Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft

Schlussbericht

Durchgeführt im Auftrag der Bundesnetzagentur

Referat 121 Digitalisierung und Vernetzung; Internetplattformen

Stand: 28. Februar 2023

Forschungsgemeinschaft

Prof. Dr. Andreas Wiebe, LL.M. (Virginia)

RAin Dr. Céline Helmschrot

Prof. Dr. Oliver Kreutz

Inhaltsverzeichnis

A. Executive Summary

Mit dem bereits seit vielen Jahren bestehenden Einsatz von Software und Sensoren in Kraftfahrzeugen entstand auch die Frage, wer die Kontrolle über die Daten ausüben soll und wem Zugang zu den erzeugten Daten zu gewähren ist. Diese auf connected cars bezogene Fragestellung ist nur ein, wenn auch besonders wichtiger, Ausschnitt aus der allgemeinen Diskussion über Data Sharing und einen Rahmen für Data Governance in der digitalen Wirtschaft, was sich zu einer Grundproblematik der Digitalisierung entwickelt hat.

Die EU-Kommission hat die seit 2016 intensiv geführte Diskussion zu Eigentumsrechten an nicht-personenbezogenen Daten aufgegriffen und bereits 2017 erste Überlegungen zur Schaffung neuer Leistungsschutzrechte an Daten angestellt. Dies erwies sich jedoch theoretisch und praktisch als nicht angemessen. Mit dem **Entwurf zum Data Act** wurde ein alternativer Weg beschritten, der vor allem darauf abzielt, die exklusive Kontrolle der Dateninhaber aufzubrechen und Zugangsrechte für die Nutzer von IoT-Geräten zu schaffen, die dann indirekt auch Diensteanbietern auf Sekundärmärkten zugutekommen. Während der Mobilitätssektor einer der Hauptanwendungsbereiche des Data Act sein wird, bestehen zugleich bereits spezifische, eng begrenzte, Regelungen, die einen fairen Zugang von Reparatur- und Wartungsdiensten im Interesse der Verbraucher sicherstellen sollen.

Vor diesem Hintergrund ist es **Ziel der Studie**, die verschiedenen Ebenen aufzuarbeiten, ein differenziertes Bild der Gesamtsituation unter Einbeziehung der rechtspolitischen Diskussion und der rechtlichen Regelungsvorschläge zu erstellen und eine Bewertung unter dem Gesichtspunkt der Sicherung eines fairen und innovationsfördernden Wettbewerbs durchzuführen, die in konkreten Handlungsempfehlungen mündet.

Ziel des **Arbeitspaketes 1** ist eine Darstellung der im „connected car“ bzw. „vernetzen Fahrzeug“ erhobenen und verarbeiteten Datenarten. Daneben wird die Interessenlage diverser Marktakteure entlang der gesamten Wertschöpfungskette der Automobil- und Mobilitätswirtschaft analysiert. Abschließend wird ein Überblick über die bedeutendsten gegenwärtig wie zukünftig zu erwartenden datenbasierten Konnektivitätsdienste und Geschäftsmodelle der Automobil- und Mobilitätswirtschaft gegeben.

Grundsätzlich erfolgt die Datenerzeugung im modernen vernetzten Fahrzeug mit Hilfe von miteinander vernetzten Multifunktionskameras, Radar-, Ultraschall- und Lidarsensoren. So werden unterschiedliche Bereiche des vernetzten Fahrzeugs von unterschiedlichen Sensoren zu einer Vielzahl von Zwecken überwacht. Dabei lassen sich im Wesentlichen zwischen zwei Arten von Sensoren unterscheiden:

- Sensoren zur Erhebung von internen Daten (z.B. Beschleunigungssensor, Pedalweggeber, Reifenluftdruckverlust-Sensor, Tankdrucksensor, Sitzbelegungssensor, Drehzahlsensor)
- Sensoren zur Erhebung von externen Daten (z.B. Frontkameras, Rückkameras, Radar, Lidar und Ultraschallsensoren, Notbremssensoren, Regensensor, Temperatursensoren).

Die im connected car erhobenen Daten lassen sich grundsätzlich in die folgenden drei Kategorien einteilen:

(1) Umgebungsdaten
(2) Fahrzeugbezogene Daten und
(3) Fahrerbezogene Daten

Die durch die Datenverarbeitung im vernetzten Fahrzeug gewonnen Erkenntnisse dienen einer Vielzahl von Datenverarbeitungszwecken. Dazu zählen insbesondere:

- Fahrersicherheitszwecke
- Versicherungszwecke
- Verkehrseffizienzzwecke
- Umweltzwecke

- Unterhaltungs- und Informationszwecke bis hin zu
- Marketingzwecke.

Die bereits gegenwärtig verfügbaren Konnektivitätsdienste und -anwendungen im Kontext des vernetzten Fahrzeugs sind vielfältig, und können gemessen an ihrem übergeordneten Ziel wie folgt geclustert werden:

- Fahrerassistenzsysteme (Advanced Driver Assistance Systems) und Verkehrssicherheit
- Mobilitäts-/ Navigationsmanagement
- Fahrzeug-/ Wartungsmanagement
- Infotainment und Entertainment
- Wohlbefinden.

In **Arbeitspaket 2** erfolgt die Darstellung und Beurteilung bereits bestehender gesetzlicher Regelungen sowie die Darstellung und Analyse von Konzepten und Projekten zum Austausch von Mobilitätdaten in Deutschland.

Im Ergebnis gibt es keine umfassenden rechtlichen Regelungen darüber, wie der enorme Umfang an Daten, den moderne Fahrzeuge heutzutage produzieren, konkret von wem verwendet werden darf, wem der Fahrzeugnutzer seine Daten auf welche Weise zur Verfügung stellen kann und wie dabei Transparenz und Sicherheit in Bezug auf die Daten gewährleistet werden kann. Der Zugang zu technischen Daten für Reparaturen und Wartungen ist europarechtlich durch die Rahmenverordnung (EU) 2018/858 (TypGVO) weitgehend geregelt, er umfasst aber nur einen begrenzten Datensatz über eine bestimmte (analoge) Technik. Daneben gibt es im Sektor Mobilität mit der Verordnung (EU) 2015/758 (eCall-VO) und der Richtlinie 2010/40/EU (IVS-RL) vereinzelte europarechtliche Vorgaben zum Datenteilen auf Basis einer Übermittlungsverpflichtung, wobei die Daten aber den Marktakteuren für den Betrieb oder die Entwicklung von (innovativen) Geschäftsmodellen gar nicht zur Verfügung stehen oder aber nur limitierte Daten zum Nutzen bestimmter Markakteure frei verfügbar sind. Das Kartellrecht scheint für das Thema Datenteilen und Datenzugang mit Bezug zum Mobilitätssektor im Untersuchungskontext eine grundsätzlich geeignete Materie zu sein. Selbst bei Vorliegen aller Voraussetzungen der Essential-Facilities-Doktrin sind aber die Fragen der Datenportabilität sowie der Latenzzeit des Datenzugriffs in diesem Kontext nicht geklärt. Der Anspruch umfasst die Belieferung mit Daten, weshalb es aber nur um bereits bestehende (und möglicherweise sogar aufbereitete) Daten(sätze) gehen kann. Mit Blick auf die für innovative Geschäftsmodelle relevanten Echtzeitdaten wäre ein direkter Zugriff auf Rohdaten (Daten, die nicht aufbereitet sind und die man so direkt wie möglich am entsprechenden Sensor ausliest) notwendig. Zudem wäre es in diesem Kontext auch notwendig, dass Marktakteure auf nachgelagerten Märkten entlang der Wertschöpfungskette nicht nur Zugang zu (fahrzeuggenerierten) Daten erhalten, sondern auch Daten an das Fahrzeug zurücksenden können und mit dem Fahrer eines Fahrzeuges auch über alle vorhandenen Kommunikationsschnittstellen kommunizieren können.

Ebenso unklar ist, ob die Fahrzeughersteller zur Entwicklung offener interoperabler Telematikplattformen verpflichtet werden können. Zu erwähnen bleibt schließlich, dass das Wettbewerbsrecht – selbst bei Vorliegen der Voraussetzungen – traditionell nur eingeschränkt geeignet ist, Dritten den erforderlichen Zugang zu den Daten zu ermöglichen. Grund hierfür ist, dass derartige Verfahren sehr viel Zeit in Anspruch nehmen und damit in schnelllebigen Märkten wie jenem der Datenökonomie für die Dritten in der Regel keine ausreichende Abhilfe schaffen.

Die Automobilwirtschaft hat versucht, durch die Entwicklung und Anwendung eigener Konzepte die Kontrolle über die Datenflüsse zu behalten („extended vehicle-Konzept“) und damit auch die Möglichkeit zu schaffen, die dadurch entstehenden Wettbewerbsvorteile auf Sekundärmärkten für abgeleitete Produkte und Dienstleistungen für das connected car zu erhalten und zu nutzen. Gleichzeitig wurden von anderen Stakeholdern alternative Konzepte entwickelt, die einen gleichen und fairen Zugang für

alle Beteiligten ermöglichen sollen und damit dem Ziel eines fairen und innovationsfördernden Wettbewerbs besser gerecht werden können (Data Shared Server-Konzept, OTP-Konzept).

Die privatwirtschaftlichen Konzepte und Projekte zum (zukünftigen) Austausch von Daten in der Automobilwirtschaft zwischen den Marktakteuren lassen sich in zwei sich gegenüberstehende Lager einteilen, die jeweils unterschiedliche technische Ansätze verfolgen und von jeweils unterschiedlichen Interessensvertretern propagiert werden. Zudem unterscheiden sich die Modelle auch hinsichtlich ihres zeitlichen Umsetzungshorizontes.

In **Arbeitspaket 3** wird zunächst der derzeit noch im Gesetzgebungsprozess befindliche Entwurf des Data Act in den Kernpunkten dargestellt und unklare Punkte herausgearbeitet, wobei auch mögliche Änderungen und Ergänzungen vorgeschlagen wurden. Das Modell des DA-E wird dann auf die bereits praktizierten oder in der Diskussion befindlichen Konzepte zur Data Governance beim connected car angewandt und dabei der Einfluss auf die bestehenden Datenflüsse und der Grad der Kompatibilität zwischen den Konzepten und dem DA-E herausgearbeitet. Es ergibt sich, dass der DA-E grundsätzlich mit allen drei Hauptkonzepten zu einem unterschiedlichen Grad kompatibel ist. Allerdings gilt dies für das extended vehicle-Konzept nur sehr eingeschränkt, da das nutzerzentrierte Modell des DA-E dem Hersteller die Kontrolle über die Datenverwendung („Gatekeeper“-Position) nimmt und dies den Kern etwa von ADAXO darstellt.

Im Einzelnen ergibt sich, dass die Rollenverteilung, die dem DA-E zugrunde liegt, auch die Verhältnisse beim connected car widerspiegeln. Allerdings wird mit es zunehmend schwieriger werden, den Nutzer zu bestimmen, etwa bei Geschäftsmodellen mit häufig wechselnden Fahrern. Hinsichtlich der Art der Zugangsgewährung ist der DA-E noch nicht ganz klar. Ein Echtzeitzugriff wird von ADAXO und auch beim Data Shared Server-Konzept nicht bereitgestellt, ist aber nach dem DA-E nicht bedingungslos zu gewähren. Besonders problematisch ist die Regelung, dass die Zwecke der Verwendung der erlangten Daten zwischen Nutzer und Drittem geregelt werden, so dass der Dateninhaber insoweit nach dem DA-E die Kontrolle über die Datenverwendung verliert. Dies ist mit dem extended vehicle-Konzept, anders als hinsichtlich der beiden anderen Hauptkonzepte, nicht vereinbar. Der DA-E ist hier auch unklar, was die Grenzen einer Zweckbestimmung angeht. Vor allem ist nicht klar, ob auch eine nicht zweckgebundene Weitervermarktung der Daten auf Datenmärkten abgedeckt ist. Diese Möglichkeit scheint nicht ausgeschlossen, steht aber in gewissem Widerspruch zu dem Bestreben, die Entwicklung von Konkurrenzprodukten auf dem Primärmarkt aus den erlangten Daten auszuschließen. Auch wird die Möglichkeit für den Dateninhaber beim extended vehicle-Konzept, strategische Informationen über die durch Wettbewerber genutzten Daten zu erlangen („business monitoring“), durch den DA-E nicht beseitigt.

Weiterhin ergibt die Analyse des DA-E, dass dieser hinter dem Ziel der Schaffung von fairen und innovativen Wettbewerbsbedingungen zurückbleibt. Dies gilt einmal durch die Beschränkung auf Rohdaten und Ausschluss von aggregierten und abgeleiteten Daten, die ebenfalls für die Innovation auf Sekundärmärkten von Bedeutung sein können. Dies wurde im Gesetzgebungsprozess zumindest insoweit nachgebessert, als die erste Aufbereitung der Rohdaten („curation“) in den Anwendungsbereich einbezogen wurde. Es bleibt jedoch bei der Beschränkung des Zugangs auf generierte Rohdaten. Auch ist es für innovative Entwicklungen wichtig, dass dritte Diensteanbieter Zugang zu den Funktionen des Fahrzeugs, einschließlich eines Schreibzugriffs, bekommen sowie zur Kommunikationsschnittstelle mit dem Nutzer (HMI). Dies wird vom DA-E nicht gewährleistet. Weiterhin wird zu Recht kritisiert, dass der DA-E zu wenig zur Förderung der für den Wettbewerb esentiellen Interoperabilität von Daten und Diensten beiträgt. Letztlich bestehen auch ernsthafte Zweifel, ob das nutzerorientierte Modell des DA-E sich in der Praxis umsetzen lässt. Hier scheint die vorausgesetzte Datensouveränität des Nutzers aufgrund der entstehenden Transaktionskosten und auch der Probleme bei der Umsetzung von FRAND-Bedingungen in der Praxis kaum herstellbar. Dann wären aber auch die positiven Ansätze des DA-E wirkungslos.

Insoweit ist es nur folgerichtig, dass die EU-Kommission gerade den Mobilitätssektor als ersten Kandidaten für sektorspezifische ergänzende Regelungen sieht und eine Initiative zur Erweiterung der TypGVO ergriffen hat. In einem nächsten Schritt werden in der Studie daher zunächst die bestehenden spezifischen Regelungen auf ihre Kompatibilität mit dem DA-E untersucht und verbleibende Lücken herausgearbeitet. Dabei ergibt sich, dass diese hinsichtlich der einbezogenen Daten einem funktionsorientierten Ansatz folgten, der den Zugang zu den für den jeweiligen Dienst benötigten Daten einbezieht, und daher sachgerechter als eine Beschränkung auf Rohdaten ist. Allerdings geht der DA-E mit der Ermöglichung von Echtzeitzugriff unter bestimmten Voraussetzungen über die spezifischen Regelungen hinaus. Ein großer Vorteil der spezifischen Regelungen ist die Gewährung eines direkten Zugangsanspruchs für Dritte, was die Schwächen des nutzerorientierten Modells des DA-E vermeidet. Letzteres ist mit den sektorspezifischen Regelungen nicht vereinbar. Es bleibt aber bei den bestehenden spezifischen Regelungen das Problem des eingeschränkten Anwendungsbereichs, etwa auf Reparatur- und Wartungsarbeiten. Außerdem ist weder ein Echtzeitzugang noch ein Zugriff auf Funktionen und HMI gewährleistet. Auch das Business Monitoring wird nicht klar ausgeschlossen. Die Anwendung des allgemeinen und im Hinblick auf die Datennutzung überarbeiteten Kartellrechts ist derzeit in ihrer Effektivität kaum abzuschätzen. Es lässt sich aber feststellen, dass dieses nicht als vollwertige Alternative zu spezifischen Regelungen anzusehen ist, sondern allenfalls in Zukunft ergänzende Bedeutung vor allem für marktbeherrschende Unternehmen erlangen kann. Insoweit ist eine detaillierte sektorspezifische Regelung vorzugswürdig.

Einige „Querschnittsthemen“ zur derzeitigen regulatorischen Diskussion werden näher analysiert. Die Sicherstellung von Datensicherheit als wichtigem Interesse aller Stakeholder ist mit allen drei Hauptkonzepten des Data Governance bei connected cars vereinbar, wie am Beispiel der UNECE R 155 und R 156 aufgezeigt werden konnte, und ein Ausgleich zwischen Zugang und Datensicherheit kann gelingen.

Ein wichtiges und zu schützendes Gegeninteresse der Hersteller zum Datenzugang ist der Schutz von Betriebs- und Geschäftsgeheimnissen. Ein Geheimnisschutz ist grundsätzlich auch bezüglich einzelner Daten oder Datensätze möglich, allerdings dürfte die praktische Bedeutung grundsätzlich eher gering sein. Der DA-E sieht einen grundsätzlichen Vorrang des Datenzugangs unter größtmöglicher Sicherstellung von Schutzmaßnahmen zugunsten des Geheimnisschutzes vor. Dieser Ansatz im ursprünglichen Entwurf des DA-E ist sinnvoll und notwendig, um ein „overclaiming“ in Bezug auf Geheimnisschutz zu verhindern und die Effektivierung der Zugangsrechte zu sichern. Die im Gesetzgebungsverfahren eingeführte Spezifizierungslast des Geheimnisinhabers kann dies sinnvoll unterstützen und lässt sich in allen drei Konzepten für das Data Governance umsetzen. Im Fünften Kompromissvorschlag zum DA-E wurde allerdings eine Ausnahme vom Zugangsrecht geschaffen, die das Potenzial hat, die Effektivität der Zugangsgewährung durch den DA-E aufzuweichen und weiter zu schwächen.

Ein grundlegendes Problem ist auch die Vereinbarkeit des Datenzugangs mit dem bestehenden datenschutzrechtlichen Rahmen, vor allem der DSGVO. Da es sich bei den vom Datenzugang umfassten Daten im connected car überwiegend auch um personenbezogene Daten handelt, bedarf es zu deren Verarbeitung einer datenschutzrechtlichen Grundlage. Diese wird durch den DA-E selbst sowie die spezifischen Regelungen nicht zusätzlich geschaffen. Daher verbleibt es bei der Notwendigkeit einer Einwilligung des Betroffenen, deren strenge Voraussetzungen nach Art. 6 bis 9 DSGVO aber nicht einfach herzustellen sind. Hier kann vor allem der Einsatz von technischen Lösungen Abhilfe schaffen, etwa möglichst frühzeitiger Anonymisierung sowie von Personal Information Management Systems. Dies lässt sich ebenfalls mit allen drei Hauptkonzepten des Data Governance vereinbaren.

Defizite verbleiben nach der derzeitigen Gesetzeslage auch für die Möglichkeiten zum Datenzugang im öffentlichen Interesse, etwa Umweltschutz und Verkehrssicherheit. Der Zugang öffentlicher Stellen ist

sowohl nach DA-E, als auch nach der eCall-VO sowie der IVS-Gesetzgebung sehr eng begrenzt und teilweise nur auf freiwilliger Basis möglich.

Es wird dann weiterhin untersucht, inwieweit die verbleibenden Defizite durch die drei untersuchten Hauptkonzepte, die für das Data Governance im connected car bestehen bzw. diskutiert werden, kompensiert werden. Für das extended vehicle-Konzept bleibt das grundlegende Problem, dass der Dateninhaber seine Kontrollposition und damit die Möglichkeit behält, den Wettbewerb auf Sekundärmärkten einzuschränken und damit Innovation zu behindern. Dies ist bei den beiden weiteren Konzepten nicht mehr der Fall. Beim Data Shared Services-Konzept wird der Datenzugang über eine neutrale Plattform gewährt und dem Dateninhaber damit die Kontrolle über den Datenzugang entzogen, so dass dieser rechtlich und technisch diskriminierungsfrei ausgestaltet werden kann. Ein wichtiger Aspekt ist dabei die Funktionstrennung. Dies lässt sich gut umsetzen mit dem Einsatz von neutralen Datentreuhändern, wobei dabei auch ein differenziertes Rollenkonzept wie das des „Mobilitätsdatenwächters“ einsetzbar ist. Dies müsste regulatorisch vorgegeben werden. Beim Data Shared Server-Modell bleiben aber Defizite hinsichtlich des Zugangs zu Funktionen und HMI im Fahrzeug sowie der Ermöglichung eine Echtzeitzugangs.

Demgegenüber werden diese Defizite beim OTP-Modell durch die direkte Integration der offenen Plattform in das Fahrzeug vermieden. Hier wäre der direkte Zugang zu Daten und Funktionen ebenso wie zum HMI gewährleistet und dem Hersteller die Kontrolle technisch und rechtlich vollständig entzogen. Es müsste regulatorisch sichergestellt werden, dass der Hersteller diesen Verlust nicht durch vertragliche Restriktionen kompensieren kann, wobei der AGB-Kontrolle eine wichtige Rolle zukommt. Da bei diesem Konzept auch die weitreichendsten Anforderungen an Standardisierung und Interoperabilität bestehen, ergeben sich auch insoweit zusätzliche Regulierungsnotwendigkeiten, die noch einige Zeit zu ihrer Umsetzung in Anspruch nehmen werden.

Vor dem Hintergrund dieses regulatorischen Gesamtbildes werden dann die aktuellen Vorschläge der EU-Kommission zur Überarbeitung der TypGVO näher beleuchtet und bewertet. Dabei ergibt sich, dass der Vorschlag sektorspezifisch einen Großteil der verbleibenden Lücken des DA-E schließen könnte, vor allem den direkten Zugriff auf Funktionen und HMI sowie die Möglichkeit eines Fernzugriffs. Die Vorgabe eines entsprechenden Grundbestands sowie bestimmter Formate in Option 2 und 3 des Vorschlags ist zur Effektivierung der Zugangsrechte sinnvoll. Auch kann der Vorschlag zu einer angemessenen Berücksichtigung von öffentlichen Interessen beim Datenzugang führen. Einige Punkte wären aber weiter klarzustellen. Dazu gehört zum einen die Klarstellung, dass der Zugang unter FRAND-Bedingungen erfolgen soll. Zum zweiten wären wegen der Schwächen des nutzerzentrierten Modells Direktansprüche der Dritten vorzuziehen. Schließlich wäre auch zu regeln, ob die zweckungebundene Weitervermarktung der Daten auf Datenmärkten ausdrücklich zuzulassen wäre. Eine vollständige Öffnung der Daten auch für direkten Wettbewerb wird hier befürwortet, um Innovation bestmöglich zu fördern. Dies gilt natürlich unter der Einschränkung der Wahrung von Geheimnisschutz und Datenschutz, wie bereits ausgeführt.

Unter Einbeziehung dieser innovationsfördernden Aspekte des Vorschlags zur Überarbeitung der TypGVO und der Analyse der drei Hauptkonzepte für das Data Governance im connnected car ergeben sich aus der Studie konkrete Handlungsempfehlungen. Kernpunkt ist insoweit, ausgehend von den Überlegungen zur Überarbeitung der TypGVO, eine weitere regulatorische Flankierung, die eine Loslösung vom extended vehicle-Konzept und der damit verbundenen Erhaltung der Gatekeeper-Funktion der Fahrzeughersteller mit der Möglichkeit des Business Monitoring sicherstellt. Dazu sollte die Umsetzung des Prinzips der Funktionstrennung und entsprechender Treuhandlösungen einbezogen werden. Dies könnte zunächst auch auf der Basis des extended vehicle-Konzept erfolgen, soweit man den Zugang zu Daten, Funktionen und HMI unter FRAND-Bedingungen regulatorisch festschreibt und dazu jeweils einen entsprechenden Mindestbestand festschreibt. Dies wäre vorzugsweise durch Direktzugang der dritten Diensteanbieter über eine Schnittstelle im Fahrzeug zu gewährleisten. Da das Grundproblem der verbleibenden technischen Restkontrolle durch den

Fahrzeughersteller bleibt, ist langfristig eine Umsetzung des OTP-Konzepts anzustreben, das einen direkten Zugang dritter Diensteanbieter zu Daten, Funktionen und HMI in Echtzeit ermöglicht. Dies müsste regulatorisch abgesichert und flankiert werden durch die Etablierung eines Zugangs- und Berechtigungskonzepts, einschließlich der Regelung des Umfangs der weiteren Nutzung der Daten. Die Nutzung von Treuhandlösungen ist auch hier sinnvoll zu integrieren und kann ebenfalls der Compliance mit Anforderungen des Datenschutzrechts sowie des Geheimnisschutzes dienen. Wegen der umfangreichen Standardisierungsnotwendigkeiten bedarf es noch erheblicher Entwicklungsarbeit zur Implementierung. Dies schließt aber die Entwicklung entsprechender Regulierungskonzepte nicht aus, sondern diese kann im Gegenteil zur effektiven Umsetzung frühzeitig beitragen.

B. Einleitung

Das Konzept des „vernetzten Fahrzeugs“ ist gegenwärtig – neben der Elektromobilität, dem autonomen Fahren und der Mobilität als Dienstleistung – einer der bedeutendsten Trends in der Automobil- und Mobilitätsbranche und zugleich eine der größten Datenquellen der Gegenwart.[1] Moderne Fahrzeuge sind heute nicht länger Fortbewegungsmittel, sondern entwickeln sich zum „3rd living space“,[2] in dem die Freude am Fahren zunehmend durch die Freude beim Fahren abgelöst wird. Revolutionen in der Automobilwirtschaft werden heute nicht mehr durch neue Antriebstechniken ausgelöst, sondern durch den zunehmenden Grad der Konnektivität und Automatisierung des Fahrens. Die Konnektivität eines Fahrzeugs macht es als Device zum essenziellen Bestandteil der vernetzten Welt.

Das „vernetzte Fahrzeug“ (connected car) ist als ein umfassendes Konzept zu verstehen. Es wird als Fahrzeug definiert,

> *das mit vielen elektronischen Steuergeräten [...] ausgestattet ist, die über ein fahrzeuginternes Netzwerk miteinander verbunden sind, sowie mit Konnektivitätseinrichtungen, die es ermöglichen, Informationen mit anderen Geräten sowohl innerhalb als auch außerhalb des Fahrzeugs auszutauschen. Auf diese Weise können Daten zwischen dem Fahrzeug und den daran angeschlossenen persönlichen Geräten ausgetauscht werden, was beispielsweise die Spiegelung mobiler Anwendungen auf die im Armaturenbrett des Fahrzeugs integrierte Informations- und Unterhaltungseinheit ermöglicht. […].“*[3]

Die Konnektivitätsfunktionen eines vernetzten Fahrzeugs sind vielfältig.[4] Mit der Zunahme der Konnektivität von modernen Fahrzeugen auf dem Weg hin zum autonomen Fahren geht die Produktion immer größerer Datenmengen einher. Moderne Autos generieren schätzungsweise in der Stunde 25 Gigabyte an Daten, wobei dies nicht einmal der Datenmenge gleichkommt, die tatsächlich erfasst und durch die Fahrzeughersteller (OEM) gespeichert werden.[5] Diese variiert je nach den im Fahrzeug verfügbaren Diensten sowie den Anwendungsfällen. Die Menge der erzeugten Daten verspricht vielen Akteuren der Wertschöpfungskette der Automobil- und Mobilitätswirtschaft, insbesondere auf dem Sekundärmarkt, ein bedeutendes monetäres Potential.

