigentümer des im Kfz verbauten Speichermediums bzw. zugunsten des MD-Anbieters als Eigentümer des Speichermediums
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		
4b) Transfer von Daten aus Fahrzeugsystemen (über die Mobilitätsdienstplattform) zum Mobilitätsdienst und zum MD-Anbieter		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen	Fahrer = Eigentümer des Kfz <i>Hersteller (-system)</i> MDP- Anbieter MD-Anbieter	Integritätsschutz über § 823 BGB zugunsten des MD-Anbieters als Eigentümer des Speichermediums, auf dem sich die Daten nach dem Transfer befinden
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen (z. B. Name und Adresse)		

Fallstudie 5 Car-2-X-Kommunikation	Akteure	Zivilrechtliche Zuordnung zu ...
5a) Periodische oder ereignisbezogene Aussendung aus dem Fahrzeug		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz	Integritätsschutz über § 823 BGB zugunsten des Fahrzeugeigentümers als Eigentümer des im Kfz verbauten Speichermediums
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		
5b) Empfang und Speicherung von Daten durch Infrastrukturbetreiber		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Infrastrukturbetreiber	Integritätsschutz über § 823 BGB zugunsten des Infrastrukturbetreibers als Eigentümer des Speichermediums, auf dem sich die Daten nach dem Transfer befinden
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		
5c) Empfang (und Speicherung) von Daten durch andere Verkehrsteilnehmer		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer und Halter des Kfz Verkehrsteilnehmer	Integritätsschutz über § 823 BGB zugunsten der jeweiligen Verkehrsteilnehmer als Eigentümer der Speichermedien, auf denen sich die Daten nach dem Transfer befinden
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		
5d) Transfer der Daten vom Infrastrukturbetreiber an Dritte		
Daten, die keinen einer Person zuzuordnenden Aussagegehalt aufweisen (z. B. Länge und Breite des Fahrzeugs)	Fahrer = Eigentümer des Kfz Infrastrukturbetreiber Dritter (z. B. Anbieter von Navigationsdiensten)	Integritätsschutz über § 823 BGB zugunsten der Dritten als Eigentümer der Speichermedien, auf denen sich die Daten nach dem Transfer befinden
Daten, die einen einer Person (Fahrer) zuzuordnenden Aussagegehalt aufweisen		

Abbildungsverzeichnis

Abbildung 1: Historie der Digitalisierung im Fahrzeugbau	12
Abbildung 2: Akteursübersicht der fünf Fallstudien	19
Abbildung 3: Kategorisierung von Mobilitätsdaten.....	20
Abbildung 4: Datenflüsse der Fallstudie „Kfz-Instandhaltung und -Wartung“	22
Abbildung 5: Wertschöpfungsnetzwerk der Fallstudie „Kfz-Instandhaltung und -Wartung“	24
Abbildung 6: Datenflüsse der Fallstudie „Carsharing“	26
Abbildung 7: Wertschöpfungsnetzwerk der Fallstudie „Carsharing“	29
Abbildung 8: Datenflüsse der Fallstudie „Mobilitätsdienstplattform“	30
Abbildung 9: Wertschöpfungsnetzwerk der Fallstudie „Mobilitätsdienstplattform“	31
Abbildung 10: Datenflüsse der Fallstudie „Mobilitätsdienste“	33
Abbildung 11: Wertschöpfungsnetzwerk der Fallstudie „Mobilitätsdienste“	34
Abbildung 12: Datenflüsse der Fallstudie „Car-2-Infrastructure-Kommunikation“	36
Abbildung 13: Wertschöpfungsnetzwerk der Fallstudie „Car-2-Infrastructure-Kommunikation“	38
Abbildung 14: Übersicht datenbezogener Vorgänge in Fallstudien 1 bis 5.....	42
Abbildung 15: Ebenenmodell.....	43
Abbildung 16: Kollision bereichsspezifischer Regelungen zur Frage „Dateneigentum“	61
Abbildung 17: Charakteristiken der Digitalisierung	67
Abbildung 18: Anforderungen deutscher Kunden im Kontext der Digitalisierung	68
Abbildung 19: Abstrakte Wertschöpfungskette der Datennutzung und -verwertung.....	69
Abbildung 20: Klassifikation wirtschaftlicher Güter nach Rivalität und Ausschließbarkeit	75
Abbildung 21: Eigenschaften wirtschaftlicher Güter: Rivalität und Ausschließbarkeit.....	76
Abbildung 22: Klassifikation von Daten als Wirtschaftsgut.....	76
Abbildung 23: Rechtliche Regelungsoptionen zur Realisierung von Datensouveränität	86
Abbildung 24: Gründe zur Schaffung von Immaterialgüterrechten.....	90
Abbildung 25: Zuweisung nach der Investition in die Datenerzeugung (Anwendung auf die Fallstudien)	99
Abbildung 26: Rechtliche und ökonomische Bewertung der Zuordnungsansätze	103
Abbildung 27: Indizien zur Ermittlung des Dateneigentümers gemäß des entwickelten Zuordnungsansatzes	104
Abbildung 28: Anwendung des kombinierten Ansatzes auf die Fallstudie	106
Abbildung 29: Übertragbarkeit des Zuordnungsansatzes in einen Normtext	108
Abbildung 30: Schaffung eines Integritätsschutzes	114
Abbildung 31: Umsetzungshorizont der Handlungsempfehlungen.....	122