Mit dem bereits seit vielen Jahren bestehenden Einsatz von Software und Sensoren in Kraftfahrzeugen entstand auch die Frage, wer die Kontrolle über die Daten ausüben soll und wem Zugang zu den erzeugten Daten zu gewähren ist. Diese auf connected cars bezogene Fragestellung ist nur ein, wenn auch besonders wichtiger, Ausschnitt aus der allgemeinen Diskussion über Data Sharing und einen Rahmen für Data Governance in der digitalen Wirtschaft, was sich zu einer Grundproblematik der Digitalisierung entwickelt hat.

Die Automobilwirtschaft hat versucht, durch die Entwicklung und Anwendung eigener Konzepte die Kontrolle über die Datenflüsse zu behalten („extended vehicle-Konzept“) und damit auch die Möglichkeit zu schaffen, die dadurch entstehenden Wettbewerbsvorteile auf Sekundärmärkten für abgeleitete Produkte und Dienstleistungen für das connected car zu erhalten und zu nutzen. Gleichzeitig wurden von anderen Stakeholdern alternative Konzepte entwickelt, die einen gleichen und fairen Zugang für

---

[1] Kienbaum, Connected-Car-Studie, 2016, abrufbar unter https://media.kienbaum.com/wp-content/uploads/sites/13/2019/05/New_Kienbaum_Connected_Car_Studie_2016.pdf.

[2] Bosch, The Car as 3rd living space, abrufbar unter https://www.bosch.com/stories/the-car-as-3rd-living-space/.

[3] European Data Protection Board, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0 vom 9. März 2021, S. 10, Rn. 21, abrufbar unter https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf

[4] *Holland/Zand-Niapour,* 2017; *Johanning/Mildner,* 2015; *Vogt*, Geschäftsmodelle für das vernetzte Fahrzeug, HNU Working Paper Nr. 30 (2014).

[5] Brandt, Statista - Datenschleuder Connected Car, abrufbar unter https://de.statista.com/infografik/8007/datenerzeugung-von-connected-cars-im-vergleich/.

alle Beteiligten ermöglichen sollen und damit dem Ziel eines fairen und innovationsfördernden Wettbewerbs besser gerecht werden können (Data Shared Server-Konzept, OTP-Konzept).

Die EU-Kommission hat die seit 2016 intensiv geführte Diskussion zu Eigentumsrechten an nicht-personenbezogenen Daten aufgegriffen und bereits 2017 erste Überlegungen zur Schaffung neuer Leistungsschutzrechte an Daten angestellt. Dies erwies sich jedoch theoretisch und praktisch als nicht angemessen. Mit dem Entwurf zum Data Act wurde ein alternativer Weg beschritten, der vor allem darauf abzielt, die exklusive Kontrolle der Dateninhaber aufzubrechen und Zugangsrechte für die Nutzer von IoT-Geräten zu schaffen, die dann indirekt auch Diensteanbietern auf Sekundärmärkten zugutekommen. Während der Mobilitätssektor einer der Hauptanwendungsbereiche des Data Act sein wird, bestehen zugleich bereits spezifische, eng begrenzte, Regelungen, die einen fairen Zugang von Reparatur- und Wartungsdiensten im Interesse der Verbraucher sicherstellen sollen.

Vor diesem Hintergrund ist es Ziel der Studie, die verschiedenen Ebenen aufzuarbeiten, ein differenziertes Bild der Gesamtsituation unter Einbeziehung der rechtspolitischen Diskussion und der rechtlichen Regelungsvorschläge zu erstellen und eine Bewertung unter dem Gesichtspunkt der Sicherung eines fairen und innovationsfördernden Wettbewerbs durchzuführen, die in konkreten Handlungsempfehlungen mündet.

C. Methodik

Zur Beantwortung der in den einzelnen Arbeitspaketen aufgeworfenen Fragen wurde zurückgegriffen auf bereits existierende Literatur zum Thema des vernetzten Fahrzeugs. Diese wurde systematisch recherchiert und ausgewertet. Dabei wurden unterschiedliche, sowohl wissenschaftliche als auch (fach-) journalistische, Informationsquellen sowie durch die Wirtschaft selbst in Auftrag gegebene Studien berücksichtigt. Die aus der Literaturanalyse gewonnenen Erkenntnisse wurden ergänzt um qualitative Experten-Interviews mit offenen Fragen. Der Interviewfragebogen ist der Studie als **Anlage** beigefügt. Ziel der mündlich geführten Interviews war es mit Blick auf den Data Act subjektive Einschätzungen verschiedener Betroffener (Automobilhersteller und Akteure auf dem After Market) und individuelle Perspektiven zu erhalten. Diese fanden Einfluss im Rahmen der Bewertung des Data Acts (Ziff. F).

Insgesamt wurden im Rahmen der Forschungsstudien sechs Experten-Interviews aus den Bereichen der Automobil- und Mobilitätsbranche geführt. An dem moderierten Experten-Interviews haben die folgenden Stakeholder teilgenommen:

(1) Zentralverband Deutsches Kraftfahrzeuggewerbe (ZDK)
(2) Allgemeiner Deutscher Automobil-Club e.V. (ADAC)
(3) Bosch
(4) BMW

Die Experten-Interviews wurden insbesondere mit Blick auf die Bewertung des Data Acts ausgewertet.

D. Arbeitspaket 1

Ziel des Arbeitspaketes 1 ist es darzustellen, welche Arten von (personenbezogenen und nicht personenbezogenen) Daten gegenwärtig und zukünftig mit Bezug zu dem Fahrzeug und dem Fahrer im Rahmen der Nutzung des sogenannten „connected car" bzw. „vernetzen Fahrzeug" durch die Fahrzeughersteller erfasst, gespeichert und verarbeitet werden.[6] Zudem soll aufgezeigt werden, für welche Marktakteure entlang der gesamten Wertschöpfungskette der Automobil- und Mobilitätswirtschaft diese Daten im Rahmen der Entwicklung innovativer Dienste und Geschäftsmodelle von Bedeutung sein können. Abschließend wird ein Überblick über die bedeutendsten bereits heute angebotenen und zukünftig zu erwartenden datenbasierten Konnektivitätsdienste und Geschäftsmodelle dieses Wirtschaftssektors gegeben.

I. Datenerzeugung und Datenarten im vernetzen Fahrzeug

1. Datenerzeugung zur Konnektivität

Im vernetzten Fahrzeug werden Daten erzeugt und verarbeitet, unabhängig davon, ob es sich im Bewegungs- oder Ruhezustand befindet.[7] Dazu werden Telematikboxen, mobile Anwendungen (z.B. Zugriff von einem Gerät des Fahrers) und insbesondere Fahrzeugsensoren genutzt.[8] In einem modernen Fahrzeug sind heutzutage weit mehr als 100 unterschiedliche Zustands- und Fahrsensoren eingebaut, wobei die Tendenz deutlich steigt.[9] Diese Sensoren werden oftmals als „Sinnesorgane des Fahrzeuges" bezeichnet.[10] Zur Gewinnung der Daten ist eine Vielzahl von Technologien im vernetzten Fahrzeug integriert, die einer rasanten Entwicklung unterliegen.[11]

Grundsätzlich erfolgt die Datenerzeugung im modernen vernetzten Fahrzeug mit Hilfe von miteinander vernetzten Multifunktionskameras,[12] Radar-, Ultraschall- und Lidarsensoren.[13] So werden unterschiedliche Bereiche des vernetzten Fahrzeugs (Fahrerbereich, Fahrzeuginnenbereich, Fahrzeugumfeld etc.) von unterschiedlichen Sensoren mit unterschiedlichen Messprinzipien zu unterschiedlichen Zwecken überwacht. Dabei lassen sich im Wesentlichen zwischen zwei Arten von Sensoren unterscheiden:

- **Sensoren zur Erhebung von internen Daten** (z.B. Beschleunigungssensor, Pedalweggeber,[14] Reifenluftdruckverlust-Sensor,[15] Tankdrucksensor, Sitzbelegungssensor, Drehzahlsensor[16]) und

---

[6] Auf die datenschutzrechtlichen Aspekte der Datenverarbeitung im vernetzten Fahrzeug wird im Rahmen dieser Studie nur am Rande eingegangen. Zu den datenschutzrechtlichen Fragen im Zusammenhang mit vernetzten Fahrzeugen vgl. European Data Protection Board (EDPB), Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0 vom 9. März 2021, S. 10, Rn. 21, abrufbar unter https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf.

[7] ADAC e.V., Spion im Auto: Diese Fahrzeugdaten werden gespeichert, 19.08.2022, abrufbar unter https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/daten-modernes-auto/#diese-fahrzeugdaten-werden-gesammelt.

[8] European Data Protection Board, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0 vom 9. März 2021, S. 11, Rn. 28, abrufbar unter https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf.

[9] *Kreutzer/Lahmann/Schallaböck,* 2016, S. 64; *Gatzke* et al., 2016, S. 19.

[10] *Gatzke*, et al., 2016, S. 19.

[11] Für einen Überblick über die verbauten Technologien im vernetzten Fahrzeug auf dem Weg zum autonomen Fahrzeug, vgl. z.B. https://www.bosch-mobility-solutions.com/de/mobility-themen/automatisierte-mobilitaet/.

[12] Zur Funktionsweise von Multifunktionskameras, vgl. https://www.bosch-mobility-solutions.com/de/loesungen/kamera/multifunktionskamera/.

[13] Für eine Übersicht der im vernetzten Fahrzeug verbauten Sensoren, vgl. *Reif*, 2016.

[14] Diese Art erfasst den Bremswunsch des Fahrers, vgl. https://www.bosch-mobility-solutions.com/de/?compId=1076#.

[15] Vgl. Continental, Wie das vernetzte Auto die Zukunft der Mobilität vorantreibt, abrufbar unter https://www.continental-reifen.de/autoreifen/stories/technologie-und-innovation/vernetztes-auto.

[16] *Reif,* 2016.

- **Sensoren zur Erhebung von externen Daten** (z.B. Frontkameras, Rückkameras, Radar, Lidar und Ultraschallsensoren, Notbremssensoren, Regensensor, Temperatursensoren).[17]

Die durch die Sensoren erhobenen internen wie externen Daten (Sensordaten) werden dabei in elektrisch messbare Signale weiterverarbeitet, die ein exaktes Bild des Fahrzeugumfeldes erstellen können.[18] Die Erhebung und Verarbeitung der Sensordaten verfolgt neben der möglichst exakten Umfelderfassung des Fahrzeugs den übergeordneten Zweck der Verbindung des Fahrzeugs mit dem Internet bzw. anderen Teilnehmern innerhalb und außerhalb des Verkehrsgeschehens (Vernetzung) sowie der Entwicklung und Nutzung unterschiedlichster Konnektivitätsfunktionen und -services (Kommunikation).[19]

Bereits heute sind einige der produzierten Autos mit über 50 Konnektivitätsfunktionen ausgestattet.[20] Insbesondere der Aspekt der Konnektivität bzw. Kommunikation ist beim vernetzten Fahrzeug von herausragender Bedeutung: So können vernetzte Fahrzeuge einerseits mit den im Fahrzeug selbst befindlichen Kontroll- und Steuereinheiten kommunizieren (sog. fahrzeuginterne Kommunikation).[21] Andererseits kann das vernetzte Fahrzeug über verschiedene Kommunikationskanäle in Echtzeit u.a. mit anderen Fahrzeugen (sog. Car-to-Car-Kommunikation), der öffentlichen Verkehrsinfrastruktur (sog. Car-to-Infrastructure Kommunikation) in der Umgebung,[22] aber auch mit anderen vernetzten Serviceanbietern (sog. Car-to-Enterprise, z.B. Werkstätten, Tankstellen, Hotels etc.) und Gegenständen durch den Austausch von Daten als Sender und Empfänger untereinander kommunizieren (sog. fahrzeugexterne Kommunikation).[23] Die Nutzungszwecke der fahrzeuginternen wie -externen Kommunikation liegen typischerweise in den Bereichen Verkehrssicherheit[24], Komfort, Zeitersparnis und Kostenreduktion.[25]

Mit der Erzeugung immer größerer Datenmengen und unzähliger Datenverarbeitungsvorgänge im vernetzten Fahrzeug wurden die bisherigen physischen, kabelgebundenen Schnittstellen im Fahrzeug im Sinne eines On-Board-Speichers zunehmend durch eine zentrale Telematik-Schnittstelle ersetzt. Über diese Schnittstelle werden die Daten heutzutage per Mobilfunk (sog. Over-the-Air Technologie) an die Fahrzeughersteller gesendet.[26] Die Over-the-Air Technologie ermöglicht Updates von Anwendungen, Diensten und Konfigurationen über das Mobilfunknetz – ohne physischen Kontakt. Für die Speicherung und Übertragung der Daten sowie für eine schnelle Kommunikation werden Cloud-Lösungen sowie Satelliten und Server bedeutender. Das vernetzte Fahrzeug kommuniziert damit in der Regel in einem geschlossenen „proprietären Datenzugangssystem“ mit dem Hersteller. Da momentan

---

[17] *Reif*, 2016.

[18] *Gatzke* et al., 2016, S. 19.

[19] *Vogt*, Geschäftsmodelle für das vernetzte Fahrzeug, HNU Working Paper Nr. 30 (2014); *Stoklas/Wendt*, Das vernetzte und autonome Fahrzeug – Datenschutzrechtliche Herausforderungen, 2018, S. 8.

[20] Vgl. Continental, Wie das vernetzte Auto die Zukunft der Mobilität vorantreibt, abrufbar unter https://www.continental-reifen.de/autoreifen/stories/technologie-und-innovation/vernetztes-auto.

[21] Für die fahrzeuginterne Kommunikation kann beispielhaft an die Start-Stopp-Automatik von Fahrzeugen gedacht werden oder das Spurhalteassistenz-System.

[22] *Knorre/Müller-Peters/Wagner*, Die Big-Data-Debatte. Chancen und Risiken der digital vernetzten Gesellschaft. Wiesbaden 2020. Damit Vernetzung und Informationsaustausch möglich wird, müssen neben den Fahrzeugen selbst, auch die Verkehrsinfrastruktur mit der erforderlichen Technik ausgestattet sein.

[23] Vgl. *Wendt*, ZD-Aktuell 2018, 06034. Für die fahrzeugexterne Kommunikation lässt sich als Beispiel der Warnhinweis oder die Geschwindigkeitsreduzierung des Fahrzeugs bei der Erkennung von Geschwindigkeitsbegrenzungen nennen.

[24] Die bedeutendsten gesellschaftlichen Potentiale des vernetzten Fahrens werden in der Erhöhung der Verkehrssicherheit durch die Reduzierung von Verkehrsunfällen und eine Steigerung der Verkehrseffizienz durch intelligente Verkehrssteuerung gesehen, vgl. Bundesministerium für Verkehr und digitale Infrastruktur, 2015, S. 9; *Kielman/ Dettling*, 2014, S. 1.

[25] McKinsey, Monetizing car data. New service business opportunities to create new customer beneftis, 2016, abrufbar unter http://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%data/Monetizing-car-data.ashx.

[26] Gesamtverband Autoteile Handel (GVA), Stellungnahme vom 13.02.2020, Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkung für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), abrufbar unter https://www.gva.de/files/dokumente/GVA-Stellungnahme_Ref_Entw_10__GWB-Novelle_final.pdf.

jegliche Art der Datenbereitstellung und damit auch Kommunikation bei diesem Konzept (Extended Vehicle – ExVe, vgl. auch Ziff. E.II.1) über die Server der Fahrzeughersteller als sogenannte „Gatekeeper“ kanalisiert wird, haben Dritte lediglich begrenzt die Möglichkeit, Zugang zu den in diesem geschlossenen System erzeugten Daten zu erhalten.

2. Datenarten

Durch die Vernetzung und Digitalisierung von Fahrzeugen werden große Mengen an Daten bzw. Datenkategorien durch die Fahrzeuge selbst, den Fahrzeugfahrer, die Fahrzeuggäste sowie smarte Umgebungen produziert.[27] Das vernetzte Fahrzeug hinterlässt für die Allgemeinheit eine unsichtbare Datenspur, die mit dem Grad der Automatisierung des Fahrens zukünftig weiter steigt. Aufgrund der Vielfalt der im vernetzten Fahrzeug erzeugten Daten und der Möglichkeit zu ihrer Kombination kann von einer neuen Art der „Datenflut“ in diesem Kontext gesprochen werden.[28]

Welche Daten im vernetzten Fahrzeug verarbeitet werden, variiert stark nach Fahrzeughersteller, Modell des Fahrzeugs und zudem danach, ob der Fahrzeugfahrer die Übermittlung der Daten an den OEM aktiviert hat.[29] Im Wesentlichen lassen sich die Daten, die im Ruhezustand wie beim Gebrauch eines vernetzten Fahrzeugs erzeugt werden können, aber in die folgenden drei Kategorien einteilen:

1. **Umgebungsdaten**
2. **Fahrzeugbezogene Daten und**
3. **Fahrerbezogene Daten**

Das nachfolgende Schaubild (vgl. **Abb. 1**) gibt einen Überblick über die zu diesen drei Kategorien gehörenden Daten im vernetzten Fahrzeug, die in der Regel erzeugt und verarbeitet werden. Neben den drei zuvor genannten Gruppen können ebenso drittanbieterbezogene Daten von z.B. Versicherungen, Navigationsdienstleistern etc. erzeugt und verarbeitet werden.[30]

[27] *Flügge*/*Roth,* Erlebnisraum Auto. In: Flügge, Smart Mobility in der Praxis: Das Auto – unverzichtbar für den intermodalen Verkehr?, S. 53-55; *Vieweg*, 2015, S. 1; *Karaboga et al.,* 2015, S. 18.

[28] *Niederländer/Katzlinger*, Digital Business für Verkehr und Mobilität – Ist die Zukunft autonom und digital?, Teil 7, Rn. 9; *Reiter/Methner/Schenkel/Kinzler,* „Neutrale Server“ für Fahrzeugdaten: Garant für Datenschutz und Datensicherheit am Beispiel des Fahrmodusspeichers, S. 153, 156, in: Stiftung Datenschutz, Datenschutz im vernetzten Fahrzeug, 2020.

[29] ADAC e.V., Spion im Auto: Diese Fahrzeugdaten werden gespeichert, abrufbar unter https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/daten-modernes-auto/#diese-fahrzeugdaten-werden-gesammelt. 19.08.2022; bei vielen Fahrzeugherstellern kann der Fahrer Einstellungen zu seiner „Privatsphäre“ selbst treffen und damit festlegen welche Daten über ihn gespeichert werden.

[30] *Barth,* Big Data Analytics für Connected Cars, in: Proff/Fojcik, Mobilität und digitale Transformation: Technische und betriebswirtschaftliche Aspekte, S. 137-151; *Hornung*, Ökonomische Verwertung und informationelle Selbstbestimmung, in: Roßnagel/Hornung, Grundrechtsschutz im Smart Car - Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug, S. 109-126.

Abb. 1 – Übersicht über die im vernetzten Fahrzeug erzeugten Daten[31]

3. Nutzungszwecke der Daten

Die durch die Datenverarbeitung im vernetzten Fahrzeug gewonnen Erkenntnisse dienen einer Vielzahl von Datenverarbeitungszwecken. Dazu zählen insbesondere:

- **Fahrersicherheitszwecke**
- **Versicherungszwecke**
- **Verkehrseffizienzzwecke**
- **Umweltzwecke**
- **Unterhaltungs- und Informationszwecke bis hin zu**

[31] Angelehnt an *Hansen*, Kampf um die Datenhoheit, c´t 1/2022, 2, 20 f.

- **Marketingzwecke.**

Grundlegend lässt sich der Nutzungszweck der erzeugten Daten je nach Kategorie der Daten (vgl. Ziff. 2) wie folgt beschreiben:

1. **Umgebungsdaten** dienen primär dem Zweck der **Erhöhung der Verkehrssicherheit**.
2. **Fahrzeugbezogene Daten** dienen primär dem **Zweck der Produktverbesserung durch die Automobilhersteller.**
3. **Fahrerbezogene Daten** sind besonders für **Anbieter softwarebasierter Dienste und Anwendungen** interessant, weil sich auf ihrer Basis mit Hilfe von Big Data Analysen neue digitale Dienste und Anwendungen für Autofahrer entwickeln lassen.[32] Hierbei sind nicht zwingend die Daten eines bestimmten Fahrers oder gar Fahrzeugherstellers interessant, sondern gleichermaßen die Masse an Daten aus unterschiedlichen Fahrzeugen.

   Werden die im vernetzten Fahrzeug erzeugten Daten softwarebasiert verarbeitet, kombiniert, integriert, analysiert, geclustert bzw. visualisiert, lassen sich hieraus fahrerbezogene Nutzungsprofile ableiten. Dazu zählen Persönlichkeits-, Bewegungs-, Fahrverhaltens- und sonstige Verhaltensprofile sowie individuelle Fahrerpräferenzen. Aus diesen Profilen ergeben sich wiederum z.B. Rückschlüsse auf die Intensität der Nutzung, die Anzahl der Fahrer, den Fahrstil und die Typisierung des Fahrers.

   Wie vielfältig, die aus den erzeugten Daten ableitbaren Erkenntnisse sind, zeigt beispielhaft die folgende Übersicht (vgl. **Abb. 2**)[33], die eine weitere Differenzierung der Nutzungszecke vornimmt:

[32] *Stricker/Wegener/Anding*, 2014, S. 5 ff.; *Weisser/Färber*, MMR 2015, 506 f.
[33] Vgl. *Hansen*, Kampf um die Datenhoheit, c´t 1/2022, 2, 20 f.

Datum	Erkenntnis
Umgebungsdaten	
Umwelt	Das Fahrzeug erfasst lokale Daten der Umwelt, wie z.B. Wetterdaten und Luftwerte für die Motorsteuerung.
Kamerasysteme	Kamerasysteme erfassen das räumliche Umfeld des Fahrzeugs im Straßenverkehr. Dazu zählen Verkehrsteilnehmer wie z.B. Fußgänger, Radfahrer oder andere Fahrzeuge.
Fahrzeugkomponenten	Einzelne Fahrzeugteile erfassen ihren Zustand. Die Bremsschreiben etwa dokumentieren ihren Verschleiß oder die Reifen ihren Reifendruck.
Fahrbahnzustand	Kamerasysteme, Lidar über die Fahrzeugdynamik geben Hinweise zu der Fahrbahnbeschaffenheit.
Vernetzte Fahrzeug im Verkehr	Es werden Live-Verkehrsdaten gesendet zur Verkehrsdichte oder frei verfügbaren Parkplätzen.
Fahrzeugbezogene Daten	
On-Board-Diagnosesystem (OBD)	Überwachung wichtiger Fahrzeugsteuergeräte zur Gefahrenabwehr und Schonung der Umwelt und Verhinderung von Motorschäden. Zudem können Wartungs- und Reparaturarbeiten direkt ausgelesen werden.
Fehlerspeicher	Im Fehlerspeicher werden Meldungen der einzelnen Fahrzeugsysteme mit einem Zeitstempel erfasst und ausgelesen.
Fahrerbezogene Daten	
Kopplungen mit Smartphones	Rückschluss zu Fahrzeuginsassen
Anruflisten	Rückschlüsse auf Gesprächshistorie,
Kurznachrichten	SMS werden auf Fahrerwunsch gespeichert und mit dem Infotainmentsystem synchronisiert
Radiosender und Musikstreaming	Persönliche Fahrerpräferenzen zur Typisierung des Fahrers erkennbar sowie Hinweise auf Stimmungsbild des Fahrers
Sprachbefehle	Fragmente der Fahrzeugbefehle werden gespeichert und analysiert
Navigationsziele, Standortdaten, Routenprotokolle	Bewegungsdaten und regelmäßige Fahrrouten machen den Fahrer identifizierbar
Fahrmodusoptionen	Typisierung des Fahrers hinsichtlich seines Fahrverhaltens vom Eco- bis Sportmodus
Klimaeinstellungen	Anhand von Nutzungsgewohnheiten sind Fahrzeugfahrer unterscheidbar sowie Rückschlüsse zu Anzahl von Fahrgästen möglich
Müdigkeitswarnsystem	Durch Erfassung biometrischer Daten werden sicherheitsrelevante Informationen verarbeitet und Fahrer unterscheidbar
Airbag-Steuergerät	Aufklärung von Verursachungsbeiträgen an Unfällen
Sitzposition und Gurtsensor	Rückschlüsse zu Körpergröße, Gewicht, Insassenanzahl
Schließsystem	Bei Funkschlüsseln wird der Zeitpunkt des letzten Fahrzeugkontaktes gespeichert
Fahrzeugbeschleunigung und Bremsverhalten	Rückschlüsse zu Fahrstil und -verhalten
Eingriff in die Fahrdynamik durch Assitenzsysteme	Eingriff eines Assistenzsystems wird protokolliert und gibt Hinweise zum Fahrverhalten

Abb. 2 – Übersicht über die im vernetzten Fahrzeug erzeugten Daten

An Bedeutung für die Automobilindustrie gewinnt auch das „Emotional Monitoring“ als Teil des sogenannten „Driver Monitorings“ (DMS). Beim „Emotional Monitoring“ des Fahrers werden gewisse Gesundheitsparameter verarbeitet.[34] Ziel dieses Ansatzes ist es, die emotionale Verfassung des Fahrers, z.B. seine Konzentrationsfähigkeit zu analysieren,[35] um in Sekundenschelle entsprechende Gegenmaßnahmen (Anpassung von Musik, Lichtverhältnissen, Geschwindigkeitsreduzierung) im Falle von z.B. Müdigkeitsanzeichen oder einem aggressiven Fahrstil einleiten zu können.[36] Biometrische Daten gelangen auch zum Zweck der eindeutigen Identifizierung einer natürlichen Person in den Fokus der Automobilhersteller, etwa um dem Fahrer Zugang zu einem Fahrzeug zu ermöglichen, den Fahrer bzw. Fahrzeughalter zu authentifizieren oder den Zugriff auf die Profileinstellungen und Präferenzen eines Fahrers zu ermöglichen.

Parallel zeigen sich Entwicklungstrends, die neben dem Fahrzeugfahrer die Fahrzeuginsassen in den Blick nehmen (sog. Cabin-Monitoring System– CMS).[37] Dabei werden z.B. Atmung und Herzfrequenz weiterer Passagiere im Fahrgastraum mittels niederfrequenten Radars erfasst. Ziel dieser Entwicklung ist es u.a. zukünftig zu verhindern, dass Kleinkinder im geparkten Fahrzeug zu Schaden kommen.[38] Daneben können die mittels einer Kamera erfassten Bilder der Insassen (Insassendetektion) nach einem Unfall direkte an die Notrufzentrale übermittelt werden, sodass die Rettungskräfte auf ihren Einsatz bestmöglich einstellen können. Auch mit Blick auf Unterhaltungselemente beim Fahren bietet das Cabin-Monitoring neue Chancen. So kann auf Grundlage der durch die Innenraumkameras erzeugten Bilder das Infotainment-Display je nach Blickrichtung der Insassen optimiert gesteuert werden.[39] Bei modernen Fahrzeugen kommt diese Technologie bereits heute durch sog. Head-up-Displays, die in die Windschutzscheibe des Fahrzeugs projiziert werden, zum Einsatz.[40]

Tatsächlich können einige Arten personenbezogener Daten aus vernetzten Fahrzeugen auch Aufschluss darüber geben, ob eine Ordnungswidrigkeit, Straftat oder ein sonstiger Verkehrsverstoß begangen wurde (Event Data Recording – EDR). Als Beispiel kann das Airbag-Steuergerät angeführt werden, das den Einschlagwinkel des Lenkrades, Beschleunigungsdaten, sowie die Positionen des Brems- und Gaspedals in den letzten Sekunden vor dem Verkehrsereignis aufzeichnet.[41] Nach einem Unfall können Ermittlungsbehörden vom Fahrzeughersteller zur weiteren Aufklärung des Unfallhergangs – zumindest theoretisch – HD-Aufzeichnungen der Fahrzeugkameras sowie sonstigen Systeme erhalten. Ab dem Jahr 2022 wird das Event Data Recording (ereignisbezogenen Datenaufzeichnung – Black Box) zusammen mit dem Fahrer-Assistenzsystem zum Einhalten der Geschwindigkeitsbegrenzung verpflichtend für neue Fahrzeugmodelle und ab 2024 für alle Neufahrzeuge eingeführt.[42]

---

[34] Angelehnt an Infografik „Data and the connected car“ (Daten und das vernetzte Fahrzeug) des Future of Privacy Forum, abrufbar unter https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

[35] *Niederländer/Katzlinger*, Digital Business für Verkehr und Mobilität – Ist die Zukunft autonom und digital?, Teil 7, Rn. 7-14.

[36] Beispiele hierfür: Der Automobilhersteller Ford entwickelte ein sog. „Heart Rate Monitoring Seat“ der als EKG-Messsystem Gesundheitsdaten wie Herzschlag, Hauttemperatur oder Atmungswerte überwachen kann, abrufbar unter http://www.zeit.de/mobilitaet/2015-05/autofahrer-gesundheit-sensoren-autotechnik/seite-2; BMW entwickelte einen Nothalte-Assistenten, der das Fahrzeug auf Autobahnen oder ähnlichen Straßen ggf. auf einen seitlichen Stand- oder Pannenstreifen lenkt, abgebremst und automatisch einen SOS-Notruf an den Rettungsdienst mitsamt der Herz- und Kreislaufdaten des Fahrers absetzt, abrufbar unter https://faq.bmw.de/s/article/Fahrerassistenzsysteme-Intelligentes-Fahren-Nothalteassistent-Funktionsweise-Z2OLF?language=de.

[37] *Hansen*, Der Spion, den ich leaste, c´t 1/2022, 2, S. 19, 22.

[38] Ein solches CMS wurde jüngst durch Continental vorgestellt, vgl. Cabin sensing, abrufbar unter https://conti-engineering.com/technology-systems/components/hmi-components/cabin-sensing/.

[39] IAV, Vehicle In-Cabin-Monitoing, abrufbar unter https://www.iav.com/was-uns-bewegt/fahrzeuginsassen-im-blick/.

[40] *Geiger,* Hey! Augen auf die Straße!, 02.02.2021, abrufbar unter https://www.spiegel.de/auto/head-up-display-im-auto-innovationen-auf-der-frontscheibe-a-0d07d31b-2f93-40fd-87fe-e57931923a71.

[41] *Hansen*, Der Spion, den ich leaste, c´t 1/2022, 2, S. 19.

[42] EU-Kommission, 26. Januar 2022, zur Ergänzung der Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates durch Festlegung detaillierter Vorschriften für die spezifischen Prüfverfahren und technischen Anforderungen für die Typgenehmigung von Kraftfahrzeugen hinsichtlich ihrer Ereignisdatenspeicher und für die Typgenehmigung von Ereignisdatenspeichern als

II. Marktakteure der Wertschöpfungskette in der Automobil- und Mobilitätwirtschaft

Das Ökosystem des vernetzten Fahrzeugs eröffnet einer Vielzahl von Marktteilnehmern den Zugang zu innovativen Geschäftsmodellen in der Automobil- und Mobilitätsbranche, wodurch die bisher unantastbaren Geschäftsmodelle revolutioniert werden. Interessenten in der Wertschöpfungskette der Automobil- und Mobilitätsindustrie sind nicht länger ausschließlich die traditionellen Akteure, wie z.B. Fahrzeughersteller, Fahrzeugausrüstungshersteller und Automobilzulieferer, Reparaturwerkstätten und Vertragshändler.[43] Stattdessen treten vor allem neue Akteure aus der digitalen Wirtschaft in den Sekundärmarkt ein, die die Schnittstelle zum vernetzten Fahrzeug und damit die Fahrzeugdaten nutzen wollen, um ihre Dienstleistungen anbieten zu können. Diese neuen, oft branchenfremden, Wettbewerber bieten in der Regel softwarebasierte Konnektivitätsdienste für das vernetzte Fahrzeug an, z.B. Apps, Informations- und Unterhaltungsdienste wie Online-Musik, Straßenzustands- und Verkehrsinformationen oder Fahrerassistenzsysteme und -dienste wie Autopilot-Software, Aktualisierungen über den Fahrzeugzustand, nutzungsabhängige Versicherungen oder dynamisches Kartenmaterial. Auch Werbeunternehmen haben längst verstanden, dass das Auto der digitale Touchpoint für die individuelle Kundenansprache wird:[44] Sie versuchen sich am Markt rechtzeitig zu positionieren, um dem Fahrzeugführer sowie den Fahrzeuginsassen zukünftig mit personalisierter Werbung direkt im Fahrzeug oder entlang der Fahrroute zu erreichen.[45] Die Wertschöpfungspotentiale der im vernetzten Fahrzeug gewonnen Daten haben nicht als letztes auch die etablierten Automobilhersteller erkannt, die sich nicht mehr ausschließlich als Produktanbieter oder Mobilitätsdienstleister, sondern zunehmend auch als Service-Provider und IT-Dienstleister verstehen und entwickeln.[46]

Software wird im Kontext des vernetzten Fahrzeugs somit zur Schlüsseltechnologie. Die Neugewichtung zwischen Hardware und Software zur Verwertung des Datenschatzes im Ökosystem des vernetzten Fahrzeugs ist damit zu einem entscheidenden Wettbewerbsfaktor geworden.[47] Dies veranschaulichen auch Studienergebnisse aus dem Jahr 2019, wonach davon auszugehen ist, dass der Gewinn aus dem traditionellen Automobilherstellungsgeschäft (Verkauf, Teilverkauf und After-Sales-Services) bis zum Jahr 2030 um 55-70 % sinken wird, wohingegen der Gewinn branchenfremder Newcomer um 5-25 % steigen wird.[48]

Dieser digitalen Transformation begegnen einige Automobilhersteller mit ausgewählten strategischen Partnerschaften mit prominenten Softwareunternehmen anderer Branchen (z.B. Partnerschaft von Audi und Apple[49]; Partnerschaft von Pivotal mit Mercedes-Benz zur Entwicklung der Connected Car-App „Mercedes-Me“) um die bisherigen Branchengrenzen aufzubrechen und sich Marktanteile zu sichern.[50]

---

selbstständige technische Einheiten sowie zur Änderung von Anhang II der genannten Verordnung, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12989-Vehicle-safety-technical-requirements-test-procedures-for-EU-type-approval-of-event-data-recorders-EDRs-_en.

[43] *Roßnagel,* Zeitschrift für die Praxis der Verkehrsjuristen 2014, 281.

[44] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle., abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[45] *Schönfeld,* in: Hoeren/Kolany-Raiser, Big Data zwischen Kausalität und Korrelation, S. 63, 64.

[46] Hierauf wurde im Rahmen mehrerer Experten-Interviews hingewiesen.

[47] McKinsey, Mobility of the future – Opportunities for automotive OEMs, Februar 2012, abrufbar unter https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/automotive%20and%20assembly/pdfs/mobility_of_the_future_brochure.ashx.

[48] PWC, The 2019 Digital Auto Report: addressing market reality, abrufbar unter https://www.strategyand.pwc.com/de/en/industries/automotive/digital-auto-report.html.

[49] Audi integriert z.B. Apple Music in eine Vielzahl seiner Modelle, wodurch Kunden mittels Internet-Datenanbindung im Fahrzeug direkt und intuitiv über das Multi Media Interface (MMI) auf den Dienst zugreifen können. Mit der Mercedes-Me App kann der Fahrer Informationen über den Status seines Fahrzeugs wie Tankfüllstand, Reifendruck etc. in Echtzeit über sein Smartphone oder andere smarte Wearables abrufen.

[50] *Johanning/Mildner/Niederländer/Katzlinger*, Digital Business für Verkehr und Mobilität – Ist die Zukunft autonom und digital?, Teil 7, Rn. 8-19.

In diesem Zusammenhang ist zu erwarten, dass auch eine Gewichtsverschiebung zugunsten der Zuliefernetzwerke zu erwarten ist. Um der dynamischen Marktentwicklung stand zu halten, ist die Entwicklung datenzentrierter Software-Konzepte für die Automobilhersteller, gepaart mit dem Outsourcing weniger wettbewerbsentscheidender Aufgaben bezüglich der Produktherstellung, erfolgsentscheidend.[51]

Schaut man sich die Marktakteure entlang der gesamten Wertschöpfungskette der Automobil- und Mobilitätsindustrie im Detail an, lässt sich ein breites Spektrum von Wettbewerbern mit einem Interesse an der Verwertung der Daten identifizieren:

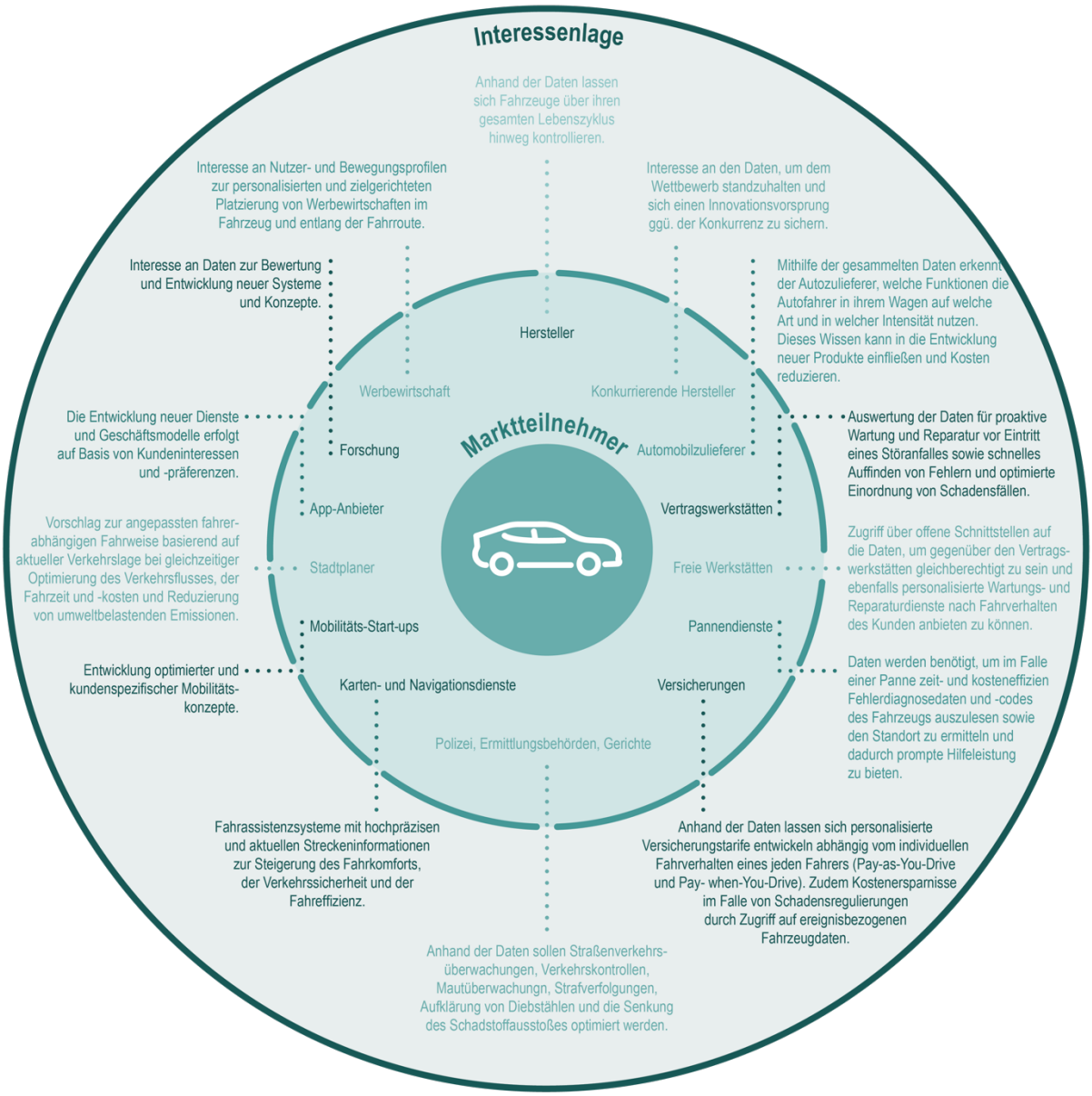


Abb. 3 – Übersicht über die Kategorien von Konnektivitätsdiensten und -Geschäftsmodellen[52]

[51] *Alich/Bauer/Danne/Gründinger/Martifgnoni/Rist/Schneider*, BVDW Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[52] Die Abbildung ist angelehnt an die Übersicht bei *Hansen*, Kampf um die Datenhoheit, c´t 1/2022, 2, S. 20 f.

III. Konnektivitätsdienste und Geschäftsmodelle in der Automobil- und Mobilitätswirtschaft

1. Übersicht

Die Analyse großer Datenmengen aus dem vernetzten Fahrzeug eröffnet für die Marktakteure der Automobil- und Mobilitätsindustrie die Chance, Dienste und Services sowie Geschäftsmodelle an den Bedürfnissen und Präferenzen des Nutzers zu entwickeln. Im Rahmen der Entwicklung von Konnektivitätsdiensten spielen darüber hinaus auch Kriterien wie die festgestellte Nutzungsart, Gebrauchshäufigkeit und Fahrverhaltensweise eine entscheidende Rolle. Im Mittelpunkt der Datenanalyse steht die Entwicklung individueller und personalisierter Dienste und Anwendungen, die das Fahren sicherer, effizienter und komfortabler machen.

Die bereits gegenwärtig verfügbaren Konnektivitätsdienste und -anwendungen im Kontext des vernetzten Fahrzeugs sind vielfältig, lassen sich grundsätzlich aber, gemessen an ihrem übergeordneten Ziel, wie folgt clustern, wobei die in diesem Zusammenhang möglichen Anwendungsfälle der einzelnen Cluster eine exemplarische (und keine abschließende) Auswahl darstellt:[53]

- **Fahrerassistenzsysteme (Advanced Driver Assistance Systems) und Verkehrssicherheit:** Fahrunterstützungssysteme zur Erhöhung der Verkehrssicherheit durch Warnung vor externen Gefahren und internen Reaktionen. Die Anzahl von Beispielen für solche Systeme ist umfangreich. Sie umfasst Sprach- und Gestensteuerung, Totwinkel-Kamera-Systeme; Geschwindigkeitsassistenten, Berganfahrhilfen; elektronische Stabilitätsprogramme, Notbremssysteme (Active Brake Assist) und -licht; automatische Unfallmeldung (eCall); Abbiege-Assistenten; Abstandsregeltempomat; Regen- und Lichtsensoren; Spurhalte-Assistenten; Rückfahrassistenten; Arbeitsscheinwerfer; automatisch aktivierbare Warnblinker, Müdigkeits- und Aufmerksamkeitswarner, Fußgängererkennung; Fahrzeugerkennung.
- **Mobilitäts-/ Navigationsmanagement**: Funktionen, die es dem Fahrer ermöglichen, durch eine an den Verkehrsereignissen und -umständen orientierte Routenplanung auf schnelle und kosteneffiziente Weise ein Ziel zu erreichen. Dazu werden Informationen in Echtzeit über die GPS-Navigation, potenziell gefährliche Umgebungsbedingungen (z. B. vereiste Straßen), Verkehrsstaus oder Straßenbauarbeiten, Unterstützung bei der Parkplatz- oder Werkstattsuche oder zur Optimierung des Kraftstoffverbrauchs oder der Straßenbenutzungsgebühren im Rahmen der Routenplanung berücksichtigt.[54] Auch Fahrpläne werden bereitgestellt, die auf den Zeiten verschiedener Verkehrsträger beruhen.
- **Fahrzeug-/ Wartungsmanagement**: Dienste mit dem Ziel der Senkung von Betriebskosten, der Verbesserung des Bedienkomforts und Erhöhung der Nutzerzufriedenheit. Dazu gehören Benachrichtigungen über den Fahrzeugzustand und Erinnerungen an fällige Servicearbeiten, maßgeschneiderte nutzungsabhängige Versicherungstarife, ferngesteuerte Bedienungen (z. B. der Standheizungsanlage) oder die Möglichkeit zur Konfiguration einzelner Fahrer-Profile (z. B. der Sitzposition, Temperatur, Radiosender). Dazu zählt auch das vorausschauende und personalisierte Wartungsmanagement (Predictive Maintenance) zur Ableitung von zeitlich perfektionierten Wartungsempfehlungen anhand der Echtzeit basierten Analyse von Maschinen- und Produktionsdaten. Ziel ist es Qualitätsstandards zu halten sowie Stillstände und

[53] EDPB, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, angenommen am 9. März 2021, S. 10, abrufbar unter https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf.

[54] EDPB, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, angenommen am 9. März 2021, S. 10, abrufbar unter https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf.

Störungszeiten zu vermeiden. Wartung und Auslastung der Werkstätten sowie das benötigte Inventar können effizient gesteuert werden.[55]

- **Infotainment und Entertainment**: Funktionen zur Information und Unterhaltung des Fahrers und der Insassen für eine erlebte Mobilitätserfahrung. Zu diesem Bereich zählen Funktionen wie beispielsweise Smartphone-Schnittstellen, Freisprechanlage, sprachgenerierte Textnachrichten oder WLAN-Hotspots. Umfasst sind Musik-, Video-, Videokonferenz- und Internetdienste sowie soziale Medien, mobiles Büro oder intelligente Haustechnik.[56]
- **Wohlbefinden:** Funktionen, die den Komfort, die Fahrfähigkeit und die Fahrtauglichkeit des Fahrers überwachen, wie z.B. die Müdigkeitserkennung des Fahrers.[57]

2. Ausgewählte Trends und Entwicklungsfelder im Bereich datengetriebener Konnektivitätsdienste und Geschäftsmodelle

Das Fahrzeug der Zukunft wird sich zu einer Art drittem Lebensraum für Fahrer und Insassen wandeln und dadurch ein ganzheitliches sowie hoch personalisiertes Nutzungserlebnis bieten sowie als neues vernetztes Device dienen, da eine Vielzahl neuer Interaktionsmöglichkeiten mit der Umwelt realisiert werden können.[58] Diese werden mit dem Fortschreiten der Technik sowie dem Forcieren des (teil-) autonomen Fahrens immer größere Relevanz entlang der gesamten Wertschöpfungskette erfahren.[59] Im Folgenden werden die bedeutendsten Trends digitaler und datenbasierter Dienste und Geschäftsmodelle aus dem Bereich des vernetzten Fahrzeugs überblicksartig dargestellt.

a) Car-to-X Technologie

Durch die fortschreitende Vernetzung von Fahrzeugen untereinander (Car-to-Car) und mit der Umwelt (Car-to-Infrastructure; Car-to-Pedestrian; Car-to-Home) wird eine Echtzeit-Kommunikation mit der Außenwelt (Car-to-X) möglich.[60] Diese Kommunikation führt basierend auf einer Art der Kollektivintelligenz z.B. zu einer effizienten Mobilität durch eine Reduzierung von Verkehrsüberlastungen, Verkehrsemissionen sowie Unfällen mit Toten und Verletzten. Die umfassende Vernetzung von Verkehrsteilnehmern mit der Umwelt ermöglicht zudem eine zeit- und ressourcen-optimierte Verkehrsführung durch die rechtzeitige Warnung vor Staus, Unfällen oder Pannen, aber auch Hinweise zu dem jeweiligen Straßenzustand.[61]

Auch wird durch die Car-to-X Technologie eine Vernetzung mit der Smart City z.B. zum einfachen Auffinden von verfügbaren Parkplätzen sowie dem Smart Home z.B. zum Laden eines Elektrofahrzeugs möglich.

---

[55] Fraunhofer Institut für Techno- und Wirtschaftsmathematik, Predictive Maintenance zur Optimierung von Anlagen-Effektivität, 2019, abrufbar unter https://www.itwm.fraunhofer.de/de/abteilungen/sys/maschinenmonitoring-und-regelung/predictive-maintenance-instandhaltung-machinelearning.html .

[56] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[57] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[58] *Flügge/Roth*, Erlebnisraum Auto. In: Flügge, Smart Mobility in der Praxis: Das Auto – unverzichtbar für den intermodalen Verkehr?, S. 49.

[59] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[60] ADAC e.V.: Car2X: Wie Kommunikationstechnik Unfälle komplett verhindert, vom 21.11.2022, abrufbar unter https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/car2x/.

[61] Fraunhofer Institut für Integrierte Schaltungen, Vernetzte Mobilität – Fahrzeugkommunikation, 2022, abrufbar unter https://www.iis.fraunhofer.de/de/ff/kom/automotive/vernetzte-mobilitaet.html .

b) Mobility-on-Demand

Mit dem Anstieg des Verlangens nach flexiblen Mobilitätslösungen und dem zunehmenden Bewusstsein für ökologische Aspekte sowie Verkehrsprobleme, ist zu erwarten, dass das traditionelle Geschäftsmodell des Fahrzeugkaufs oder Leasings zukünftig durch Mobility-On-Demand Services ergänzt wird. Bereits heute seien Tendenzen dafür zu erkennen, dass die Bedeutung des ausschließlich privat genutzten Fahrzeugs abnimmt und die geteilte Mobilität (Shared-Mobility) zunimmt, wobei diese Entwicklung durch Fahrautomatisierungsfunktionen zusätzlich angefeuert wird.[62] Nutzer verlangen integrierte und multimodale Mobilitätslösungen nach Bedarf, für einen bestimmten Zweck und über ihr Smartphone.[63]

Insbesondere in städtischen Ballungsräumen sind flexible Mobilitätslösungen gefragt. Es wird prognostiziert, dass sich insbesondere in diesen Räumen der multimodale Transport zu einem neuen Standard entwickeln wird, da die hier verfügbare größere System-Interoperabilität den Nutzern die Chance bietet sich mittels mehrerer Verkehrsmittel zu einem Festpreis, der über ein einheitliches Bezahlsystem erhoben wird, entsprechend ihren persönlichen Bedürfnissen fortzubewegen.[64]

c) Infotainment und Entertainment

Mit einem zunehmenden Grad der Automatisierung des Fahrens werden Nutzer, die im Fahrzeug verbrachte Zeit zunehmend als aktiv-produktive bzw. kreative Zeit verstehen. Das Fahrzeug wird ein Raum für den Konsum von informativen und unterhaltenden Audio- und auch Videoinhalten bieten.[65] Vor diesem Hintergrund wird sich die bisherige „Driving Experience“ im Fahrzeug immer stärker zu einer „User Experience“ entwickeln.[66]

Im Bereich des Infotainments und Entertainments im vernetzten Fahrzeug gibt es gegenwärtig zwei Wege, Konnektivitätsdienste zu nutzen. Zum einen können Dienste über verbaute Systeme – also Lösungen, die in das Computersystem des Automobils durch die Hersteller selbst integriert sind (sog. Embedded Solutions) – genutzt werden. Die Nutzeroberfläche ist bei dieser Lösung nicht mehr auf das zentrale Display im Fahrzeug begrenzt. Stattdessen wird das gesamte Fahrzeuginterieur von der Frontscheibe, dem Rückspiegel, den Armaturen und Seitenscheiben über Displays in Rückenlehnen und der Heckscheibe als mögliche Abbildungsfläche von Inhalten genutzt (Human-Machine-Interfaces, HMI). Nutzererlebnisse werden dadurch intuitiver und eng mit dem Fahrerlebnis selbst verbunden, sodass letztlich durch die Integration von Markenerlebnissen in das Fahrerlebnis ganzheitliche markenspezifische Erlebniskonzepte designt werden. Diese sollen den Kundenwert nachhaltig steigern.

Diese tiefintegrierten Infotainment- und Entertainmenterlebnisse werden auch als „Immersive Car Experience“ bezeichnet. Entwickelt und erprobt werden hier insbesondere audio-visuelle Erlebnisse, die das Fahrzeug zur live erlebten Spieleplattform oder einem Kinosaal werden lassen.[67] So werden Film, Sitzvibrationen, Sound und Innenlichtanimationen mit dem Fahrwerk kombiniert; Kissen und Lehnen an den Vordersitzen werden mit Hilfe kleiner Motoren in Vibrationen gebracht, um dem Nutzer

---

[62] Salesforce, Metastudie – Die Mobilität von morgen – Eine Herausforderung für die Automobilindustrie, 2020, S. 15, abrufbar unter https://www.salesforce.com/content/dam/web/de_de/www/PDF/de-automotive-whitepaper-metastudies.pdf.
[63] McKinsey, Disruptive trends that will transform the auto industry, 2016, abrufbar unter https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry.
[64] Salesforce, Metastudie – Die Mobilität von morgen – Eine Herausforderung für die Automobilindustrie, 2020, S. 16, abrufbar unter https://www.salesforce.com/content/dam/web/de_de/www/PDF/de-automotive-whitepaper-metastudies.pdf.
[65] *Flügge/Roth*, Erlebnisraum Auto. In Flügge, B. (Hrsg), Smart Mobility in der Praxis: Das Auto – unverzichtbar für den intermodalen Verkehr?, S. 53-55.
[66] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.
[67] *Fuchslocher*, Entertainment im Fahrzeug – So mutieren Autos zu Spieleplattformen und Kinosälen, v. 13.10.2020, abrufbar unter https://www.automotiveit.eu/technology/so-mutieren-autos-zu-spieleplattformen-und-kinosaelen-315.html.

ein mit allen Sinnen wahrnehmbares ganzheitliches Spiele- oder Filmerlebnis bieten zu können. Zudem werden Lösungen erarbeitet, die es ermöglichen Bewegungen des Fahrzeugs beim Gaming in ein Spiel einzubinden und über Außenkameras am Fahrzeug die reale und virtuelle Umgebung miteinander zu verschmelzen.[68]

Neben den zuvor genannten Embedded Solutions stellt das Tethering den zweiten bedeutenden Trend im Bereich des Infotainments und Entertainments dar. Dieser Trend erfüllt die Erwartung der Nutzer ihr Smartphone nahtlos über USB, WLAN oder Bluetooth in das vernetzte Fahrzeug zu integrieren. Auf die auf dem Smartphone der Nutzer verfügbaren Applikationen kann nach der Integration dann über Spiegelungstechnologien (z. B. „Apple Car Play“) zugriffen werden.[69] Um den sicherheitsrechtlichen Aspekten ausreichend Rechnung zu tragen, werden die Anwendungen auf das Fahrzeugdisplay oder sogar eine Head Unit projiziert.

d) Functions-on-Demand

Bei den sogenannten Functions-on-Demand handelt es sich um käuflich erwerbbare Funktionen nach dem Fahrzeugkauf, also ein dazu buchbares Feature. Sie sind bedeutender Bestandteil neuer digitaler Geschäftsmodelle und bieten dem Nutzer nach Bedarf die Möglichkeit, das Fahrzeug seinen eigenen, auch temporär auftretenden, Bedürfnissen anzupassen. Die dazu benötigte Technik wird im Regelfall direkt im Rahmen der Fahrzeugherstellung verbaut, und die angebotene Funktion wird sodann per Lizenzkauf beim Hersteller (mittels eines Over-the-Air Updates) freigeschaltet. Damit eröffnen sich für Fahrzeughersteller auch nach dem Fahrzeugverkauf zusätzliche Einnahmequellen und dem Fahrer die Möglichkeit, individuelle Functions-on-Demand zu nutzen. Der Fahrzeughersteller Audi bietet als Function-on-Demand z.B. im Bereich der Lichttechnologie eine Nutzung der LED-Matrix-Scheinwerfer, im Bereich der Fahrerassistenzsysteme einen Parkassistenten oder im Bereich des Infotainments ein Smartphone Interface an.[70] Denkbar ist der Erwerb zusätzlicher Funktionen für flexible Laufzeiten, z.B. ein bis sechs Monate, ein bis drei Jahre oder lebenslang).[71] Weiterhin scheinen standortbasierte Services wie ein Karten-Upgrade, die GPS-Fahrzeugortung, die Nutzung des Navigationssystems oder die GPS-Fahrtenaufzeichnung al Function-on-Demand denkbar. Das gilt auch für Komfortfunktionen, wie z.B. eine Sitzheizung oder ein beheiztes Lenkrad.

e) Predictive Maintenance

Angesichts der zunehmenden Anzahl von assistierten Fahrsystemen im vernetzten Fahrzeug und der damit verbundenen Erhöhung von Verkehrssicherheit und Fahrkomfort, steht das bisherige Geschäftsmodell von Reparatur- und Wartungsservices im Falle von Fahrzeugpannen vor neuen Herausforderungen. Dieser Herausforderung begegnet der nachgelagerte Markt für

---

[68] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[69] *Öksüz/Schulze/Rusch-Rodosthemnous/Scheibel,* Connected Car nimmt Fahrt auf – Wohin steuert das Auto der Zukunft?, Verbraucherzentrale NRW, 2017, S. 15, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

[70] Audi, Functions on demands, abrufbar unter https://www.audi.de/de/brand/de/neuwagen/functions-on-demand.html?csref=sea:cdi:114169268289_kwd-982089533703&gclid=Cj0KCQiAm5ycBhCXARIsAPldzoXURS6NUc5WfD46R6YcGuONrWbmu6Gd20xwHbNmPSHIhUJWnARS7AUaAnzFEALw_wcB&gclsrc=aw.ds.