Abkürzungsverzeichnis

3G	3. Generation von Mobilfunkstandards
ABS	Antiblockiersystem
ADAC	Allgemeiner Deutscher Automobil-Club
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
API	Application Programming Interface
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BVerfG	Bundesverfassungsgericht
CAM	Cooperative Awareness Messages
DENM	Decentralised Environmental Notification Messages
DSGVO	Datenschutz-Grundverordnung
EGBGB	Einführungsgesetz zum Bürgerlichen Gesetzbuche
EMRK	Europäische Menschenrechtskonvention
EuGH	Europäischer Gerichtshof
ETSI	European Telecommunications Standards Institute
GeoZG	Geodatenzugangsgesetz
GHz	Gigahertz
GRC	Charta der Grundrechte der Europäischen Union
GG	Grundgesetz
GPS	Global Positioning System
GWB	Gesetz gegen Wettbewerbsbeschränkungen
IEEE	Institute of Electrical and Electronics Engineers
IFG	Berliner Informationsfreiheitsgesetz
i. S. d.	im Sinne des
IVI	In-Vehicle Infotainment
i. V. m.	in Verbindung mit
IVSG	Intelligente Verkehrssysteme Gesetz
Kfz	Kraftfahrzeug
MD	Mobilitätsdienst
MDM	Mobilitäts Daten Marktplatz
MDP	Mobilitätsdienstplattform
OBD	On-Board-Diagnose
OEM	Original Equipment Manufacturer
PID	Parameter ID
PIN	personal identification number
PKW	Personenkraftwagen
RL	Richtlinie

RSU	Roadside-Unit
SAE	Society of Automotive Engineers
StGB	Strafgesetzbuch
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TRIPS	Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums
UIG	Umweltinformationsgesetz
UrhG	Urheberrechtsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VDA	Verband der Automobilindustrie e.V.
VIN	Vehicle Identification Number

Impressum

Herausgeber

Bundesministerium für Verkehr und digitale Infrastruktur
Invalidenstraße 44
10115 Berlin

Internet

www.bmvi.de

Stand

August 2017

Gestaltung | Druck

Bundesministerium für Verkehr und digitale Infrastruktur
Referat Z 32, Druckvorstufe | Hausdruckerei

Bildnachweis

Titelbild: © iconimage - Fotolia.com

Kapitel 1, Kapitel 4, Kapitel 7: Partnerschaft Deutschland

Kapitel 2: Fraunhofer FOKUS

Kapitel 3, Kapitel 5: Lorenz-von-Stein-Institut, Universität Kassel

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der Bundesregierung.
Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