[71] ADAC e.V., Updates over the air: Wie das Auto per Software aufgefrischt wird, vom 27.07.2021, abrufbar unter https://www.adac.de/rund-ums-fahrzeug/reparatur-pflege-wartung/reparatur-rueckruf/updates-over-the-air/.

Fahrzeugreparaturen und -wartungen mit der Lösung einer prädiktiven Instandhaltung (Predictive Maintenance).[72]

Durch die in Echtzeit verfügbaren instandhaltungsrelevanten Fahrzeugdaten wird es möglich, Real-Time Diagnosen zu erstellen und so einer Fahrzeugpanne vorzubeugen, bevor sie tatsächlich auftritt. Ergänzend dazu können Wartungszyklen und Werkstatt-Termine personalisiert – je nach Fahrhäufigkeit und Fahrstil – terminiert werden. Diese Lösung erhöht auf der einen Seite die Zufriedenheit der Kunden, auf der anderen Seite bietet sie die Möglichkeit, die Wartung und Auslastung der Werkstätten und das benötigte Inventar effizienter zu steuern, was sich letztendlich auch positiv auf den Kundenservice auswirkt.

f) Pay-as-you-Drive und Pay-how-you drive

Auch in der Versicherungsbranche ist bereits ein Wandel sichtbar geworden: So werden die bisherigen Flatrate-Versicherungsmodelle abgelöst von telematikbasierten Modellen, die sich an der nutzerspezifischen Nutzungsintensität des Fahrzeugs sowie dem Fahrstil des Nutzers orientieren. Diese als „Pay-as-You-Drive“ (PAYD) bezeichneten Versicherungs-Tarife basieren auf einer Tarifierung des Risikos der Fahrweise (Pay-how-You-Drive) und einer nutzungsbasierten Bezahlung der Versicherung (Pay-when-You-Drive).[73] Telematik-Programme sollen einen Anreiz für einen verantwortungsvollen, sichereren Fahrstil oder auch für ein gesundheitsbewusstes Verhalten (Bewegung, Ernährung, etc.) setzen. Insbesondere die Pay-when-You-Drive Tarife orientieren sich an dem stark wachsenden Carsharing-Markt als ein On-Demand-Dienst.

Bedeutend für die Versicherungsbranche ist zudem der gesetzlich vorgeschriebene eCall als automatischer Notruf. Durch die real-time Erfassung der Unfalldaten durch diese Technologie wird es nicht nur möglich, schnelle und bedarfsorientierte Ersthilfe zu leisten. Auch die nachgelagerte Schadensregulierung lässt sich zeit-, und kosteneffizienter abwickeln.

[72] Fraunhofer Institut für Techno- und Wirtschaftsmathematik, Predictive Maintenance zur Optimierung von Anlagen-Effektivität, 2019, abrufbar unter https://www.itwm.fraunhofer.de/de/abteilungen/sys/maschinenmonitoring-und-regelung/predictive-maintenance-instandhaltung-machinelearning.html.

[73] *Alich/Bauer/Danne/Gründinger/Martignoni*, Connected Cars – Geschäftsmodelle, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

E. Arbeitspaket 2

Ziel des Arbeitspaketes 2 ist die Darstellung und Beurteilung bereits bestehender gesetzlicher Regelungen sowie die Darstellung und Analyse von Konzepten und Projekten zum Austausch von Mobilitätdaten in Deutschland. Im Einzelnen werden folgende Punkte näher untersucht:

- Nachdem im Arbeitspaket 1 dargestellt wurde, welche Daten derzeit und zukünftig in vernetzen Fahrzeugen erzeugt werden und welche Markteilnehmer mit welchen Geschäftsmodellen agieren (werden), wird in Arbeitspaket 2 aufgezeigt, inwiefern bereits sektorspezifische Datenzugangs- und Datennutzungsrechte, -pflichten und -anreize in der Automobilwirtschaft in Deutschland existieren.
- Es wird zudem ausführlich dargestellt, welche darüberhinausgehenden privatwirtschaftlichen Konzepte und Projekte zum (zukünftigen) Austausch von Daten in der Automobilwirtschaft zwischen den Marktakteuren in Deutschland derzeit diskutiert werden.
- Anschließend wird analysiert, inwiefern die zuvor aufgezeigten Zugangs- und Nutzungsrechte, -pflichten und -anreize sowie die dargestellten privatwirtschaftlichen Konzepte und Projekte zu einem diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich beitragen können.

I. Bestehende sektorspezifische Datenzugangs- und Datennutzungsrechte sowie -pflichten

Um die Gesetzeslage de lege lata hinsichtlich sektorspezifischer Datenzugangs- und Datennutzungsrechte sowie -pflichten in der Automobilwirtschaft in Deutschland darzustellen, ist eine literaturbasierte Recherche der in Betracht kommenden Normen sowie eine inhaltliche Analyse derselben erfolgt. Diesbezüglich wurde zunächst die bestehende Fachliteratur zum Forschungsthema ausgewertet.[74] Ergänzend konnten die ausgewählten Experten der Interviews hierzu befragt werden.

Nicht alle vorhandenen Datenzugangsregelungen sind zudem für die Marktakteure im Mobilitätsbereich und das Betreiben oder die Entwicklung von (innovativen) Geschäftsmodellen von Bedeutung, sondern zielen oft auf die Berechtigung von staatlichen Stellen zum Zugang zu bestimmten Fahrzeugdaten ab, oder die Regelungen enthalten Zwecke, die für den Untersuchungskontext nicht relevant sind. Auf diese Regelungen soll daher mit Blick auf den definierten Untersuchungskontext nicht weiter eingegangen werden, da sie innerhalb der Wertschöpfungskette in der Regel keinen direkten Beitrag zur Entwicklung oder zum Betrieb von (innovativen) Geschäftsmodellen leisten.[75]

1. Typengenehmigungsverordnung (EU) 2018/858

Bereits 2007 wurden in der Richtlinie 2007/46/EG[76], die den Rahmen für die Typgenehmigung von Fahrzeugen der Klassen M, N und O vorgab, Datenzugangsregeln verankert. So war der Zugang zu wesentlichen Reparatur- und Wartungsinformationen und Daten (insbesondere Fahrzeugdiagnosedaten), über welche nur die Fahrzeughersteller verfügen, normiert. Es sollte damit ein unverzerrter Wettbewerb zwischen den Fahrzeugherstellern (und ihren Vertragswerkstätten) und

[74] Zur Dokumentenanalyse als Methode der Rechtstatsachenforschung *Rehbinder*, Rechtssoziologie, 8. Aufl. 2014, S. 59 f.

[75] Zu nennen ist hier insbesondere § 63a StVG. Für Kraftfahrzeuge mit hoch- oder vollautomatisierter Fahrfunktion gilt gem. § 63a Abs. 3 StVG, dass die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben für den Fall eines Wechsels der Fahrzeugsteuerung zwischen dem Fahrzeugführer und dem hoch- oder vollautomatisierten System im Fahrzeug gespeichert werden müssen. § 63a Abs. 2 StVG regelt, dass die gespeicherten Angaben auf Verlangen an die für die Ahndung von Verkehrsverstößen zuständigen Behörden übermittelt werden dürfen und diese die Daten auch speichern und nutzen dürfen. Der Fahrzeughalter hat die Übermittlung dieser Daten gem. § 63a Abs. 3 StVG an Dritte zu veranlassen, etwa zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit einem in § 7 Abs. 1 StVG geregelten Ereignis. Ausführlich hierzu *Hoeren/Böckers*, JurPC Web-Dok. 21/2020, Abs. 1 – 148, abrufbar unter https://www.jurpc.de/jurpc/show?id=20200021#fn3; *Schmid/Wessels*, NZV 2017, 357.

[76] Richtlinie 2007/46/EG des Europäischen Parlaments und des Rates vom 5. September 2007 zur Schaffung eines Rahmens für die Genehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge (ABl. L 263 vom 9.10.2007, S. 1), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32007L0046&from=DE.

den unabhängigen Reparatur- und Wartungsbetrieben (sowie Ersatzteilherstellern) sichergestellt werden.[77] Die konkreten Anforderungen an die Bereitstellung von Reparatur- und Wartungsinformationen wurden in den Verordnungen (EG) Nr. 715/2007[78] und (EG) Nr. 595/2009[79] festgeschrieben.

Im September 2020 wurde die bisherige Richtlinie 2007/46/EG durch die neue Rahmenverordnung (EU) 2018/858[80] abgelöst, und die Anforderungen in den Delegierten Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 wurden geändert. Damit ist eine grundlegende Reform des europäischen Typgenehmigungsverfahrens erfolgt. Anbieter von Ersatz- und Zusatzteilen sowie Sensoren und Software für das offene Fahrzeug müssen sich den gleichen technischen Anforderungen stellen wie bei Modellzulassungen. Als wesentlich für ein besseres Funktionieren des Binnenmarkts wurde vom Verordnungsgeber der unbeschränkte Zugang zu Reparatur- und Wartungsinformationen mittels eines vereinheitlichten Formats zum Auffinden technischer Informationen[81] und ein wirksamer Wettbewerb auf dem Markt für Dienstleistungen zur Bereitstellung solcher Informationen angesehen.[82]

Gemäß Art. 61 Abs. 1 i. V. m. Anhang X der Rahmenverordnung (EU) 2018/858 unabhängigen Wirtschaftsakteuren gem. Art. 3 Nr. 45 (wie z. B. freie Reparatur- und Wartungsbetriebe) als sektorspezifischer wettbewerblicher Regelung für den Zugriff auf Fahrzeugdaten haben Fahrzeughersteller uneingeschränkten, standardisierten und diskriminierungsfreien Zugang über die standardisierte elektronische Fahrzeugschnittstelle (OBD)[83] auf standardisierte emissionsrelevante Fahrzeugdaten und proprietäre Fahrzeugdaten zu gewähren, insbesondere zu Fahrzeug-OBD-Informationen nach Art. 3 Nr. 49 sowie zu Reparatur- und Wartungsinformationen nach Art. 3 Nr. 48.[84] Es sind zudem einheitliche Formate der Informationsbereitstellung, regulatorische Maßnahmen mit Bezug auf die Fahrzeugsicherheit sowie eine Gebührenregelung für die Bereitstellung dieser Informationen enthalten.[85] Der Zugang zu sicherheits- und diebstahlrelevanten Reparatur- und Wartungsinformationen für Kfz-Betriebe wird durch das in Anhang X beschriebene SERMI-Schema gewährleistet und gilt für alle Fahrzeughersteller beziehungsweise typgenehmigte Fahrzeuge, die in der EU zugelassen werden. Die OBD-Schnittstellen müssen daher auch während der Fahrt offen bleiben.[86] Dies ermöglicht es Fahrzeughaltern und unabhängigen Herstellern, auf Fahrzeugdaten zuzugreifen,

[77] Erwägungsgrund 20 zur Richtlinie 2007/46/EG (ABl. L 263 vom 9.10.2007, S. 3).

[78] Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge (ABl. L 171 vom 29.6.2007, S. 1), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32007R0715&from=DE.

[79] Verordnung (EG) Nr. 595/2009 des Europäischen Parlaments und des Rates vom 18. Juni 2009 über die Typgenehmigung von Kraftfahrzeugen und Motoren hinsichtlich der Emissionen von schweren Nutzfahrzeugen (Euro VI) und über den Zugang zu Fahrzeugreparatur- und -wartungsinformationen, zur Änderung der Verordnung (EG) Nr. 715/2007 und der Richtlinie 2007/46/EG sowie zur Aufhebung der Richtlinien 80/1269/EWG, 2005/55/EG und 2005/78/EG (ABl. L 188 vom 18.7.2009, S. 1), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R0595.

[80] Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG (ABl. L 151 vom 14.6.2018, S. 1), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX%3a32018R0858&msclkid=50a9122bc52711ecbaba81329e042001.

[81] Hinsichtlich der Anforderungen an die Form der Informationen in der Verordnung (EG) Nr. 715/2007 vor der oben genannten Anpassung hat der EuGH festgestellt, dass Automobilhersteller nicht verpflichtet waren, unabhängigen Marktteilnehmern Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge in elektronisch weiterzuverarbeitender Form zu gewähren, EuGH, 19.9.2019, C-527/18, Rn. 37 - Gesamtverband Autoteile-Handel.

[82] Erwägungsgrund 50 der Verordnung (EU) 2018/858 (ABl. L 151 vom 14.6.2018, S. 7).

[83] Der normierte Standard ist OBD II. Die Fehlercodes (DTC – Diagnostic Trouble Code), auch P0-Codes genannt, sind in der Norm SAE J2012 bzw. ISO-Norm 15031-6 festgelegt, vgl. https://www.iso.org/standard/66369.html.

[84] Vgl. VO (EU) 2018/858, Annex X, Abschnitt 2.9: freier Zugang über den OBD-Port zur Diagnose, Wartung und Reparatur; direkter Datenstrom aus dem Fahrzeug über einen seriellen Anschluss gemäß der UN-Regelung Nr. 83, Anhang 11, Anlage 1, Nummer 6.5.1.4, und der UN-Regelung Nr. 49, Anhang 9B, Nummer 4.7.3.

[85] Vgl. Art. 63 VO (EU) 2018/858.

[86] Art. 61 Abs. 1 Satz 3, Abs. 6, Abs. 4 VO (EU) 2018/858, 2.9. Anhang X VO (EU) 2018/858 i.V.m. UN-Regelung Nr. 83 Anhang 11 Anlage 1 Nr. 6.5.1.4 und UN-Regelung Nr. 49 Anhang 9B Nr. 4.7.3.

zusätzliche Geräte anzuschließen (z.B. Telematik-Geräte) und neue Systeme zu entwickeln. Ab etwa Mitte 2023 bekommen Betriebe ohne Autorisierung keinen Zugang mehr zu diebstahl- und sicherheitsrelevanten Reparatur- und Wartungsinformationen über die Portale der Fahrzeughersteller und auch keine OBD-Informationen über deren Diagnosesysteme.[87]

2. Gruppenfreistellungsverordnung für den Kraftfahrzeugsektor (EU) 461/2010

Nach der Gruppenfreistellungsverordnung für den Kraftfahrzeugsektor (Kfz-GVO)[88] sind vertikale Vereinbarungen, welche die Bedingungen betreffen, unter denen die beteiligten Unternehmen neue Kraftfahrzeuge beziehen, verkaufen oder weiterverkaufen oder Reparatur- und Wartungsdienstleistungen für Kraftfahrzeuge erbringen dürfen, vorbehaltlich bestimmter Beschränkungen von der Anwendung des Art. 101 Abs. 1 AEUV freigestellt. In Bezug auf Vereinbarungen über den Verkauf oder den Weiterverkauf von Kraftfahrzeugersatzteilen oder die Erbringung von Instandsetzungs- und Wartungsdienstleistungen für Kraftfahrzeuge sieht die Kfz-GVO vor, dass Art. 101 Abs. 1 AEUV nicht gilt, sofern diese Vereinbarungen die Freistellungsvoraussetzungen der allgemeinen Vorschrift erfüllen und keine der in der Kfz-GVO aufgeführten Beschränkungen enthalten, die zum Ausschluss des Rechtsvorteils der Gruppenfreistellung führen. Die Ergänzenden Leitlinien[89] enthalten Grundsätze für die Beurteilung von bestimmten, durch solche Vereinbarungen aufgeworfenen Fragen nach Art. 101 AEUV.

Hinsichtlich Datenzugangsregelungen sieht die KfZ-GVO einen Zugangsanspruch zu technischen Informationen für unabhängige Marktbeteiligte vor.[90] Zur Verfügung gestellt werden sollen sämtliche mit dem zugelassenen Netzwerk (Werkstätten und/oder Teilehändlern) geteilte Informationen. Hintergrund ist, dass gerade in den Märkten für die Erbringung von Instandsetzungs- und Wartungsdienstleistungen für Kraftfahrzeuge die Wettbewerbsfähigkeit der Marktakteure von dem ungehinderten Zugang zu wesentlichen Vorleistungen wie Ersatzteilen und technischen Informationen abhängt.[91] Bezüglich des Zugangs unabhängiger Werkstätten zu technischen Informationen und Werkzeugen soll mit den Ergänzenden Leitlinien verhindert werden, dass Kraftfahrzeuganbieter ihre zugelassenen Werkstätten gegenüber unabhängigen Werkstätten bevorzugen, wenn es um die Bereitstellung von Daten geht, die vollständig vom Fahrzeughersteller kontrolliert werden und nicht von anderen Quellen bezogen werden können. Ein fehlender Zugang zu den erforderlichen technischen Informationen würde zu einer Schwächung der Marktposition der unabhängigen Marktteilnehmer führen, was insbesondere für die Verbraucher von Nachteil wäre, da dies eine erhebliche Verringerung der Auswahl an Teilen, höhere Preise für Instandsetzungs- und Wartungsdienstleistungen, eine geringere Auswahl an Reparaturwerkstätten und möglicherweise auch Sicherheitsprobleme zur Folge hätte.[92]

---

[87] Mit „SERMA“ („Secure Repair and Maintenance Autorisation“) stellt der Zentralverband Deutsches Kaftfahrzeuggewerbe e.V. (ZDK) Kfz-Servicebetrieben eine Erleichterung beim Zugang zu Reparatur- und Wartungsinformationen in Aussicht. Werkstätten, die das neue, standardisierte Autorisierungsverfahren nutzen, müssen sich künftig nicht mehr bei jedem einzelnen Fahrzeughersteller - nach unterschiedlichen Kriterien - autorisieren lassen, um Zugang zu geschützten Informationen zu erhalten. SERMA beinhaltet ein neues Akkreditierungsschema, welches markenfremde Betriebe gegenüber den jeweiligen Fahrzeugherstellern als sogenannte berechtigte Dritte ausweist. Dieses Konzept ist eine Umsetzung des SERMI-Schemas des Anhangs X zur Rahmenverordnung (EU) 2018/858, vgl. hierzu https://www.serma.eu.

[88] Verordnung (EU) Nr. 461/2010 der Kommission vom 27. Mai 2010 über die Anwendung von Artikel 101 Absatz 3 des Vertrags über die Arbeitsweise der Europäischen Union auf Gruppen von vertikalen Vereinbarungen und abgestimmten Verhaltensweisen im Kraftfahrzeugsektor (ABl. L 129 vom 28.5.2010, S. 52), abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:129:0052:0057:DE:PDF.

[89] Bekanntmachung der Kommission – Ergänzende Leitlinien für vertikale Beschränkungen in Vereinbarungen über den Verkauf und die Instandsetzung von Kraftfahrzeugen und den Vertrieb von Kraftfahrzeugersatzteilen (ABl. C 138 vom 28.5.2010, S. 16), abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:138:0016:0027:DE:PDF.

[90] Zu den Voraussetzungen der Kfz-GVO in den Anschlussmärkten und deren praktische Auswirkungen *Wegner*, BB 2010, 1803; *dies.,* BB 2010, 1867.

[91] Erwägungsgrund 13 zur Verordnung (EU) Nr. 461/2010 (siehe Fn. 92).

[92] Ergänzende Leitlinien (siehe Fn. 94), S. 25 Rn. 64.

Unklar ist insoweit, ob auch Rohdaten, welche dem Werkstattnetz in dieser Form in der Regel nicht zur Verfügung gestellt werden, zu den in diesem Zusammenhang zwingend herauszugebenden Informationen gehören. Dies wird aber dann der Fall sein, wenn (zukünftig) die betreffenden Informationen zur Identifikation der zu verwendenden Teile zwingend erforderlich wären[93] und auch dem Werkstattnetz in dieser Form zur Verfügung gestellt werden würden. Insgesamt soll der Begriff der technischen Informationen aber nicht starr sein, sondern sich mit den tatsächlichen Gegebenheiten und dem technischen Fortschritt weiterentwickeln.[94] Der Zugang muss in verwendungsfähiger Form ohne unangemessene zeitliche Verzögerung und zu angemessenen (nicht abschreckenden) Preisen zu gewähren sein. Die Kommission hat in diesem Zusammenhang darauf hingewiesen, dass es für die Frage, ob eine Information weiterzugeben ist, auch darauf ankommt, ob diese letztlich für die Reparatur genutzt wird.[95]

3. eCall-Verordnung (EU) 2015/758

Nach der eCall-Verordnung[96] müssen seit dem 31. März 2018 alle neu typgenehmigten Fahrzeuge der Klassen M1 und N1 so ausgestattet sein, dass nach einem Unfall ein Notruf an die Nummer 112 abgesetzt und ein Minimaldatensatz automatisch an die Notrufleitstelle übermittelt werden kann. Ziel ist es, den Zeitraum zwischen einem Unfall und dem Eintreffen der Rettungskräfte auf ein Minimum zu reduzieren. Die Verbreitung von eCall-Systemen steigt sukzessive mit der Marktdurchdringung von Fahrzeugen, die ab diesem Zeitpunkt typgenehmigt wurden.

Die Europäische Kommission hat als delegierten Rechtsakt die Delegierte Verordnung (EU) 2017/79[97] beschlossen. Diese Verordnung ergänzt und ändert die Verordnung (EU) 2015/758 zur Festlegung detaillierter technischer Anforderungen und Prüfverfahren für die Typgenehmigung von Kraftfahrzeugen hinsichtlich ihrer auf dem 112-Notruf basierenden bordeigenen eCall-Systeme, von auf dem 112-Notruf basierenden bordeigenen selbstständigen eCall-Einheiten und Bauteilen.

Über eine Funkverbindung werden permanent dynamische Daten, die für eine Notfallrettung relevant sind, aus dem Fahrzeug ausgelesen und gesendet. Der Minimaldatensatz ist standardisiert[98] und enthält im Wesentlichen die Koordinaten des Unfallorts, Fahrtrichtung, Fahrzeug-Identifizierungsnummer (FIN), Typ des Fahrzeugs, Antriebstechnologie und die Angabe, ob der Notruf automatisch oder manuell ausgelöst wurde. Die Verordnung sieht vor, dass sich die bordeigenen eCall-

[93] Ergänzende Leitlinien (siehe Fn. 94), S. 26 Rn. 66.
[94] Ergänzende Leitlinien (siehe Fn. 94), S. 26 Rn. 66.
[95] Ergänzende Leitlinien (siehe Fn. 94), S. 26 Rn. 65.
[96] Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG (ABl. L 123 vom 19.5.2015, S. 77), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R0758&from=EN.
[97] Delegierte Verordnung (EU) 2017/79 der Kommission vom 12. September 2016 zur Festlegung detaillierter technischer Anforderungen und Prüfverfahren für die EG-Typgenehmigung von Kraftfahrzeugen hinsichtlich ihrer auf dem 112-Notruf basierenden bordeigenen eCall-Systeme, von auf dem 112-Notruf basierenden bordeigenen selbstständigen technischen eCall-Einheiten und Bauteilen und zur Ergänzung und Änderung der Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates im Hinblick auf die Ausnahmen und die anzuwendenden Normen (ABl. L 12 vom 17.1.2017, S. 44), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R0079&from=DE.
[98] DIN EN 15722:2011: Intelligente Transportsysteme - Elektronische Sicherheit - Minimaler Datensatz (MSD) für den elektronischen Notruf eCall.

Systeme auf eine interoperable, standardisierte, sichere und frei zugängliche Plattform[99] stützen, womit Vorgaben an die Systemarchitektur von Telematikdiensten bei Personenfahrzeugen gestellt werden.[100]

eCall ist ein schlafendes Notrufsystem, was bedeutet, dass Positionsdaten nur im Notfall übermittelt werden dürfen. Erst wenn das Auto einen verletzungsrelevanten Unfall registriert, wählt die SIM-Karte des Systems über das vor Ort stärkste Mobilfunknetz die 112. Ungenutzte Informationen werden kontinuierlich gelöscht. Somit kann eCall keine Bewegungsprofile erstellen. Bei vernetzten Fahrzeugen, deren SIM-Karte dauerhaft aktiv und mit dem Internet verbunden ist, ist dies aber nicht der Fall. Bei diesen Fahrzeugen lassen sich zum Beispiel im Falle eines Diebstahls jederzeit Informationen zur aktuellen Position ermitteln. Die eCall-Verordnung zieht in dieser Hinsicht eine klare Grenze, indem sie den Datenaustausch zwischen dem gesetzlich vorgeschriebenen eCall-System und herstellerspezifischen Connected-Services verbietet.[101]

4. IVS-Richtlinie 2010/40/EU und IVSG

Die IVS-Richtlinie[102] dient seit 2010 dazu, eine koordinierte Einführung intelligenter Verkehrssysteme auf der Grundlage europäischer Spezifikationen und Normen in der gesamten EU sicherzustellen. Intelligente Verkehrssysteme (IVS) sind Anwendungen von Informations- und Kommunikationstechnologien im Verkehr, z. B. für Reiseplaner, eCall-Systeme und automatisiertes Fahren, und können dazu beitragen, die Mobilität sicherer, effizienter und nachhaltiger zu machen. Über IVS können Autofahrerinnen und Autofahrer z. B. bessere Informationen über Verkehrsvorschriften und Baustellen erhalten. Durch IVS wird das Fahren somit insgesamt sichererer, effizienterer und bequemer.[103]

Die IVS-Richtlinie legt fest, dass die Mitgliedstaaten der Europäischen Union, sofern sie nach Art. 3 aufgeführte vorrangige Maßnahmen einführen, die von der Kommission erlassenen Spezifikationen anzuwenden haben. Vorrangige Bereiche im Sinne der Richtlinie sind die optimale Nutzung von Straßen-, Verkehrs- und Reisedaten, die Kontinuität der Dienste intelligenter Verkehrssysteme in den Bereichen Verkehrs- und Frachtmanagement, die Anwendungen intelligenter Verkehrssysteme für die Straßenverkehrssicherheit sowie die Verbindung zwischen Fahrzeug und Verkehrsinfrastruktur. Straßenverkehrsteilnehmern sind im Rahmen intelligenter Verkehrssysteme Straßen-, Verkehrs- und Reisedaten zur Verfügung zu stellen. Gerade die Einführung intelligenter Verkehrssysteme wird von der Kommission als wichtige Maßnahme für den Aufbau eines vernetzten und automatisierten multimodalen Mobilitätssystems genannt.[104]

---

[99] Eine Plattform ist eine Infrastruktur, die es zwei oder mehr Gruppen ermöglicht zu interagieren. Dabei positioniert sich die Plattform als Vermittlerin zwischen den unterschiedlichen Gruppen. Zudem ist sie der Ort, an dem alle Aktivitäten stattfinden, wodurch sie exklusiven Zugang zu allen Daten und Aktivitäten der Interaktionspartner erhält, vgl. *Niederländer/Katzlinger*, in: Höller/Illetits-Motta/Küll/Niederländer/Stabauer: Digital Business für Verkehr und Mobilität. Ist die Zukunft autonom und digital?, 2020, Teil 7, S. 6, abrufbar unter https://www.idb.edu/wp-content/uploads/2021/01/CONNECTED-CARS-–-PROFITEURE-RISIKEN-UND-GESCHAeFTSFELDER.pdf.

[100] Vgl. Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG, Rn. 16 (ABl. L 123 vom 19.5.2015, S. 79), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R0758&from=EN.

[101] Erwägungsgrund 15 zur Verordnung (EU) 2015/758 (siehe Fn. 105).

[102] Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern, abrufbar unter https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:DE:PDF.

[103] Pressemitteilung der EU-Kommission vom 14.12.2021, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_6727.

[104] Vgl. Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlamentes und des Rates zur Änderung der Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern vom 14. Dezember 2021, 2021/0419 (COD), S. 1, abrufbar unter https://eur-lex.europa.eu/resource.html?uri=cellar:26277bcb-5db8-11ec-9c6c-01aa75ed71a1.0007.02/DOC_1&format=PDF.

Die auf der IVS-Richtlinie aufbauende Delegierte Verordnung (EU) 2017/1926[105] legt Mindestanforderungen fest, die der Zugänglichkeit, dem Austausch und der Aktualisierung von standardisierten Reise- und Verkehrsdaten dienen. Seit dem 1. Dezember 2019 sind Verkehrsbehörden, Verkehrsbetreiber, Infrastrukturbetreiber und Anbieter nachfrageorientierter Verkehrsangebote verpflichtet, Reise- und Verkehrsdaten über einen Nationalen Zugangspunkt (National Access Point – NAP) zugänglich zu machen. Dieser Nationale Zugangspunkt ist selbst kein Auskunftssystem für Reisende und Verkehrsteilnehmende, sondern schafft vielmehr die Grundlage, dass solche Informationsdienste künftig geschaffen werden können.

Ziel der Delegierten Verordnung (EU) 2017/1926 ist die grenzüberschreitende EU-weite Versorgung Reisender mit multimodalen, hochwertigen und durchgängigen Reiseinformationen vor und während der kompletten Reise. Die Verfügbarmachung dynamischer Daten auf Grundlage der Delegierten Verordnung (EU) 2017/1926 ist nicht verpflichtend, kann jedoch vom jeweiligen Mitgliedstaat eingefordert werden. Nur solche Daten sind verfügbar zu machen, die bereits in maschinenlesbaren Formaten vorliegen, d.h. aus der Verordnung ergibt sich keine Verpflichtung zur Erhebung neuer Daten. Die Weiterverwendung der Daten darf nicht unnötig eingeschränkt werden. Wird eine finanzielle Vergütung in Erwägung gezogen, hat diese angemessen und verhältnismäßig zu sein.

Das „Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern“ (IVSG)[106] ist am 21. Juni 2013 in Kraft getreten. Mit dem IVSG wurde die IVS-Richtlinie in deutsches Recht umgesetzt. Am 25. Juli 2017 ist das Erste Gesetz zur Änderung des IVSG in Kraft getreten.[107] Danach wurde eine „Nationale Stelle“ geschaffen, um die von Datenlieferanten zur Verfügung gestellten Straßen-, Verkehrs- und Reisedaten auf Konformität zu den Anforderungen der Delegierten Verordnungen zu überprüfen. Die Zuständigkeit und Aufgabenwahrnehmung der „Nationalen Stelle“ wurde der Bundesanstalt für Straßenwesen (BASt) übertragen.

Seit Juli 2022 bietet das Bundesministerium für Digitales und Verkehr (BMDV) einen neuen zentralen, einheitlichen und benutzerfreundlichen Zugang zu Mobilitätsdaten an, der den Nationalen Zugangspunkt für Mobilitätsdaten im oberen Sinne darstellt.

Die Mobilithek[108] löst das OpenData-Portal mCLOUD und den Mobilitäts Daten Marktplatz (MDM) als Nationalen Zugangspunkt für Mobilitätsdaten ab. Alle Informationen, die beispielsweise für Planung und Reisen durch Deutschland notwendig sind, können zukünftig dort zentral abgerufen und in Informationsangebote integriert werden. So soll die Grundlage geschaffen werden, dass Mobilitätsdienste geschaffen werden können. Daten, die über die Mobilithek bereitgestellt werden, sind vor allem solche von besonderer verkehrspolitischer Bedeutung im Sinne der IVS-Richtlinie. Daneben bietet die Mobilithek die Möglichkeit für einen darüberhinausgehenden Datenaustausch mit individuellen Nutzungsrechten und eröffnet so insbesondere Start-Ups und Unternehmen einen einfachen Weg, um neue Geschäftsmodelle zu entwickeln und zu erproben.

5. Kartellrecht (AEUV und GWB)

Sowohl das europäische als auch das deutsche Kartellrecht bieten Ansatzpunkte, um einen kartellrechtlichen Datenzugangsanspruch für die Marktakteure im Mobilitätsbereich näher zu untersuchen. Dabei stellt ein Zugang zu Informationen über das Kartellrecht keine grundsätzliche

[105] Verordnung (EU) 2017/1926 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter multimodaler Reiseinformationsdienste vom 31.5.2017 (Abl. L 272 vom 21.10.2017, S. 1), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R1926&from=FR.
[106] BGBl. 2013 Teil I Nr. 29, S. 1553.
[107] BGBl. 2017 Teil I Nr. 49, S. 2640.
[108] https://mobilithek.info.

Neuerung dar.[109] Im Hinblick auf das vernetzte Auto stellt sich die Frage, ob unabhängige Anbieter von Diensten auf Anschlussmärkten Zugang zu bestimmten Arten von fahrzeuginternen oder -generierten Daten mit der Begründung beanspruchen können, dass die Weigerung der Fahrzeughersteller, Zugang zu den Daten zu gewähren oder diese zu teilen, ein missbräuchliches Verhalten eines Unternehmens mit Marktmacht darstellt.

a) Art. 102 AEUV

Ein solcher Anspruch könnte auf das Verbot des missbräuchlichen Verhaltens marktbeherrschender Unternehmen nach Art. 102 AEUV gestützt werden. Zudem kommt grundsätzlich auch die Anwendung der sogenannten Essential-Facilities-Doktrin in Betracht, die jedoch bisher sehr hohen Anforderungen unterliegt.

Für die Ansprüche grundlegend ist aber zunächst das Vorhandensein einer marktbeherrschenden Stellung eines Unternehmens auf einem bestimmten Markt. Eine solche Bewertung wird aber eine Frage des Einzelfalles bleiben. Für die dogmatische Begründung ist eine wichtige Differenzierung vorzunehmen zwischen der Marktmacht auf dem Datenmarkt einerseits und der Marktmacht auf dem vorgelagerten Markt andererseits. Schließlich ist noch eine Abgrenzung nötig von der Position auf dem abgeleiteten (nachgelagerten) Markt.

Bezogen auf Datenmärkte[110] ist bisher nicht letztgültig geklärt, wann eine marktbeherrschende Stellung anzunehmen ist.[111] Zudem ist die Zahl denkbarer Datenzugangskonstellationen in diesem Bereich vielfältig. Sollte im jeweiligen Fall ein Hersteller auf einem definierten Markt eine beherrschende Stellung innehaben, so könnte eine Verweigerung des Datenzugangs für andere Marktakteure ein missbräuchliches Verhalten darstellen.[112]

Im Kartellrecht besteht nach der aus Art. 102 AEUV abgeleiteten sog. Essential-Facilities-Doktrin unter bestimmten Voraussetzungen ein Anspruch auf Teilhabe an einer für den Marktzugang notwendigen Ressource („essential facility“).[113] Es müssen jedoch mehrere Bedingungen mit hohen Anforderungen erfüllt sein und ein Zugang kommt nach er Rechtsprechung des EuGH nur unter „außergewöhnlichen Umständen“ in Betracht.[114] Die Annahme solcher „außergewöhnlichen Umstände“ setzt danach (kumulativ) voraus, dass (1) der Zugang der Wettbewerber zu der Einrichtung unerlässlich für den Zugang zu einem benachbarten Markt ist, (2) dass die Zugangsverweigerung jeden wirksamen Wettbewerb auf diesem Markt ausschließt, (3) dass keine objektive Rechtfertigung für die Zugangsverweigerung besteht sowie – im Falle des Zugangs zu Immaterialgüterrechten oder Geschäftsgeheimnissen – (4) zusätzlich, dass die Zugangsverweigerung das Erscheinen eines neuen Produkts verhindert.[115] Insbesondere in der Diskussion um die Verwendung der Essential-Facilities-Doktrin des Art. 102 AEUV als Instrument zur Gewährung des Datenzugangs wird in der Literatur sehr zurückhaltend bewertet, ob dies ein praktikables und empfehlenswertes Instrument sein kann.[116] Noch weitgehend ungeklärt ist unter welchen Voraussetzungen das Innehaben von größeren Datensätzen zur Marktbeherrschung führt und unter welchen Voraussetzungen der Zugang zu solchen Datensätzen

[109] Vgl. EuGH, Urt. 6.4.1995, Verb. Rs. C-241/91 P und C-242/91 P, Slg. 1995, I-743 – RTE und ITP gegen Kommission (“Magill”); EuG, Urt. v. 17.9.2007, T-201/04, Slg. 2007, II-3601 – Microsoft gegen Kommission.
[110] In diesem Zusammenhang wird häufig auch von Primärmärkten für Daten oder von Märkten der Zurverfügungstellung (der Daten) gesprochen, vgl. *Peitz/Schweitzer,*NJW 2018, 275; *Wolf/Westermann,* in: MüKoWettbR Bd. 2, 4. Aufl. 2022, § 19 GWB Rn. 146.
[111] Zu Daten als Marktgegenstände sowie zum Zusammenhang von Datenmacht und Marktmacht *Körber,* NZKart 2016, 303, 304 f.
[112] So wohl im Ergebnis wohl *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 406.
[113] Zu den Grundlagen der Essential-Facilities-Doktrin *Louven*, NZKart 2018, 271, 218.
[114] EuGH, Urt. v. 6.4.1995, verb. Rs. C-241/91 und C-242/91, Slg. 1995, I-743 – Magill (RTE und ITP).
[115] EuGH, Urt. v. 29.4.2004, C-418/01, Slg. 2004, I-5039, Rn. 38 – IMS Health GmbH. Zur Zugangsverweigerung bei Bestehen eines gewerblichen Schutzrechtes EuGH, 26.11.1998, Rs. C-7/97, Slg. 1998, I-7791, Rn. 38 ff. – Bronner.
[116] Vgl. *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 396 mit weiteren Nachweisen.

als unentbehrlich angesehen werden kann.[117] Bislang gibt es zudem kaum Rechtsprechung oder behördliche Fallpraxis zur missbräuchlichen Verweigerung des Zugangs zu Daten.

b) §§ 19 Abs. 2 Nr. 4, 20 Abs. 1a GWB

Mit Blick auf nationale Regelungen im Kartellrecht sind insbesondere die Regelungen § 19 Abs. 2 Nr. 4 und § 20 Abs. 1a GWB zu untersuchen.[118] Gerade beim vernetzten Fahrzeug mit der Kontrolle des Datenzuganges durch den Fahrzeughersteller könnte es sich bei einer Verweigerung des Zuganges zu Daten um eine missbräuchliche Verhaltensweise eines Unternehmens mit Marktbeherrschung oder relativer Marktmacht handeln.

Im Zuge des GWB-Digitalisierungsgesetzes[119] wurde der Missbrauchstatbestand gemäß § 19 Abs. 2 Nr. 4 GWB ergänzt. Diese Regelung stellt die deutsche Essential-Facility-Regelung dar. Nach der Gesetzesbegründung sollen durch die Norm auch strukturelle Datenzugangsprobleme auf Anschlussmärkten erfasst werden.[120] Die Vorschrift geht von dem Missbrauch einer marktbeherrschenden Stellung eines Unternehmens nunmehr insbesondere auch dann aus, wenn sich das marktbeherrschende Unternehmen weigert, einem dritten Unternehmen Zugang zu vorhandenen Daten zu gewähren, die Gewährung des Datenzugangs für eine Tätigkeit auf einem vor- oder nachgelagerten Markt objektiv notwendig ist und die Weigerung des Zugangs den wirksamen Wettbewerb auf diesem Markt auszuschalten droht.[121] Die Datenüberlassung bewirkt sodann – zur Erfüllung des Anspruchs aus § 33 Abs. 1 GWB – die Auflösung der Missbrauchshandlung.

Ob und inwieweit ein Unternehmen mit marktbeherrschender Stellung i.S.v. § 18 Abs. 1 GWB zu qualifizieren ist, kann nicht einheitlich beantwortet werden, da dies eine marktbezogenen Wertung erfordert. Potentiell kann aber die Inhaberschaft über Daten im Sinne eines faktischen Monopols eine marktbeherrschende Stellung im Sinne des § 18 Abs. 1 GWB darstellen, aus der bei einer missbräuchlichen Geschäftsverweigerung ebenso eine kartellrechtliche Zwangslizenz folgen kann.[122] Dabei ist aber zu beachten, dass Datenmacht als solche nicht grundsätzlich mit Marktmacht gleichzusetzen ist. Der weit gefasste Wortlaut von § 19 Abs. 2 Nr. 4 GWB („Zugang zu Daten, zu Netzen oder anderen Infrastruktureinrichtungen“) soll ermöglichen, dass die Weigerung eines marktbeherrschenden Unternehmens, einem anderen Unternehmen Zugang zu Daten, Plattformen oder Schnittstellen zu gewähren, als missbräuchliches Verhalten gewertet werden kann. Zu beachten ist, dass, ebenso wie bei Art. 102 AEUV, auch bei § 19 Abs. 2 Nr. 4 GWB hohe Anforderungen an eine Zugangsgewährung gestellt werden. Die bei Art. 102 AEUV bereits erläuterten Voraussetzungen 1–3 finden sich auch in § 19 Abs. 2 Nr. 4 GWB wieder.

Im Zuge der genannten Novelle wurde § 20 Abs. 1a GWB in das Gesetz eingefügt, womit die Fallgruppe der datenbedingten Abhängigkeit gesetzlich normiert ist. Nach Ansicht des Gesetzgebers wird der Datenzugang zumindest mitentscheidend für die Wettbewerbsfähigkeit einer Volkswirtschaft sein, weshalb die zuständige Wettbewerbsbehörde im Fall einer relativen Marktmacht den Datenzugang zu wettbewerbsrelevanten Daten anordnen kann.[123] Damit wird klargestellt, dass eine Abhängigkeit von einem bei einem Unternehmen vorliegenden Datenbestand unterhalb der Marktbeherrschung bestehen

---

[117] *Drexl*, NZKart 2017, 415, 418.

[118] Es kommen zudem grundsätzlich weitere kartellrechtliche Ansprüche in Betracht, wie z.B. das kartellrechtliche Diskriminierungsverbot gem. § 19 Abs. 2 Nr. 1 GWB oder der Konditionen- und Preismissbrauch gem. § 19 Abs. 2 Nr. 2 GWB, die jedoch im hier relevanten Untersuchungskontext keine Besonderheiten aufweisen und daher folgend nicht explizit untersucht werden.

[119] Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen vom 18.1.2021, BGBl. 2021 Teil I Nr. 1, S. 2.

[120] BT-Drucksache 19/23492 vom 19.10.2020, S. 72, abrufbar unter https://dserver.bundestag.de/btd/19/234/1923492.pdf.

[121] Zur Markmacht durch Daten vgl. *Fast/Schnurr/Wohlfarth*, in: Specht-Riemenschneider/Werry/Werry, Datenrecht in der Digitalisierung, 2020, S. 745 ff.; *Louven*, in: Specht-Riemenschneider/Werry/Werry, Datenrecht in der Digitalisierung, 2020, S. 779 ff.

[122] *Louven*, NZKart 2018, 271, 219.

[123] BT-Drs. 19/23492, S. 80, abrufbar unter https://dserver.bundestag.de/btd/19/234/1923492.pdf.

kann.[124] Die Verweigerung des Zugangs zu diesen Daten kann eine unbillige Behinderung im Sinne von § 20 Abs. 1 GWB in Verbindung mit § 19 Abs. 2 Nr. 1 GWB darstellen. Mit dem Bezug ist insbesondere ein Rückgriff auf die bisherige Rechtsprechung zu § 20 Abs. 1 GWB möglich. Nach § 20 Abs. 1 GWB wird missbräuchliches Verhalten auch Unternehmen untersagt, die zwar nicht marktbeherrschend sind, aber über sogenannte relative oder überlegene Marktmacht verfügen. Mit § 20 Abs. 1 GWB existiert daher eine Regelung zur Erfassung von Ungleichgewichten unterhalb der Schwelle der Marktbeherrschung. Zu dieser Norm hat sich in der Vergangenheit eine Anwendungspraxis etabliert, die kritische Datenzugangskonstellationen unterhalb der Schwelle der Marktbeherrschung erfassen kann.

II. Konzepte und Projekte in der Automobilwirtschaft

Im Rahmen einer Marktrecherche unter Einbeziehung einer inhaltlichen Analyse wurde ermittelt, welche privatwirtschaftlichen Konzepte und Projekte zum (zukünftigen) Austausch von Daten in der Automobilwirtschaft zwischen den Marktakteuren in Deutschland derzeit diskutiert werden. Ergänzend konnten die ausgewählten Experten der Interviews hierzu befragt werden.

Grundsätzlich lässt sich festhalten, dass sich die Konzepte zwei unterschiedlichen technischen Systemen zuordnen lassen: Zum einen basieren viele Konzepte auf einem geschlossenen technischen System der Datenerzeugung, und der nachgelagerte Zugang zu den erzeugten Daten für die Marktakteure wird in verschiedenen Ausgestaltungen skizziert. Zum anderen basieren einige Konzepte auf einem offenen technischen System, bei dem nicht ein nachgelagerter Zugang zu den erzeugten Daten im Mittelpunkt des jeweiligen Konzeptes steht, sondern der direkte Zugang zum datengenerierenden Fahrzeug und unmittelbare Datenübertragung.

Nicht weiter untersucht werden folgend Konzepte, die auf einer externen Erhebung von Fahrzeugdaten durch Anbringung von gesonderten Erfassungsgeräten basieren, weil dabei nicht der Zugang zu Daten des vernetzten Fahrzeuges im Mittelpunkt steht.[125]

1. Fahrzeugherstellereigene Plattformen zum Datenaustausch

Grundlage für die Monetarisierung von Mobilitätsdienstleistungen, die auf Basis von vernetzen Fahrzeugen angeboten werden, sind die digitalen Plattformen der Fahrzeughersteller, auf denen die im Fahrzeug generierten Daten angeboten werden. Dritte können mit einem Fahrzeughersteller einen Vertrag schließen und bestimmte Datenarten zu bestimmten Preisen für bestimmte Verwendungszwecke erwerben. Nach dem zivilrechtlichen Grundsatz der Vertragsfreiheit können zwischen zwei Unternehmen Erhebung, Erwerb, Austausch oder Zugang zu Daten vertraglich geregelt werden, soweit dadurch keine Rechte betroffen sind, die nicht den Vertragsparteien selbst zustehen. Zugleich gibt es bislang keine gesetzlichen Regeln für Verträge, in denen sich Parteien auf einen Zugang zu Daten einigen.

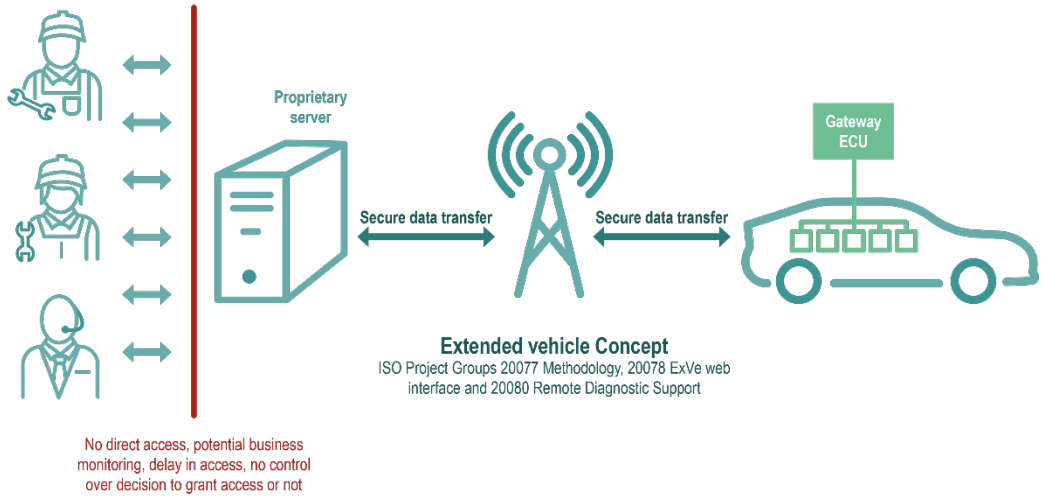
Grundlage der soeben beschriebenen Plattformen und die Möglichkeit der Monetarisierung von Fahrzeugdaten durch die Fahrzeughersteller ist das Extended Vehicle-Konzept. „Extended Vehicle“ ist der Oberbegriff für die Bereitstellung sowie elektronische Weitergabe und Nutzung von fahrzeuggenerierten Daten über eine Webschnittstelle, wobei eine internationale Normung in diesem

[124] Zum Grundgedanken der relativen Marktmacht in § 20 Abs. 1 GWB *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 409.

[125] Zu nennen ist in diesem Zusammenhang das (bereits abgeschlossene) Projekt „OpenTrafficCount“, bei welchem aus bestehenden Open Source Komponenten Prototypen von mobilen Bilderkennungssystemen entwickelt wurden, welche am Fahrzeug angebracht wurden und die erhobenen Daten in eine Cloud-basierte Datenbank zum Abruf unter freier Lizenz einspeisten, vgl. https://www.technologiestiftung-berlin.de/projekte/open-traffic-count.

Bereich vorliegt.[126] Das (technische) Prinzip des Extended Vehicle sieht vor, dass Over-the-Air Zugriffe auf ein Fahrzeug niemals direkt, sondern ausschließlich über einen abgesicherten Backend-Server, der vom Fahrzeughersteller bereitgestellt und verwaltet wird, erfolgen. Auf diese Weise verbleiben die Hoheit über Daten, der Zugriff auf das Fahrzeug und die Zugangskontrolle in den Händen des Fahrzeugherstellers. Obwohl die Umsetzung nicht verpflichtend ist, integrieren viele Fahrzeughersteller seit Baujahr 2015 Telematiksysteme in ihre Fahrzeuge, die ohne Installation zusätzlicher Hardware auskommen und Sensor- und Standortdaten über eine gesicherte Webschnittstelle an die Server des jeweiligen Fahrzeugherstellers übermitteln können, was es dem Fahrzeughersteller ermöglicht, jederzeit Daten abzufragen oder auf das Fahrzeug zuzugreifen, um beispielsweise Updates durchzuführen. Dabei bildet die Verbindung zwischen Fahrzeug und Hersteller ein geschlossenes System im Sinne eines Mobilitätsökosystems. Jeder Hersteller verwendet in der Regel seine eigene Software, um die Verbindung herzustellen und zu sichern.

Einige Fahrzeughersteller öffnen den Zugriff auf die in ihrem Besitz befindlichen Daten bzw. auf Teile hiervon auf ihrer Datenplattform über Anwendungsprogrammierschnittstellen (APIs) für den Zugriff durch Drittanwendungen. Ein Eingriff in die Fahrzeugarchitektur durch die Schnittstelle ist ausgeschlossen. Es gibt daher in der Regel keinen Lesezugriff für Dritte in Echtzeit und auch keinen Schreibzugriff auf Fahrer. Dritte müssen die unterschiedlichen APIs der verschiedenen Fahrzeughersteller und auch der verschiedenen Fahrzeugtypen und -marken in ihre Systeme einbinden und pflegen.[127] Die Funktionsweise des Extended Vehicle-Konzeptes stellt die folgende Grafik (**Abb. 4**) anschaulich dar[128]:



[126] Die internationale Normung zu „Extended Vehicle“ umfasst derzeit mehrere Normenreihen. ISO 20077 beschreibt methodische Anforderungen für die Nutzung von Fahrzeugdaten über das Web-Interface sowie allgemeine Begriffe. Die Normenreihe ISO 20078 legt die eigentlichen Anforderungen an das Web-Interface hinsichtlich Zugriffs, Dateninhalten, Sicherheit und Zugriffssteuerung fest. ISO 20080 definiert eine erste Extended-Vehicle-Anwendung: den funkgestützten Diagnosezugriff von Werkstattdienstleistern. Es ist geplant, weitere Extended-Vehicle-Anwendungen zu normen und diese entweder in die bestehenden Normen aufzunehmen oder weitere Normteile zu erarbeiten. Hierzu wird derzeit im ISO/TC 22/SC 31/WG 6 „Extended Vehicle/Remote diagnostics“ eine Liste mit möglichen Themen erarbeitet. Die erste Version der ISO-Norm wurde 2019 veröffentlicht. Im Herbst 2021 wurde die zweite Ausgabe der Norm mit einigen wichtigen Erweiterungen verabschiedet.

[127] Verschiedene technische Lösungen vereinfachen diesen Prozess, indem sie verschiedene APIs von Fahrzeugherstellern anbinden und deren Daten harmonisieren und normalisieren, so dass die Entwickler mit den Daten arbeiten können, ohne sich um unterschiedliche Formate kümmern zu müssen, vgl. https://invers.com/de/press-releases/invers-oem-integrations-verbindet-fahrzeuge-ohne-zusaetzliche-hardware/ sowie https://de.high-mobility.com/auto-api.

[128] In Anlehnung an die Übersicht im Positionspapier „Policy position on car connectivity” der Fédération Internationale de l’Automobile (FIA) aus 04/2016, S. 4, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf.

Abb. 4 – Übersicht zur Funktionsweise des Extended Vehicle-Konzeptes

Weitere Zugriffe, wie beispielsweise schreibende Zugriffe von Dritten auf Fahrzeugsysteme gemäß Anforderungen an die Cybersicherheit, sollen zukünftig vermehrt möglich sein.[129] Im Rahmen der Weiterentwicklung werden verschiedene Fahrzeughersteller unter Beachtung von regulatorischen Anforderungen (z. B. UNECE R155 Cybersecurity[130]), Zertifizierungsaspekten sowie den Anforderungen an Softwareupdate-Managementsysteme (UNECE R156[131]) die Möglichkeit bieten, im Fahrzeug Software von Drittanbietern zu installieren.[132] Richtlinien oder konkrete Projekte gibt es diesbezüglich aber noch nicht. Grundlegend soll dabei bleiben, dass die Freigabe der Software und das Management von Fahrzeugressourcen (z. B. Bandbreiten für Datenübertragungen im Fahrzeug) nur durch das für die Zertifizierung des Fahrzeugs verantwortliche Unternehmen erfolgen können.

Der logische Ablauf eines Extended-Vehicle-Prozesses ist an die beteiligten Rollen angelehnt:

- **Resource Owner:** besitzt eine Ressource und ist berechtigt, Zugriffe auf die Ressource zu erteilen oder zu verweigern. Bei Ressourcen mit Personenbezug fungieren oft Fahrzeughalter oder Fahrer als Ressource Owner.
- **Accessing Party:** greift auf Ressource via Web-Schnittstelle zu. Accessing Party könnte zum Beispiel ein Versicherungsunternehmen sein, welches die Fahrzeugdaten abruft.
- **Offering Party:** Fahrzeughersteller, der den Zugriff auf die Ressourcen technisch bereitstellt.
- **Connected Vehicle:** Straßenfahrzeug, welches über eine Web-Schnittstelle mit der Außenwelt kommunizieren kann

Die folgende Übersicht (**Abb. 5**) veranschaulicht den logischen Ablauf eines Extended-Vehicle-Prozesses[133]:

[129] VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten aus 01/2022, S. 11, abrufbar unter https://www.vda.de/dam/jcr:2026d593-4515-4c7c-8eef-7bae3597ad78/VDA_5690_Positionspapier_ADAXO_RZ.pdf?mode=view.

[130] UN-Regelung Nr. 155 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387] vom 22.1.2021, abrufbar unter https://op.europa.eu/de/publication-detail/-/publication/a5081378-8079-11eb-9ac9-01aa75ed71a1. Dazu ausführlich *Arzt/Kleemann/Plappert/Rieke/Zelle*, MMR 2022, 593, 601 ff.

[131] UN-Regelung Nr. 156 — Einheitliche Bestimmungen für die Genehmigung von Kraftfahrzeugen hinsichtlich der Softwareaktualisierung und des Softwareaktualisierungsmanagementsystems [2021/388] vom 22.1.2021, abrufbar unter https://op.europa.eu/de/publication-detail/-/publication/ec74fcfc-8079-11eb-9ac9-01aa75ed71a1. Dazu ausführlich *Arzt/Kleemann/Plappert/Rieke/Zelle*, MMR 2022, 593, 603 f.

[132] VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten aus 01/2022, S. 5, abrufbar unter https://www.vda.de/dam/jcr:2026d593-4515-4c7c-8eef-7bae3597ad78/VDA_5690_Positionspapier_ADAXO_RZ.pdf?mode=view.

[133] https://www.q-perior.com/fokusthema/iso-norm-extended-vehicle-framework-zur-bereitstellung-der-fahrzeugdaten-ueber-web-schnittstelle/#iLightbox[3f2c3e0bd0ec736c834]/0.

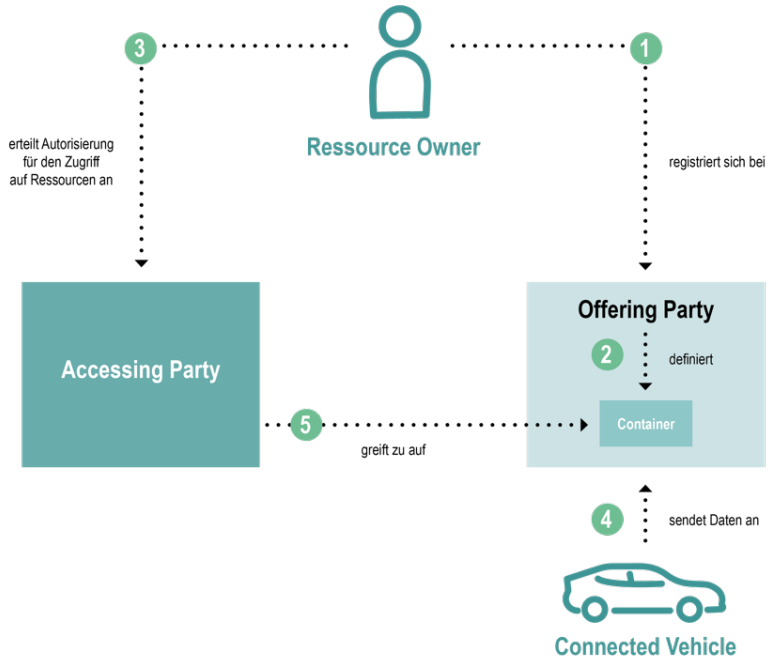


Abb. 5 – Übersicht zum Ablauf eines Extended-Vehicle-Prozesses

Als Praxisbeispiel kann BMW ConnectedDrive genannt werden. BMW ConnectedDrive ist eine von BMW aufgebaute IT-Plattform mit entsprechenden Vertragsbedingungen.[134] Bei BMW ConnectedDrive werden über eine fest verbaute SIM-Karte Online-Dienste im Auto angeboten, teilweise in Verbindung mit einer Smartphone-App. Dazu werden unter anderem folgende Daten übermittelt: GPS-Standort, Geschwindigkeit, Laufleistung, Sensorinformationen (Radar, Kamera, Mikrofon, Regen). Die durch BMW ConnectedDrive gesammelten Daten bietet BMW auf einer B2B-Datenplattform zur Nutzung durch Dritte an, BMW CarData. BMW CarData ist Marktplatz für Teile der durch BMW ConnectedDrive erhobenen Daten.

Der Autokonzern Mercedes-Benz Group geht im Zusammenhang mit dem Extended-Vehicle-Konzept einen anderen Weg und arbeitet mit einem Drittanbieter einer externen Plattform zusammen. Der Stuttgarter Automobilkonzern stellt über den Marktplatz Caruso[135] fünf Datenpakete bereit: Pay-as-you-drive (aktueller Kilometerstand eines vernetzten Pkw), Fuel Status (Tankfüllstand, verbleibende Fahrzeugreichweite auf Basis des tatsächlichen Kraftstoffstands), Vehicle Status (Status von Fahrzeugteilen wie beispielsweise Türen, Fenster oder Schiebedach) sowie Vehicle Lock Status (verriegelt oder nicht verriegelt, Ausrichtung mittels einer Kompassfunktion) und Electric Vehicle (ausschließlich für Elektrofahrzeuge: Batterieladezustand und verbleibende Reichweite). Teilehändler, Werkstätten, Versicherungen sowie Flottenmanager können auf diese Daten zugreifen und darauf basierend eigene Mobilitätslösungen entwickeln. Technisch gesehen gelangen die Daten über Programmierschnittstellen (APIs) im Mercedes-Benz Developer Portal an Caruso.

2. NEVADA und ADAXO

Auch das ADAXO-Konzept („automotive data access, extended and open“) des Bundesverbands der Automobilwirtschaft vom Januar 2022[136] wird in diesem Kontext häufig diskutiert. Vorgänger des

[134] BMW, Aftersales Online System, Nutzungsbedingungen, abrufbar unter: https://aos.bmwgroup.com/de/terms-of-use.
[135] https://www.caruso-dataplace.com.
[136] VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten aus 01/2022, abrufbar unter https://www.vda.de/dam/jcr:2026d593-4515-4c7c-8eef-7bae3597ad78/VDA_5690_Positionspapier_ADAXO_RZ.pdf?mode=view.

ADAXO-Konzepts war das Projekt NEVADA („Neutral Extended Vehicle for Advanced Data Access"), welches im Oktober 2017 veröffentlicht wurde.[137] Der zentrale Ansatz bei NEVADA als Architekturkonzept war es, Daten aus dem Fahrzeug (Extended Vehicle) über (neutrale) Server verschiedenen Parteien zur Verfügung zu stellen. Zur konkreten technischen Umsetzung bzw. verschiedener Implementierungen wurden konkrete Vorschläge unterbreitet. Dieses Konzept sah vor, dass der Hersteller den ausschließlichen Zugriff auf das Fahrzeug behält und eine zentrale Kommunikationsschnittstelle in Hintergrundsystemen des jeweiligen Herstellers als wesentliche Schnittstelle zum (neutralen) Server dient. Dem Hersteller sollte damit stets eine zentrale Rolle in der Datenwirtschaft zukommen, er sollte aber auch für die Sicherheit des Fahrzeuges verantwortlich sein. Berechtigte Dritte (z. B. Versicherungen oder freie Werkstätten) sollten die Daten nach Kundenzustimmung diskriminierungsfrei aus dem Backend übermittelt bekommen. Zur Zuordnung von Nutzungsbefugnissen an Daten aus dem vernetzten Fahrzeug unterschied NEVADA mehrere Kategorien von Daten.[138] Damit ein Marktteilnehmer Daten bei dem (neutralen) Server abrufen konnte, benötigte dieser je nach Datenkategorie einen entsprechenden Vertrag. Verschiedene Fahrzeughersteller haben das NEVADA-Konzept umgesetzt (z.B. im Rahmen prototypischer Aufbauten im Feldeinsatz) – mit Selbstbestimmungsanteilen der Nutzer. So war dies in Fahrzeugen der Marke BMW (als „BMW CarData") oder der Marke Audi (als „Audi Connect") zu finden, ebenso hatte Mercedes (als „Mercedes ME") dies implementiert.

Aufgrund neuartiger Initiativen auf europäischer Ebene, wie etwa den Diskussionen um Datenräume, wurde das bisherige Konzept weiterentwickelt. Im ADAXO-Konzept wird, anders als im NEVADA-Konzept, nicht mehr eine Datenplattform konzipiert, sondern es geht vielmehr um technische Möglichkeiten und Grundprinzipien, mit der Dritte auf die Fahrzeugdaten zugreifen können. Die im Fahrzeug generierten Daten sollen über eine einzige internetfähige Schnittstelle bereitgestellt werden, da sich aus Sicht des VDA bei dem Vorhandensein von mehreren Schnittstellen in einem Fahrzeug die Sicherheitsrisiken und Zugriffsschwierigkeiten erhöhten.

Mit einer im Konzept näher beschriebenen Schnittstelle sollen relevante Fahrzeugdaten für mehrere Marktteilnehmer zu fairen Konditionen zur Verfügung gestellt werden. Die so abrufbaren Daten gehen über die im NEVADA-Konzept angedachten Datenkategorien hinaus. Dabei beruht das ADAXO-Konzept auf dem Konzept des Extended Vehicle als integralem Bestandteil. Im Unterschied zu der Praxis auf den meisten fahrzeugherstellereigenen Datenplattformen sollen im Rahmen des ADAXO-Konzeptes von den teilnehmenden Fahrzeugherstellern alle Daten und Funktionen angeboten werden, die sie auch zur Erbringung ihrer eigenen Services nutzen. Der diskriminierungsfreie[139] Zugang zu den Daten erfolgt entweder maskiert (z. B. neutraler Server) oder direkt über den jeweiligen Fahrzeughersteller, jeweils auf der Basis von individuell ausgestalteten B2C- und B2B-Verträgen (siehe hierzu bereits oben).

---

[137] Die entsprechenden Unterlagen des VDA sind nicht mehr aufrufbar. Das NEVADA-Konzept wird jedoch ausführlich untersucht in der Studie „Datenarchitekturen fahrzeuggenerierter Daten - Eine Use-Case-basierte Bewertung" des Deutschen Zentrums für Luft- und Raumfahrt (DLR) vom 29.2.2020, S. 7 ff., abrufbar unter https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/studie-zu-datenarchitekturen-fahrzeuggenerierter-daten.pdf?__blob=publicationFile&v=6. Ebenso finden sich technische und organisatorische Erläuterungen bei *Greß/Springborn*, in: Stiftung Datenschutz, Datenschutz im vernetzen Fahrzeug, 2020, S. 55, 67 ff.

[138] Es wurden im NEVADA-Konzept fünf Datenkategorien unterschieden, die sich durch ihre Anwendungsziele sowie durch die Kategorie der personenbezogenen Daten unterscheiden, vgl. Studie „Datenarchitekturen fahrzeuggenerierter Daten - Eine Use-Case-basierte Bewertung" des Deutschen Zentrums für Luft- und Raumfahrt (DLR) vom 29.2.2020, S. 7 f., abrufbar unter https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/studie-zu-datenarchitekturen-fahrzeuggenerierter-daten.pdf?__blob=publicationFile&v=6; Stellungnahme „Rechtsfragen der digitalisierten Wirtschaft: Datenrechte" des Bitkom e.V. aus 09/2019, S. 36 f., abrufbar unter https://www.bitkom.org/sites/default/files/2019-09/bitkom-stellungnahme-zu-datenrechten_langfassung_final_0.pdf.

[139] Die VDA-Verbandsunternehmen bieten den FRAND-Zugriff für Daten und Funktionen den Unternehmen an, die sich ebenso dem FRAND-Prinzip gegenüber verpflichten.

Folgendes Schaubild des VDA (**Abb. 6**) zeigt die technischen und vertraglichen Bestandteile des ADAXO-Konzeptes[140]:

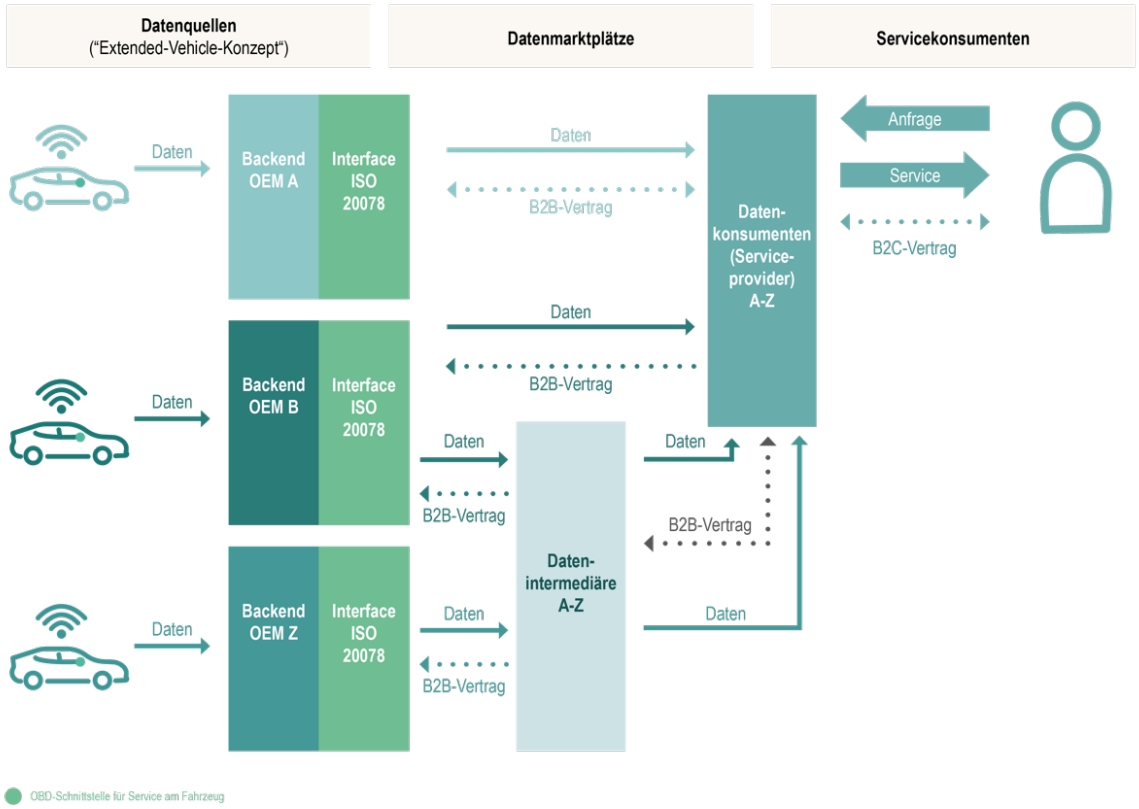


Abb. 6 – Übersicht zu den technischen und vertraglichen Bestandteilen des ADAXO-Konzeptes

3. Kollaborative Plattformen zum Datenaustausch

Im Bereich des Austauschs von Fahrzeugdaten ist zu beobachten, dass es eine Reihe an Initiativen gibt, die einen Datenaustausch zwischen verschiedenen Akteuren im Mobilitätsbereich fördern wollen und eine gemeinsame Nutzung von Daten zur Entwicklung neuer Geschäftsmodelle in Datenräumen forcieren. Datenräume vereinen Governance und Infrastruktur, um die Bündelung und Weitergabe von Daten auf kontrollierte und sichere Weise zu erleichtern.

Mit dem Mobility Data Space[141] (vormals Datenraum Mobilität) besteht eine solche Initiative, die insbesondere die Möglichkeit bietet, mit hoher Transparenz über das Datenangebot und über standardisierte Konnektoren schnell und effizient Daten aus verschiedensten Datenquellen zu beziehen. Der Mobility Data Space wird vom Bundesministerium für Digitales und Verkehr (BMDV) gefördert und ist Teil der europäischen Cloud-Initiative Gaia-X.[142] Viele Fahrzeughersteller unterstützen

[140] VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten aus 01/2022, S. 10, abrufbar unter https://www.vda.de/dam/jcr:2026d593-4515-4c7c-8eef-7bae3597ad78/VDA_5690_Positionspapier_ADAXO_RZ.pdf?mode=view.

[141] https://mobility-dataspace.eu/de.

[142] Mit Gaia-X entwickeln Vertreterinnen und Vertreter aus Wirtschaft, Wissenschaft und Politik auf internationaler Ebene eine europäischen Dateninfrastruktur. Ziel ist eine sichere und vernetzte Dateninfrastruktur, die den höchsten Ansprüchen an digitale Souveränität genügt und Innovationen fördert. In einem offenen und transparenten digitalen Ökosystem sollen Daten und Dienste verfügbar gemacht, zusammengeführt, vertrauensvoll geteilt und genutzt werden können. Die Architektur von Gaia-X basiert auf dem Prinzip der Dezentralisierung. Gaia-X ist das Zusammenspiel zahlreicher individueller Plattformen, die alle einem gemeinsamen Standard folgen - dem Gaia-X-Standard. Gemeinsam wird so eine Dateninfrastruktur entwickelt, die auf den Werten Offenheit,

bereits diesen Ansatz und fördern den weiteren Ausbau. Im Projekt werden verschiedene Plattformen für die Unterstützung datenbasierter Services im Mobilitätsbereich weiterentwickelt, indem sie um sichere und geschützte Ausführungsumgebungen für Services sowie Data-Apps erweitert und zu einem dezentralen Data Space verknüpft. Die Daten selbst bleiben dabei so lange bei den Anbietenden, bis es zum Vertrag mit einem Käufer gekommen ist.

Catena-X[143] - ein Datennetzwerk für die Zusammenarbeit in der Automobilindustrie - ist ein weiteres Projekt in diesem Kontext. Catena-X ist ebenfalls Teil der Gaia-X-Initiative und soll ein integriertes, kollaboratives, offenes Datenökosystem für alle Akteure der Wertschöpfungskette schaffen und zielt darauf ab, einheitliche Standards für den Datentransfer zu entwickeln. Der Anspruch dieses Projektes ist die Datensouveränität der Akteure: Wer Daten zur Verfügung stellt, behält die Kontrolle und entscheidet individuell, wer am Datenaustausch wie, wann, wo und unter welchen Bedingungen beteiligt wird. Auch an diesem Projekt beteiligen sich viele Fahrzeughersteller.

In der EU-Datenstrategie[144] wurde die Schaffung gemeinsamer europäischer Datenräume in Schlüsselsektoren, einschließlich der Mobilität, angekündigt. Das Programm „Digitales Europa“ (DIGITAL)[145] unterstützt die Umsetzung eines Mobilitätsdatenraums. Der gemeinsame europäische Mobilitätsdatenraum (EMDS) zielt darauf ab, im Hinblick auf eine größere Effizienz, Sicherheit, Nachhaltigkeit und Resilienz des Verkehrs den Datenzugang, die Bündelung sowie den Austausch von Daten zu erleichtern. Er beruht auf Initiativen und Anwendungen im Zusammenhang mit Verkehrsdaten und wird durch Initiativen zur Förderung der Interoperabilität, der Sicherheit sowie der Verfügbarkeit und Bereitstellung von Daten und Diensten unterstützt.[146] Eine vorbereitende Maßnahme soll bestehende Initiativen abbilden und mögliche gemeinsame Bausteine ermitteln, wobei eine Annahme durch die EU-Kommission für das zweite Quartal 2023 geplant ist. Eine Bereitstellungsaktion wird sodann dazu beitragen, große Datenmengen in maschinenlesbarem Format zur Verfügung zu stellen, wobei der Schwerpunkt auf urbaner Mobilität liegt.

4. Offene und interoperable Telematikplattform

Ein Gegenmodell zum Extended Vehicle-Konzept stellt die offene und interoperable Telematikplattform (Open Telematics Platform, OTP) dar. Grundidee ist die Annahme, dass Nutzer selbst die Kontrolle über die von ihnen im Fahrzeug generierten Daten ausüben und anderen Serviceanbietern den Zugang zum vernetzten Fahrzeug ermöglichen können. Damit soll auch der technische Bottleneck, der den Fahrzeugherstellern die exklusive Kontrolle über die Daten beziehungsweise den Zugang zum Fahrzeug verschafft, zugunsten einer neutralen Plattform beseitigt werden.[147]

Konzeptionell ist die Grundlage die sogenannte “On-Board Application Platform” (OBAP). Dies ist primär eine andere technologische Lösung als das Extended Vehicle-Konzept, bei der keine Übertragung der Daten auf einen externen Server erforderlich ist, sondern die Speicherung und Verarbeitung der Daten im Auto ermöglicht wird. Dies erfordert technisch offene und interoperable Telematiksysteme. Die On-Board Telematics Platform (OTP) skizziert eine konkrete Lösung des Modells der OBAP. Eine OTP ist eine im Fahrzeug integrierte und standardisierte Plattform, über die Dienstleister und Hersteller Applikationen im Fahrzeug ausführen und Daten abrufen können. Es sollen

---

Transparenz und Vertrauen basiert. Es entsteht also nicht nur eine Cloud, sondern vielmehr ein vernetztes System, das viele Cloud-Service-Anbieter miteinander verbindet, vgl. https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html.

[143] https://catena-x.net/de/

[144] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

[145] https://digital-strategy.ec.europa.eu/de/activities/digital-programme.

[146] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Verkehrsdaten-Schaffung-eines-gemeinsamen-europaischen-Mobilitatsdatenraums-Mitteilung-_de.

[147] Vgl. zum gesamten Konzept das Positionspapier „Policy position on car connectivity” der Fédération Internationale de l’Automobile (FIA) aus 04/2016, S. 7, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf.

nicht nur Fahrzeugdaten und Funktionen abrufbar sein, sondern auch die Kommunikation des Fahrers über das fahrzeugeigene Display mit der Werkstatt seiner Wahl kann so möglich sein. Neben den technischen Grundstrukturen[148] wurden auch IT-Sicherheitsaspekte berücksichtigt. [149]

Die Funktionsweise stellt die folgende Übersicht (**Abb. 7**) anschaulich dar[150]:

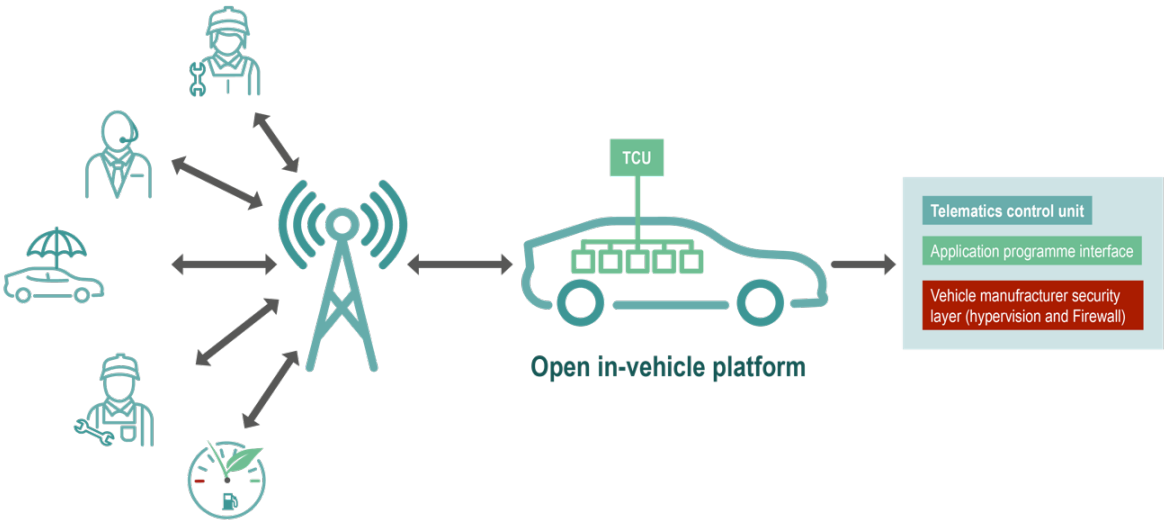


Abb. 7 – Übersicht zur Funktionsweise der On-Board Telematics Platform (OTP)

Bei dieser Lösung sind für das gesamte automobile Mobilitätssystem herstellerübergreifende Standardisierungen der Schnittstellen zum Austausch von Daten (API) und der Interoperabilität[151] mit komplementären Dienstleistungen erforderlich, ebenso wie einheitliche Sicherheitsstandards und Zertifizierungssysteme, um die notwendige Sicherheit von Fahrzeugen (inklusive Cybersicherheit) zuverlässig zu gewährleisten. Wegen dieser dringend benötigten Voraussetzungen wird für die offene und interoperable Telematikplattform noch dringender Entwicklungs- und auch Regulierungsbedarf gesehen, weshalb es sich um eine langfristig zu implementierende Lösung handelt. Dabei kann die offene und interoperable Telematikplattform für den zukünftigen Übergang zu einem integrierten Mobilitätssystem mit automatisiertem (und autonomen) Fahren eine geeignete technische Grundlage darstellen.[152]

Ein weiterer Konzeptvorschlag in diesem Zusammenhang ist die „Sichere On-Board Telematik-Plattform“ (S-OTP), welche von mehreren deutschen Verbänden unterstützt wird.[153] Auch hier bedarf es keiner zusätzlichen Hardware, da sie sich aus einer Summe von Basisdiensten im Fahrzeug (z.B.

---

[148] Zu den technischen Details ausführlich das Konzept „ON-BOARD TELEMATICS PLATFORM SECURITY“ der FIA aus 06/2020, S. 14, abrufbar unter https://www.tuvit.de/en/news/downloads/fia-study/ sowie Positionspapier „Policy position on car connectivity” der Fédération Internationale de l’Automobile (FIA) aus 04/2016, S. 7, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf.

[149] Zum IT-Security-Konzept bei On-Board-Telematik-Plattformen vgl. Konzept „ON-BOARD TELEMATICS PLATFORM SECURITY“ der FIA aus 06/2020, abrufbar unter https://www.tuvit.de/en/news/downloads/fia-study/.

[150] In Anlehnung an die Übersicht im Positionspapier „Policy position on car connectivity” der Fédération Internationale de l’Automobile (FIA) aus 04/2016, S. 6, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf.

[151] Dazu ausführlich *Kerber/Gill*, JIPITEC, 2019, 244 ff.; *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 386 ff.

[152] Zur Notwendigkeit von „On-Board Application“-Plattformen für zukünftige Mobilitätssysteme *Specht-Riemenschneider/Kerber*, Designing Data Trustees – A Purpose Based Approach, 2022, S. 66, abrufbar unter https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d.

[153] Gemeinsames Positionspapier verschiedener Verbände aus dem Mobilitätssektor „Sicherer Zugang zum vernetzten Fahrzeug für den Aftermarket“ aus 09/2021, abrufbar unter https://www.gva.de/files/Newsletter/PositionspapierFahrzeugdaten.pdf.

Rechenleistung, Speicherplatz, Schnittstellen zu Aktuatoren, Sensorik (Daten)), den Schnittstellen zum Fahrer (Fahrzeugdisplay und Bedienelemente) sowie einem klaren Zugangs- und Berechtigungskonzept für eine transparente und sichere Regelung des Zugangs zu Fahrzeugdaten und -funktionen zusammensetzt. Das Konzept soll so den wettbewerbssichernden Zugang zu Daten und Funktionen des vernetzten Fahrzeuges bei höchstmöglicher technischer Sicherheit ermöglichen und einen direkten, standardisierten, diskriminierungsfreien und sicheren Zugang zu den Daten im Fahrzeug – mit Zustimmung des Nutzers – gewährleisten und den Marktbeteiligten die Möglichkeit geben, mit den Produkten und Diensten des Herstellers zu konkurrieren und neue Dienstleistungen zu entwickeln.[154]

5. Datenplattform nach dem Data Shared Server-Prinzip

In der Automobilwirtschaft wird zudem ein weiteres Alternativkonzept zum Extended Vehicle-Konzept der Fahrzeughersteller befürwortet, welches aber ebenfalls auf der Telematik-Technologie aufsetzt. So soll die Implementierung einer unabhängig betriebenen Datenplattform nach dem Data Shared Server-Prinzip ermöglicht werden, welche die persönlichen, geografischen und servicerelevanten Daten verwaltet und bei Vorlage einer entsprechenden Autorisierung, Zertifizierung und Authentifizierung der Nutzer und Dienstleister pseudonymisiert oder anonymisiert zugänglich macht.[155] Der Fahrer des jeweiligen Fahrzeugs soll dabei die Entscheidung über die Verwendung und Verarbeitung der Daten haben und wem er diese zur Verfügung stellt.

In den Überlegungen über die Ausgestaltung wurde eine gemeinsame Datenverwaltung aller interessierten Marktteilnehmer, die Zugang zu den Daten haben wollen, angedacht.[156] Ebenso kann auch eine unabhängig betriebene Plattform aufgebaut werden. Im Rahmen dieses Modells sollen alle Marktanbieter von Dienstleistungen rund um das Fahrzeug den gleichen Zugang zu den Daten erhalten und es soll qualitativ, quantitativ und hinsichtlich der Zugriffsgeschwindigkeit keine Unterschiede geben.[157] Im Unterschied zu der (S-)OTP, wo die vom Fahrzeug generierten Daten frei abrufbar und direkt nutzbar sein sollen, sollen beim Data Shared Server-Prinzip die Daten aus dem Fahrzeug auf eine neutrale Plattform fließen und mit Zugang soll man diese Daten nutzen können.

Die Funktionsweise stellt die folgende Übersicht (**Abb. 8**) anschaulich dar:[158]

[154] Stellungnahme des ADAC e.V. zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datengesetz“) aus 05/2022, S. 4, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf.

[155] Zum Konzept *Kerber/Gill*, in: Stiftung Datenschutz, Datenschutz im vernetzen Fahrzeug, 2020, S. 85, 87 f.; zur vertragsrechtlichen Ebene in diesem Konzept *Metzger/Mischau*, in: Stiftung Datenschutz, Datenschutz im vernetzen Fahrzeug, 2020, S. 135, 140 ff.

[156] Vgl. C-ITS Platform, Final Report, 2016, S. 81 f., abrufbar unter https://www.polisnetwork.eu/wp-content/uploads/2019/09/c-its-platform-final-report-january-2016.pdf.

[157] Positionspapier „Connected Cars – Der Zugriff auf die Fahrzeugdaten“ des European Automobile Clubs (EAC) aus 11/2016, abrufbar unter https://www.eaclubs.org/de/connected-cars-access-to-vehicle-da.

[158] In Anlehnung an die Übersicht im Positionspapier „Policy position on car connectivity” der Fédération Internationale de l’Automobile (FIA) aus 04/2016, S. 5, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf.

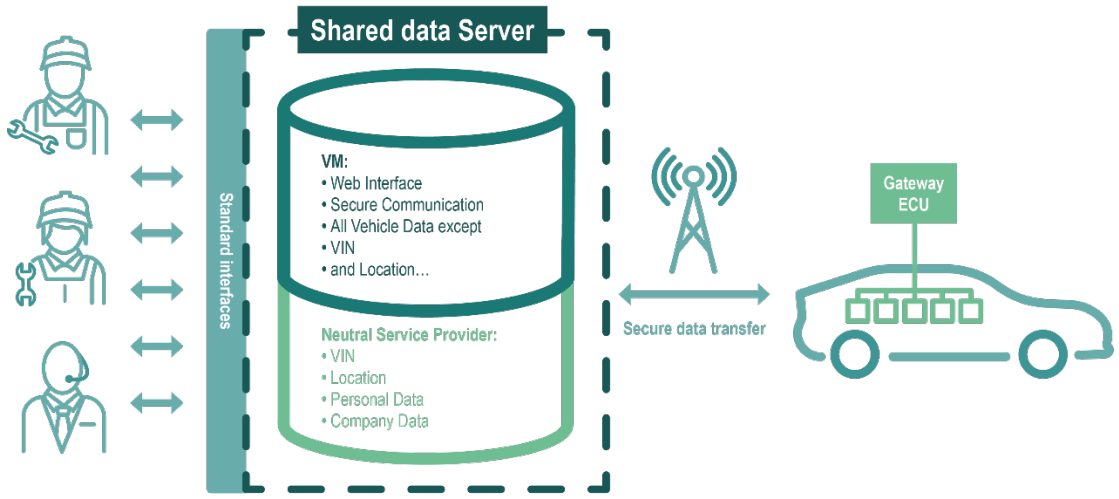


Abb. 8 – Übersicht zur Funktionsweise des Data Shared Server-Prinzips

Obwohl die Data Shared Server-Lösung bereits seit dem Jahr 2016 diskutiert wird[159], ist die Frage der konkreten Ausgestaltung bisher in der Automobilwirtschaft wenig vorangetrieben worden, denn dieses Konzept wird zwar als kurzfristig umsetzbar, aber nur als Zwischenlösung angesehen.[160]

Eng mit der ursprünglichen Data Shared-Server-Idee zusammenhängend ist auch das oft diskutierte Konzept einer Datentreuhandlösung in diesem Bereich.[161] Der Server, auf welchen die vom Fahrzeug generierten Daten über ein Telematik-System übertragen werden, soll dabei unter der Kontrolle einer neutralen Instanz stehen, die diese Daten verwaltet und nach bestimmten Prinzipien zugänglich machen kann. Institutionell kann es sich bei dieser Datentreuhand um eine staatliche Instanz handeln, wobei dann häufig von auch von einem staatlichen Trust-Center gesprochen wird, oder auch eine privatrechtlich organisierte Institution, die mit dieser datentreuhänderischen Aufgabe betraut wird.

Auch das im November 2022 vom Verbraucherzentrale Bundesverband e.V. vorgelegte Konzept eines „Mobilitätsdatenwächters" setzt an diesem Punkt an.[162] Ein Datentreuhänder soll den Zugang zu Mobilitätsdaten in technischer Hinsicht gewährleisten. In Verbindung mit diesem Datentreuhänder soll der sogenannte „Mobilitätsdatenwächter" mithilfe eines Personal Information Management Systems (PIMS) den kontrollierten und transparenten Umgang mit Mobilitätsdaten gemäß den Vorgaben des Fahrzeugnutzers für Dritte sicherstellen. Der Mobilitätsdatenwächter fungiert dabei als

[159] Vgl. Studie „Access to In-vehicle Data and Resources – Final Report" im Auftrag der EU-Kommission, durchgeführt von TRL aus 05/2017, abrufbar unter https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf.

[160] Vgl. Positionspapier „Connected Cars – Der Zugriff auf die Fahrzeugdaten" des European Automobile Clubs (EAC) aus 11/2016, abrufbar unter https://www.eaclubs.org/de/connected-cars-access-to-vehicle-da; Stellungnahme des ADAC e.V. zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datengesetz") aus 05/2022, S. 4, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf; Studie „Access to In-vehicle Data and Resources – Final Report" im Auftrag der EU-Kommission, durchgeführt von TRL aus 05/2017, S. 8 ff., abrufbar unter https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf.

[161] Zu Datentreuhändern im Mobilitätssektor ausführlich *Specht-Riemenschneider/Kerber*, Designing Data Trustees – A Purpose-Based Approach, 2022, S. 59 ff., abrufbar unter https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d.

[162] Gutachten „Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung - Notwendigkeit, Modell, gesetzliche Grundlagen" im Auftrag des Verbraucherzentrale Bundesverband e.V. vom 15.11.2022, abrufbar unter https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilitätsdatenwächter_BRC_2022-15-11_Clean_Finalversion.pdf.

Autorisierungsstelle gegenüber dem Datentreuhänder.[163] Im Rahmen dieses Konzeptes soll auch der jeweilige Fahrzeughersteller wie jeder andere Dritte behandelt werden.[164]

III. Analyse der bestehenden gesetzlichen Regelungen und (derzeitigen sowie künftigen) Konzepte/Projekte

Schließlich wird folgend analysiert, inwiefern die zuvor aufgezeigten bereits existierenden Zugangs- und Nutzungsrechte, -pflichten und -anreize sowie die dargestellten privatwirtschaftlichen Konzepte und Projekte zu einem diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich beitragen können.

1. Analyse der bestehenden gesetzlichen Regelungen

a) Typengenehmigungsverordnung

Mit Blick auf die Typengenehmigungsverordnung lässt sich feststellen, dass es sich um eine umfassende sektorspezifische Regulierung handelt, die ein verpflichtendes Zugangsregime zu den definierten Informationen (und Diagnosedaten) für unabhängige Kfz-Reparatur- und Wartungsbetriebe darstellt, welches den Wettbewerb im Bereich Reparatur- und Wartungsdienstleistungen sichern soll. Insoweit kann von einem fairen und diskriminierungsfreien Zugang zu Informationen und Daten über standardisierte technische Schnittstellen mit gebotenen Sicherheitsstandards (inklusive sicherheitsbezogenen Zertifizierungen) gesprochen werden. Die verankerte Gebührenregelung widerspricht dem grundsätzlich nicht, auch wenn die Kosten für den Zugang zu den Daten, die angemessenen (nicht abschreckend) sein sollen, aus Sicht einiger Marktakteure Hindernisse darstellen, die Einfluss auf die Marktstruktur habe und zudem die Kosten für Verbraucher wesentlich erhöhten. Häufig vorgebracht wird zudem ein hoher Verwaltungsaufwand, weil jeder Hersteller einen anderen, oftmals komplizierten Prozess für die Anmeldung verwende.[165]

Allerdings sind die so verfügbaren Daten per gesetzlicher Definition in Anhang X begrenzt auf OBD- sowie Fahrzeugreparatur- und Wartungsinformationen (Repair & Maintenance Information, RMI) und der Datenaustausch findet lediglich durch den kabelgebundenen Zugriff über die OBD-Schnittstelle statt. Mit Blick auf das vernetzte Fahrzeug und den Betrieb oder die Entwicklung von fahrzeugdatenbasierten Geschäftsmodellen kommt es teilweise bereits heute und mit großer Sicherheit in naher Zukunft maßgeblich darauf an, dass ein Datenzugang der Marktakteure per Fernzugriff auf Fahrzeugdaten sowie -funktionen und -ressourcen per Mobilfunkschnittstelle in kurzen Intervallen oder gar in Echtzeit vorhanden ist. Dies ergibt sich aus der Typengenehmigungsverordnung nicht ohne Weiteres, denn sie zielt darauf ab, z. B. freien Werkstätten den Zugang zu notwendigen Informationen

[163] Gutachten „Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung - Notwendigkeit, Modell, gesetzliche Grundlagen“ im Auftrag des Verbraucherzentrale Bundesverband e.V. vom 15.11.2022, S. 34, abrufbar unter https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilitätsdatenwächter_BRC_2022-15-11_Clean_Finalversion.pdf.

[164] Gutachten „Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung - Notwendigkeit, Modell, gesetzliche Grundlagen“ im Auftrag des Verbraucherzentrale Bundesverband e.V. vom 15.11.2022, S. 25 f., abrufbar unter https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilitätsdatenwächter_BRC_2022-15-11_Clean_Finalversion.pdf.

[165] Vgl. Stellungnahme „Eingeschränkter Zugang zur OBD (On-Board-Diagnose) bei neueren Modellen“ des ADAC e.V. aus 1/2022. Aus wirtschaftlicher Sicht entstehe durch diese Regelung für die Berechtigten im Hinblick auf die entstehenden Kosten für den Datenzugang ein hoher Kostenfaktor, denn für jedes Fabrikat werde ein Zugang zu dem Portal des jeweiligen Herstellers benötigt, so dass die Berechtigten für jeden Zugang und jeden Datenabruf Entgelte zahlen müsse. Auch wenn dieser Zugang zu angemessenen (nicht abschreckenden) Preisen zu gewähren sein solle, so sei dies für die Berechtigten ein Kostenfaktor, der sich nur durch eine Fokussierung auf bestimmte Marken, Modelle und Fabrikate amortisiere und eine Konzentration vieler (vor allem nicht finanzstarker) Marktteilnehmer auf ausgewählte Marken, Modelle und Fabrikate bewirke, was im Ergebnis aber zu weniger Auswahl für den Verbraucher führe.

für die traditionellen Reparatur- und Wartungsdienstleistungen bezüglich eines analogen Fahrzeugs zu ermöglichen.

Es ist daher festzustellen, dass die Informations- und Datenzugangsregulierung der Typengenehmigungsverordnung nicht zu der neuen Technologie vernetzter Fahrzeuge passt.[166] Ein Datenzugang für die Umsetzung digitaler, fahrzeugdatenbasierter Geschäftsmodelle ist in dem Regelungswerk nicht angelegt. Einen diskriminierungsfreien, chancengleichen Wettbewerb zwischen allen Marktakteuren im Mobilitätsdatenbereich mit Blick auf digitale Geschäftsmodelle auf Basis aktueller Fahrzeugtechnik stellt die Typengenehmigungsverordnung daher nicht sicher, sondern regelt nur für einen begrenzten Bereich innerhalb der gesamten Wertschöpfungskette einen Datenzugang, der zudem den Interessen dritter Servicedienstleister sowie der Dienstleistungsnehmer nicht vollständig gerecht wird. Zu Recht wird daher gefordert, dass diese Verordnung ein großes Update erhalten soll.[167]

b) Kfz-GVO

Ebenso wie die Typengenehmigungsverordnung ist auch die Kfz-GVO mit ihren derzeitigen Regelungen nicht geeignet, digitale Geschäftsmodelle innerhalb der Wertschöpfungskette im Mobilitätsdatenbereich zu fördern und diskriminierungsfreien, chancengleichen Wettbewerb zwischen allen Marktakteuren sicherzustellen. Es werden nur beschränkte Datenzugänge hinsichtlich bestimmter Vorleistungen angesprochen, welche „unabhängige Marktbeteiligte“ im Sinne der Kfz-GVO für die Instandsetzung von Fahrzeugen benötigen. Eine Evaluation der EU-Kommission kommt zu dem Ergebnis, dass die Regelungen im gegenwärtigen Rahmen für diese Märkte geeignet ist, aber möglicherweise in gewissem Maße aktualisiert werden sollte, um der zunehmenden Bedeutung von Daten Rechnung zu tragen.[168] Die Kommission schlägt vor, die bestehenden Grundsätze für die Bereitstellung von technischen Informationen, Werkzeugen und Schulungen, die für die Erbringung von Instandsetzungs- und Wartungsdienstleistungen erforderlich sind, explizit auf fahrzeuggenerierte Daten auszuweiten.[169]

c) eCall-VO

Die eCall-VO stellt insoweit eine Besonderheit dar, denn sie legt die Implementierung eines bordeigenen eCall-Systems im Fahrzeug fest, welche sich auf eine interoperable, standardisierte, sichere und frei zugängliche Plattform stützen muss, womit Vorgaben an die Systemarchitektur von Telematikdiensten bei Personenfahrzeugen gestellt werden. Allerdings können die so erzeugten Daten nur für den von der eCall-VO definierten Zweck verwendet werden. Ein Datenaustausch zwischen dem gesetzlich vorgeschriebenen eCall-System und herstellerspezifischen Connected-Services ist

---

[166] So auch *Kerber/Gill*, in: Stiftung Datenschutz, Datenschutz im vernetzen Fahrzeug, 2020, S. 85, 89. Kritisch zur jüngsten Reform der Typengenehmigungs-VO vgl. ausführlich *Kerber/Gill*, JIPITEC, 2019, S. 244 ff.

[167] *Kerber/Gill*, in: Stiftung Datenschutz, Datenschutz im vernetzen Fahrzeug, 2020, S. 85, 91; Stellungnahme des ADAC e.V. zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datengesetz“) aus 05/2022, S. 1, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf; Positionspapier „Sicherer Zugang zum vernetzten Fahrzeug für den Aftermarket“ aus 09/2021, S. 1, abrufbar unter https://www.gva.de/files/Newsletter/PositionspapierFahrzeugdaten.pdf; Positionspapier „ACCESS TO VEHICLE DATA, FUNCTIONS AND RESOURCES„ des International Motor Vehicle Inspection Committe (CITA) aus 06/2022, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources/F3316299_en.

[168] Bewertungsbericht der Kommission über die Anwendung der Verordnung (EU) Nr. 461/2010 (Kfz-Gruppenfreistellungsverordnung) vom 28.5.2021, COM(2021) 264 final, abrufbar unter https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)264&lang=en.

[169] Pressemitteilung der EU-Kommission vom 6.7.2022, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/IP_22_4282.

ausdrücklich untersagt. Daher stehen diese Daten im Rahmen der Wertschöpfungskette weder dem Fahrzeughersteller noch sonstigen Marktakteuren zur Verfügung.

d) IVS-Richtlinie

Die IVS-Richtlinie und auch das IVSG regeln in ihrem Anwendungsbereich eine Bereitstellungspflicht von bestimmten Mobilitätsdaten. Die Nutzung dieser Daten ist vor allem für den Betrieb und die Entwicklung von Beförderungs- und Verkehrsdienstleistungen relevant. Unternehmen, die mit diesen Mobilitätsdaten neue Geschäftsmodelle erproben wollen, müssen sich aber die Frage stellen, wie sich Risiken mangelnder Datenqualität (vertraglich) allokieren lassen. Zum einen sollen bestimmte Daten über die bereits angesprochene Mobilithek offen und uneingeschränkt zugänglich gemacht werden (sog. Open Data). Zum anderen soll die Mobilithek als Datenmarktplatz einen privaten Datenaustausch mit individuell zu verhandelnden Nutzungsrechten ermöglichen. Da diese Plattform erst seit Juli 2022 besteht und wesentliche Funktionen erst ab Februar 2023 möglich sein sollen, bleibt abzuwarten, welche Standards und Best Practices sich bei der Gestaltung der zugrundeliegenden Datenlizenzen durchsetzen werden. Insgesamt ist dabei festzustellen, dass die so verfügbar gemachten Daten nicht für alle Marktakteure in der Wertschöpfungskette relevant sind und die Begrenzung der frei zugänglichen Daten und die Notwendigkeit des Abschlusses von individuellen Verträgen für eine erweiterte Datennutzung vermutlich nicht zu einem diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich beitragen.

Derzeit wird auch eine Überarbeitung der IVS-Richtlinie diskutiert. Bei der Überarbeitung soll der Anwendungsbereich der Richtlinie erweitert werden, um neuen Diensten besser Rechnung zu tragen. Dies betrifft z. B. multimodale Informations-, Buchungs- und Ticketausstellungsdienste (z. B. Apps zur Ermittlung und Buchung von Reisen, die eine Kombination aus öffentlichen Verkehrsmitteln, Car- und Bike-Sharing nutzen), die Kommunikation zwischen Fahrzeug und Infrastruktur (für eine erhöhte Sicherheit) und die automatisierte Mobilität. Zudem sollen zentrale Daten eingeholt und wichtige Dienste bereitgestellt werden, darunter z. B. Echtzeit-Informationsdienste, die die Fahrerinnen und Fahrer über Unfälle oder Hindernisse auf der Straße informieren.[170]

e) Kartellrechtliche Überlegungen

Hinsichtlich einer Analyse zu den aufgezeigten kartellrechtlichen Regelungen, die für die Untersuchung relevant sind, ist festzustellen, dass noch keine sichere Anwendungspraxis in Bezug auf einen Datenzugangsanspruch im Zusammenhang mit dem vernetzten Fahrzeug besteht. Allgemein lässt sich feststellen, dass es im Zusammenhang mit etwaigen Pflichten marktbeherrschender bzw. relativ marktmächtiger Unternehmen zur Gewährung von Datenzugang nach Artikel 102 AEUV / §§ 19, 20 GWB bzw. nach § 20 Abs. 1a GWB annähernd keine Rechtsprechung oder Behördenentscheidungen gibt.[171]

[170] Vgl. Vorschlag der EU-Kommission für eine Richtlinie zur Änderung der Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern vom 14.12.2021, abrufbar unter https://www.bundesrat.de/SharedDocs/drucksachen/2022/0001-0100/28-22.pdf;jsessionid=77EFE994B7BC8C034BFCB6FEB7C459BD.1_cid391?__blob=publicationFile&v=1.

[171] *Schweitzer/Metzger/Blind/Richter/Niebel/Gutmann* führen dies nicht auf Defizite des Wettbewerbsrechts zurück, sondern sehen mögliche Erklärungen vielmehr in dem frühen Stadium der Datenwirtschaft, in Informationsasymmetrien und in dem Umstand, dass die Struktur und Formatierung von Datensätzen regelmäßig auf die Verwendungszwecke des jeweiligen Dateninhabers abgestimmt und für andere Zwecke nicht notwendig zielführend ist, vgl. Studie „Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy - A legal, economic and competition policy angle" vom 8.7.2022, S. 21, abrufbar unter https://pure.mpg.de/rest/items/item_3457829_2/component/file_3457831/content.

aa) Marktdefinition und Bestimmung der Marktmacht

Ob ein Fahrzeughersteller auf einem bestimmten Markt für Daten eine marktbeherrschende Stellung im Sinne des Art. 102 AUEV hat, ist derzeit unklar.

Eine marktbeherrschende Stellung auf einem (zu bestimmenden) Datenmarkt muss wohl anzunehmen sein, wenn anderen Unternehmen ohne Zugang zu den notwendigen Daten der Marktzutritt verwehrt bleibt und das den Marktzugang suchende Unternehmen die benötigten Daten nicht selbst generieren oder von Dritten erwerben kann. Wenn unabhängige Diensteanbieter Zugang zu bestimmten Datensätzen im Fahrzeug haben möchten, die sich ausschließlich im Besitz der Fahrzeughersteller befinden, können letztere als marktbeherrschend angesehen werden, soweit diese Daten nicht anderweitig zugänglich sind und die Fahrzeughersteller ein Monopol auf alle diese Daten, die in den von ihnen verkauften Fahrzeugen erzeugt werden.[172] Daher ist es durchaus möglich, einen spezifischen Markt für Daten eines bestimmten Fahrzeugherstellers abzugrenzen, die erforderlich sind, um den Nutzern dieser Fahrzeuge bestimmte Dienste anzubieten. Im Hinblick auf die Marktdefinition sind diese Sekundärmärkte daher separate Märkte.[173]

Potentiell kann aber die Inhaberschaft über Daten im Sinne eines faktischen Monopols eine marktbeherrschende Stellung darstellen, aus der bei einer missbräuchlichen Geschäftsverweigerung ebenso eine kartellrechtliche Zwangslizenz folgen kann.[174] Dabei ist aber zu beachten, dass Datenmacht als solche nicht grundsätzlich mit Marktmacht gleichzusetzen ist. Eine marktbeherrschende Stellung durch Datenmacht kommt aber jedenfalls dann in Betracht, wenn das inhabende Unternehmen durch seine Entscheidung den Wettbewerb beeinflussen kann oder sich Wettbewerbsdruck entziehen kann.[175] Das ist insbesondere der Fall, wenn der Zugang zu Daten eine Marktzutrittsschwelle darstellt oder Wettbewerber in sonstiger Weise vom Markt ausgeschlossen werden können.[176] Ob dies so ist, hängt im Einzelfall von dem jeweiligen Zugangsobjekt Daten ab.

Wie bereits aufgezeigt sind die Käufer eines vernetzten Fahrzeugs in der Regel fest in das Ökosystem des jeweilige Fahrzeugherstellers eingebunden. Gerade im Automobilbereich sind die herstellerbezogenen Daten, die nur durch den Fahrzeughersteller oder den direkt Berechtigten erstellt werden können, häufig aufgrund rechtlicher oder faktischer Hindernisse nicht duplizierbar. In diesem Fall verfügt der jeweilige Fahrzeughersteller über einen exklusiven Zugang zu bestimmten Daten. Dies wird im Untersuchungskontext noch zusätzlich dadurch verstärkt, dass bestimmte Dienste durch Dritte nur betrieben werden können, wenn Zugang zu diesen Daten besteht und daher für Dritte eine besondere Abhängigkeit besteht. Damit darf nicht zugleich vorschnell auf eine marktbeherrschende Stellung des datenkontrollierenden Fahrzeugherstellers geschlossen werden, denn entscheidend ist, ob die begehrten Daten nicht auch von anderen Anbietern zur Verfügung gestellt werden können. Diese wären dann ebenfalls dem relevanten Markt zuzuordnen, was die marktbeherrschende Stellung eines einzelnen Dateninhabers ausschließen könnte. Wie aufgezeigt liegt genau diese Situation aber wegen der geschlossenen Systeme der Fahrzeughersteller nicht vor und die ausschließliche Kontrolle der Fahrzeugherstellers über das jeweilige Ökosystems verleiht ihnen daher auch eine beherrschende Stellung auf dem fahrzeugherstellerspezifischen Anschlussmarkt und für ergänzende Dienste.[177]

[172] *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 398.
[173] *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 398.
[174] *Louven*, NZKart 2018, 271, 219.
[175] *Telle*, WRP 2016, 814, 817; *Louven*, NZKart 2018, 217, 220.
[176] *Louven*, NZKart 2018, 217, 220 mit Verweis auf Entscheidung der EU-Kommission v. 14.5.2008, COMP/M.4854 – TomTom/Tele Atlas, Rz. 193 ff.
[177] *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 398.

bb) Voraussetzungen der Essential-Facilities-Doktrin

Selbst bei Vorliegen einer marktbeherrschenden Stellung eines Fahrzeugherstellers sind hohe Voraussetzungen zu erfüllen, wenn ein Datenzugang nach der Essential-Facilities-Doktrin gewährt werden soll. So muss der gewünschte Zugang unerlässlich sein für die Erbringung der Dienstleistung der unabhängigen Dienstleistungsanbieter. Nach der Rechtsprechung des EuGH fehlt es an der Unentbehrlichkeit jedenfalls dann, wenn der Petent mit demselben Investitionsaufwand des Inhabers der Daten in der Lage wäre, denselben oder einen entsprechenden Datensatz zu generieren.[178] Dies impliziert, dass bei einer Unerlässlichkeit die Daten nicht über andere Kanäle beschafft werden oder durch andere Daten ersetzt werden können.[179] Wie bereits dargestellt ist dies im Untersuchungskontext gerade nicht der Fall.

Auch muss gerade ohne den gewünschten Zugang zu diesen Daten (oder den Zugang zum Fahrzeug) die Gefahr bestehen, dass der Wettbewerb auf den Sekundärmärkten verhindert wird. Der EuGH versteht die Regeln der Lizenzverweigerung als solche zum Behinderungswettbewerb, über den ein Wettbewerber vom Markt ferngehalten oder ausgeschlossen wird.[180] Voraussetzung ist deshalb, dass der Marktbeherrscher auch auf dem nachgelagerten Sekundärmarkt tätig ist.[181] Wenn die gewünschten Daten des Fahrzeugherstellers eine notwendige Ressource für das Angebot der Dienstleistungen von Dritten sind, dann würde die Verweigerung des Zugangs den Wettbewerb auf diesen Märkten ausschalten. Viele Fahrzeughersteller sind auch auf dem Sekundärmarkt aktiv, so dass sich das Geschäftsfeld, in dem sich der Zugangspetent bewegt, ganz grundsätzlich nicht von jenem des Dateninhabers auf diesem Markt unterscheidet und die Rechtsprechung zur Lizenzverweigerung auch bei der Verweigerung des Zugangs zu diesen Daten eingreifen kann.

Zu beachten ist aber, dass einige Fahrzeughersteller den Zugang zu den benötigten Daten über ihre eigenen Plattformen anbieten, wenn auch gegen Entgelt und in begrenztem Umfang. Auch bei Vorliegen aller Voraussetzungen der Essential-Facilities-Doktrin besteht kein Anspruch auf eine kostenfreie Zugangsgewährung zu Datenpools, sondern es ist nach der einschlägigen Rechtsprechung ein angemessener finanzieller Ausgleich zu leisten. Wie bereits erörtert können die Kosten für benötigte Datenzugänge aber in Summe zu einer hohen Belastung der Marktakteure führen mit der Folge, dass wegen der finanziell bedingten Spezialisierung nur wenig Angebot für bestimmte Dienste herrscht und dies Einfluss auf die Auswahl und die Preise für Verbraucher haben kann. Es ist daher in jedem Fall eine umfassende Analyse des Nutzens und der Kosten einer möglichen Datenzugangsverpflichtung erforderlich, deren Ergebnis auch stark von den spezifischen Datenbeständen abhängen kann, für die der Datenzugang gefordert wird.

Auch die Frage, ob durch den begrenzten oder verwerten Datenzugang ein neues Produkt verhindert wird, ist im hier relevanten Untersuchungskontext schwierig zu beantworten.

Ebenfalls ist zu berücksichtigen, dass eine Weigerung der Zugangsgewährung sachlich gerechtfertigt ist, wenn das marktbeherrschende Unternehmen überwiegende objektive Rechtfertigungsgründe für die Zugangsverweigerung anführen kann, die mit dem Ziel des Wettbewerbsschutzes abgewogen

---

[178] EuGH, Urt. v. 26.11.1998, C-7/97, Slg. 1998, I-7791, Rn. 41 ff. – Bronner.

[179] *Schweitzer/Metzger/Blind/Richter/Niebel/Gutmann* schlagen in Fällen, in denen der Datenzugang über die Möglichkeit entscheidet, innerhalb eines digitalen Ökosystems zu konkurrieren, das zu einem „bottleneck“ für den Zugang zu Kunden geworden ist, vor, dass das Kriterium der Unerlässlichkeit durch eine umfassendere Interessenabwägung ersetzt wird, die der Rolle der Daten für den Wettbewerb in digitalen Ökosystemen oder Wertschöpfungsnetzen Rechnung trägt. vgl. Studie „Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy - A legal, economic and competition policy angle” vom 8.7.2022, S. 22, abrufbar unter https://pure.mpg.de/rest/items/item_3457829_2/component/file_3457831/content. Dazu auch *Schweitzer*, GRUR 2019, 569, 577.

[180] Vgl. Vgl. EuGH, Urt. 6.4.1995, Verb. Rs. C-241/91 P und C-242/91 P, Slg. 1995, I-743 – RTE und ITP gegen Kommission (“Magill”); EuG, Urt. v. 17.9.2007, T-201/04, Slg. 2007, II-3601 – Microsoft gegen Kommission.

[181] *Drexl*, NZKart 2017, 415, 419.

werden müssen.[182] Die objektive Rechtfertigung der Verweigerung des Datenzugriffs ist in der vorliegend relevanten Konstellation ebenfalls nicht allgemein zu beantworten, da die Fahrzeughersteller eine Reihe von Gründen anführen können, die in jeweiligen Kontext des Einzelfalles bewertet werden müssen. Hinsichtlich der hier relevanten Fahrzeugdaten könnte vorgebracht werden, dass es sich um Betriebs- und Geschäftsgeheimnisse handeln kann.[183] Insoweit ist aber zu hinterfragen, ob nicht eine Bereinigung der Daten möglich ist. Ebenso könnte ein Einwand der Fahrzeughersteller sein, dass Produktions- und Produktivprozesse (z. B. Motorenabläufe, Schwankungsbandbreiten, mögliche Ineffizienzen etc.) für Wettbewerber vollständig auslesbar werden und damit Innovationsanreize verlorengehen.[184] Mit dem sogenannten Amortisationsinteresse[185] könnten Fahrzeughersteller auch hinsichtlich des durch eine Datenzugangsverpflichtung verlorengehenden Anreizes zur Gewinnung dieser Daten bei hohen Investitionen argumentieren. Dies ist allerdings in der Digitalökonomie häufig überhaupt nicht der Fall, da Daten, insbesondere bei digitalen Geschäftsmodellen, auch als Nebenprodukt ohne große Investition anfallen können.[186] Schließlich können auch die bereits dargestellten Sicherheitsinteressen der Fahrzeughersteller in diesem Kontext relevant sein.

cc) Marktmacht von Fahrzeugherstellern im Sinne des § 18 GWB

Auch im nationalen Kartellrecht bestehen derzeit noch Unsicherheiten, ob die vorhandenen Normen den betroffenen Marktakteuren einen sinnvollen Datenzugangsanspruch mit Blick auf die benötigten Daten zum Betrieb oder der Entwicklung innovativer Geschäftsmodelle im Mobilitätssektor bieten. Dies beginnt bei der Bewertung der Marktstellung eines Unternehmens. Zwar hat der Gesetzgeber mit der 10. GWB-Novelle anerkannt, dass der Zugang zu wettbewerbsrelevanten Daten in die Bewertung der Marktstellung nach § 18 Abs. 3 Nr. 3 GWB ein Kriterium zur Bestimmung der Marktmacht eines Unternehmens ist. Zugleich hat er aber auch deutlich gemacht, dass Datenhoheit nur ein Machtfaktor unter mehreren ist.[187] Je nach Marktstruktur kann sich dann in der Folge die Frage stellen, ob die Vermutung kollektiver Marktbeherrschung nach § 18 Abs. 6 GWB greift. Hier wird es im Wesentlichen darauf ankommen, ob zwischen den einzelnen Dateninhabern Wettbewerb in Bezug auf den relevanten Markt – also die Bereitstellung von Daten – zu erwarten ist. Lehnen alle Dateninhaber eine Bereitstellung ab, spricht viel dafür, dass ein wesentlicher Wettbewerb i.S.v. § 18 Abs. 7 Nr. 2 GWB nicht zu erwarten ist und sie deshalb gemeinsam marktbeherrschend sind.[188]

dd) Missbrauchshandlung nach § 19 Abs. 2 Nr. 4 GWB

Nach aktuellem Stand ist die Begründung des Zugangsanspruchs aus § 19 Abs. 2 Nr. 4 GWB generell und so auch im Hinblick auf den Zugang zu Fahrzeugdaten noch mit erheblichen Unsicherheiten behaftet.[189] Entsprechende Verwaltungsentscheidungen oder Rechtsprechung in Bezug auf den Zugang zu Daten liegen noch nicht vor. Ob die Verweigerung des Zugangs zu Fahrzeugdaten gegenüber dritten Servicedienstleistern eine Missbrauchshandlung i.S.v. § 19 Abs. 2 Nr. 4 GWB darstellt, muss sich noch zeigen.[190] Der weit gefasste Wortlaut der Norm („Zugang zu Daten, zu Netzen

---

[182] Ausführlich zur sachlichen Rechtfertigung der Verweigerung eines Datenzugangs *Huerkamp/Nuys*, NZKart 2021, 327, 331 ff.
[183] Zu diesem Einwand *Peitz/Schweitzer,* NJW 2018, 275, 279; *Louven,* NZKart 2018, 217, 221; *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 401.
[184] Vgl. Ergebnispapier „Industrie 4.0 – Kartellrechtliche Betrachtungen“ des BMWi aus 02/2021, S. 22, abrufbar unter https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Kartellrechtliche-Betrachtungen.pdf?__blob=publicationFile&v=5.
[185] Dazu *Wolf/Westermann,* in: MüKoWettbR, § 19 GWB Rn. 168
[186] *Käseberg,* NZKart 2018, 441; *Höppner/Weber,* K&R 2020, 24, 45. *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 401 differenziert bei Daten zwischen einer nahezu kostenfreien "Ernte" von Daten als Nebenprodukt eines Dienstes bis hin zu einer möglichen teuren Produktion von Daten (z. B. durch spezifische Sensoren).
[187] BT-Drucksache 19/23492 vom 19.10.2020, S. 69, abrufbar unter https://dserver.bundestag.de/btd/19/234/1923492.pdf.
[188] *Huerkamp/Nuys*, NZKart 2021, 327, 328.
[189] Zum Hintergrund der Norm *Huerkamp/Nuys*, NZKart 2021, 327.
[190] Vgl. zum Datenzugangsanspruch nach § 19 Abs. 2 Nr. 4 GWB *Huerkamp/Nuys*, NZKart 2021, 327; *Weber*, WRP 2020, 559.

oder anderen Infrastruktureinrichtungen“) soll ermöglichen, dass die Weigerung eines marktbeherrschenden Unternehmens, einem anderen Unternehmen Zugang zu Daten, Plattformen oder Schnittstellen zu gewähren, als missbräuchliches Verhalten gewertet werden kann. Selbst nach Erstreckung der Essential-Facilities-Doktrin auf Daten infolge der 10. GWB-Novelle kann die Verweigerung des Zugangs zu den eigenen Datenpools durch ein marktbeherrschendes Unternehmen nach der Rechtsprechung des EuGH, die sich auch der BGH zu eigen gemacht hat[191], nur unter „außergewöhnlichen Umständen“ einen Machtmissbrauch darstellen. Insoweit ist auf die oberen Ausführungen zu verweisen. Zudem wäre es in diesem Kontext auch notwendig, dass Marktakteure auf nachgelagerten Märkten entlang der Wertschöpfungskette nicht nur Zugang zu (fahrzeuggenerierten) Daten erhalten, sondern auch Daten an das Fahrzeug zurücksenden können und mit dem Fahrer eines Fahrzeuges auch über alle vorhandenen Kommunikationsschnittstellen kommunizieren können. Dies wird durch § 19 Abs. 2 Nr. 4 GWB wohl nicht ermöglicht.[192] Hinsichtlich eines chancengleichen, fairen und nichtdiskriminierenden Wettbewerbs bräuchten aber die Marktakteure auf nachgelagerten Märkten einen solchen Zugang zu eben jenen Daten.

ee) Datenzugang nach § 20 Abs. 1a GWB

Nach § 20 GWB können auch Unternehmen mit relativer oder überlegener Marktmach gewissen Restriktionen des Kartellrechts unterliegen. Dies bietet bei Konstellationen wie den hier untersuchten den Vorteil, dass der Fahrzeughersteller als Dateninhaber nicht als marktbeherrschend im Sinne von Art. 102 AEUV bzw. § 18 GWB angesehen werden muss, weshalb es auch nicht erforderlich ist, die Wirksamkeit des Systemwettbewerbs zu analysieren. Dies könnte im Untersuchungskontext gerade für Reparatur- und Wartungsdienstleister relevant sein, die sich auf die Erbringung von Dienstleistungen auf den Sekundärmärkten für verbundene Geräte (Primärprodukte) bestimmter Fahrzeughersteller spezialisiert haben.[193] Aber auch andere Diensteanbieter, die Aftermarket- oder andere Dienste im Ökosystem der vernetzten Autos anbieten möchten, benötigen den Zugang zu bestimmten Datensätzen und sind diesbezüglich abhängig von den Fahrzeugherstellern mit ihrer ausschließlichen Kontrolle über die Daten, weshalb eine relative Marktmacht der Fahrzeughersteller im Sinne des § 20 Abs. 1 GWB angenommen werden kann.[194]

Auch hinsichtlich § 20 Abs. 1a GWB ist festzustellen, dass das Datenzugangsproblem des Kfz-Aftermarket mit Blick auf Echtzeitdaten nicht vollumfänglich erfasst wird, da die Norm den Datenzugangsanspruch insbesondere auf die beim Anspruchsgegner vorliegenden und diesem ebenfalls zur Verfügung stehenden Daten begrenzt.[195] Ebenso birgt die vorzunehmende Unbilligkeitsprüfung, bei welcher die Interessen des Normadressaten und des Zugangspetenten abzuwägen sind, Unsicherheiten, auch wenn die Gesetzesbegründung explizit davon ausgeht, dass für eine Unbilligkeit der Verweigerung des Datenzugangs Umstände, wie beispielsweise ein Verschluss von Sekundärmärkten durch die Verweigerung des Zugangs oder ein erhebliches Potential für zusätzliche bzw. erhöhte Wertschöpfungsbeiträge auf Seiten des abhängigen Unternehmens sprechen.[196]

[191] BGH, Urt. v. 13.7.2004, KZR 40/02 – Standard-Spundfass; Beschl. v. 4.3.2008, KVR 21/07 – Soda Club II.
[192] Zur möglichen Ausgestaltung des Datenzugangsverhältnisses *Louven*, NZKart 2018, 217, 222.
[193] Hierzu ausführlich *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 410 f.
[194] *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 411.
[195] BT-Drucksache 19/23492 vom 19.10.2020, S. 81, abrufbar unter https://dserver.bundestag.de/btd/19/234/1923492.pdf.
[196] BT-Drucksache 19/23492 vom 19.10.2020, S. 81, abrufbar unter https://dserver.bundestag.de/btd/19/234/1923492.pdf.

ff) Schlussfolgerung

Das Kartellrecht bietet daher Ansätze zur Lösung des aufgezeigten Problems, ist jedoch mangels vorhandener Anwendungsfälle gerade im Bereich des Datenzugangs mit vielen Unsicherheiten behaftet.

Selbst bei Vorliegen aller Voraussetzungen der Essential-Facilities-Doktrin sind die Fragen der Datenportabilität sowie der Latenzzeit des Datenzugriffs in diesem Kontext nicht geklärt.[197] Der Anspruch umfasst die Belieferung mit Daten, weshalb es aber nur um bereits bestehende (und möglicherweise sogar aufbereitete) Daten(sätze) gehen kann. Mit Blick auf die für innovative Geschäftsmodelle relevanten Echtzeitdaten wäre ein direkter Zugriff auf Rohdaten (Daten, die nicht aufbereitet sind und die man so direkt wie möglich am entsprechenden Sensor ausliest) notwendig. Zudem wäre es in diesem Kontext auch notwendig, dass Marktakteure auf nachgelagerten Märkten entlang der Wertschöpfungskette nicht nur Zugang zu (fahrzeuggenerierten) Daten erhalten, sondern auch Daten an das Fahrzeug zurücksenden können und mit dem Fahrer eines Fahrzeuges auch über alle vorhandenen Kommunikationsschnittstellen kommunizieren können.

Ebenso unklar ist, ob die Fahrzeughersteller zur Entwicklung offener interoperabler Telematikplattformen verpflichtet werden können.[198]

Zu erwähnen bleibt schließlich, dass das Wettbewerbsrecht – selbst bei Vorliegen der Voraussetzungen – traditionell nur eingeschränkt geeignet ist, Dritten den erforderlichen Zugang zu den Daten zu ermöglichen. Grund hierfür ist, dass derartige Verfahren sehr viel Zeit in Anspruch nehmen und damit in schnelllebigen Märkten wie jenem der Datenökonomie für die Dritten in der Regel keine ausreichende Abhilfe schaffen.[199]

2. Analyse der (derzeitigen und künftigen) Konzepte/ Projekte

Die aufgezeigten Konzepte und Projekte zum derzeitigen sowie zukünftigen Datenaustausch im Mobilitätsbereich unterschieden sich stark hinsichtlich der Art und Weise der Zurverfügungstellung von Daten. Auch in zeitlicher Hinsicht der Umsetzungsmöglichkeit gibt es erhebliche Unterschiede.

a) Plattformen der Fahrzeughersteller

Im Hinblick auf einen diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich sind die Plattformen der Fahrzeughersteller in der Breite nicht geeignet, in dieser Hinsicht einen Beitrag zu leisten. Durch das Extended Vehicle-Konzept erhält der jeweilige Fahrzeughersteller exklusiven Zugriff auf die Fahrzeugdaten, weshalb sie diesem für den Betrieb oder die Entwicklung von Anschlussdiensten unmittelbar zur Verfügung stehen. Dies hat auch das Potenzial, den Fahrzeughersteller in eine privilegierte Position auf dem Markt zu bringen, auf dem der Fahrzeughersteller mit Dritten um dieselben Anschlussdienste konkurriert. Die Fahrzeughersteller gewähren in der Praxis – falls überhaupt[200] – über ihre eigenen Server außerhalb

---

[197] Dazu *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 403.

[198] *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 405 f. weist aber darauf hin, dass es möglich sein kann, die Fahrzeughersteller zu verpflichten, Sicherheits- und Sicherungssysteme für den technischen Fernzugriff auf ihre vernetzten Fahrzeuge zu entwickeln, die es unabhängigen Dienstleistern ermöglichen, bestimmte Dienstleistungen (wie z.B. Fernreparatur- und Wartungsdienste) direkt im Fahrzeug zu erbringen.

[199] Vgl. *Wendehorst/Schwamberger,* DAR 2022, 541, 543; *Kerber*, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, 381, 406.

[200] Das zurückhaltende Datenteilen im Mobilitätssektor keine Ausnahme, sondern eher die Regel im kommerziellen Bereich. Nach einer Erhebung der EU-Kommission werden bei 78 % der befragten Unternehmen die Daten unternehmensintern oder von einem Unterauftragnehmer erzeugt und analysiert. Die vertikale Integration ist in den untersuchten Sektoren nach wie vor die wichtigste Strategie. Die Daten bleiben innerhalb des Unternehmens und werden nicht mit Dritten gehandelt, vgl. COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy Accompanying the document

des Fahrzeugs den Zugriff auf bestimmte Fahrzeugdaten, wobei teilweise nur begrenzte und/oder vorverarbeitete Datensätze/Funktionen verfügbar sind. Hierzu bedarf es einer vertraglichen Vereinbarung mit dem jeweiligen Fahrzeughersteller, wodurch der Fahrzeughersteller einen erheblichen Wettbewerbs- und Verhandlungsvorteil hat. Die Fahrzeughersteller sind nach diesem Modell auch in der Lage, Kenntnis darüber zu erlangen, ob und welcher Drittanbieter wann und wie häufig den Zugriff auf Fahrzeugdaten nutzt. Sie erhalten dadurch umfassenden Einblick in die Geschäftstätigkeiten anderer Marktbeteiligter.

Zwar gibt es eine Tendenz zur Harmonisierung bestimmter Datensätze, doch gibt es derzeit keine Einheitlichkeit über Fahrzeugmarken hinweg, was datengetriebene Geschäftsmodelle erschwert und die Kosten für die Nutzung und den Austausch von Daten erhöht. Darüber hinaus gibt es keine Transparenz über die Fahrzeugmarken hinweg, was die von den Fahrzeugherstellern zur Verfügung gestellten Datenpunkte betrifft. Die Gewährung des Zugriffes eines Dritten über die Telematiksysteme direkt auf die Fahrzeugressourcen in Echtzeit scheint in der Praxis die absolute Ausnahme zu sein. Als Hauptargument, unabhängigen Dienstleistern keinen direkten Zugriff auf Fahrzeugdaten zu gewähren, werden seitens der Automobilindustrie Haftungsrisiken und IT-Sicherheitsbedenken angeführt.[201] Die Tatsache, dass andere Marktteilnehmer keinen direkten Zugang zu den Fahrzeugressourcen haben, bedeutet auch, dass der Fahrzeughersteller bei der Interaktion mit dem Nutzer eine privilegierte Stellung bei der Bereitstellung von Diensten einnimmt.

Insgesamt kann mit Blick auf das Extended Vehicle-Konzept und die Möglichkeit des Datenbezugs über die herstellereigenen Plattformen davon ausgegangen werden, dass das Risiko eines unlauteren Wettbewerbs besteht und dass der Markt für bestehende und künftige Dienste, die Fahrzeugdaten nutzen, zum Nachteil der Verbraucher verzerrt wird.[202]

Das ADAXO-Konzept bindet zwar (auch bzw. alternativ) einen neutralen Server in den Datenaustausch ein, der Bezug von Daten beruht aber weiterhin auf individuellen Verträgen zwischen den am Konzept beteiligten Fahrzeugherstellern und den Dritten, welche Daten beziehen möchten. Zudem wird in diesem Zusammenhang an dem Extended Vehicle-Konzept festgehalten, wodurch die oben bereits aufgezeigten Privilegierungen der Fahrzeughersteller erhalten bleiben.

b) Data Shared-Server

Hinsichtlich des Konzeptes des Data Shared-Servers ist festzustellen, dass dieses eine Möglichkeit darstellt, die derzeit bestehende Gatekeeper-Position der Fahrzeughersteller erst gar nicht entstehen zu lassen. So können Wettbewerbsnachteile auf Seiten der unabhängigen Marktteilnehmer vermieden werden. Dieses Konzept ist technisch gesehen vergleichbar mit dem Extended Vehicle und daher auch umsetzbar. Zudem würde so auch die Möglichkeit des Zugriffes der Fahrzeughersteller auf Geschäftsdaten unabhängiger Drittanbieter vermieden werden können.

Jedoch bestünde selbst bei Umsetzung dieses Konzeptes kein direkter Datenzugang der Marktakteure per Fernzugriff auf Fahrzeugdaten sowie -funktionen und -ressourcen per Mobilfunkschnittstelle in

---

Communication Building a European data economy, SWD(2017) 2 final vom 10.1.2017, S. 15, abrufbar unter: https://op.europa.eu/de/publication-detail/-/publication/30f7e8aa-d808-11e6-ad7c-01aa75ed71a1.

[201] Nach Auffassung des ADAC ist die Frage nach der Sicherheit der Fahrzeugdaten nicht am Speicherort festzumachen, sondern vielmehr an einer Sicherheitsarchitektur, die den Risiken von vernetzten Pkw Rechnung trägt und den Verbraucher bestmöglich schützt. Dieser Schutz sollte nach Standards erfolgen, wie sie in anderen Branchen wie dem IT-Sektor bereits üblich sind. Dieser Schutzstandard sollte von neutraler Stelle bestätigt werden, etwa durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Grundlage international zertifizierter Prozesse wie Common Criteria (ISO/IEC 15408), vgl. Positionspapier „Wettbewerb, Sicherheit und Transparenz: Daten im vernetzen Fahrzeug“ des ADAC e.V. aus 12/2020, S. 6, abrufbar unter https://www.adac.de/-/media/pdf/motorwelt/positionspapier-daten-im-fahrzeug-final-12-2020.pdf.

[202] Vgl. Studie „Access to In-vehicle Data and Resources – Final Report” im Auftrag der EU-Kommission, durchgeführt von TRL aus 05/2017, S. 136, abrufbar unter https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf.

kurzen Intervallen oder gar in Echtzeit. Im Hinblick auf einen diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich kann auch das Data Shared-Server-Konzept nicht dazu beitragen, dass die Privilegierung der Fahrzeughersteller durch das Extended Vehicle-Konzept hinsichtlich ihrer Marktchancen mit Blick auf datenbasierten Anschlussdiensten beseitigt werden. Eine Umsetzung dieses Konzeptes bedingt zudem eine Zustimmung der Fahrzeughersteller oder eine gesetzliche Vorgabe. Auch das Problem der Interoperabilität für die Erbringung von komplementären Serviceleistungen im Fahrzeug müsste durch regulatorischen Ansatz gelöst werden. Insofern sind auch bei diesem Konzept standardisierte interoperable technische Schnittstellen (für Datenaustausch und Interoperabilität) sowie ein standardisiertes Sicherheitskonzept (mit Zertifizierungslösungen für Serviceanbieter) erforderlich. Aus Sicht der Marktakteure stellt das Konzept des Data Shared-Servers nur eine kurzfristige Zwischenlösung dar.[203]

Durch die Einbindung eines Datentreuhänders in das erläuterte Mobilitätsdatenwächtermodell würde der Fahrzeughersteller seine exklusive Entscheidungshoheit über Quantität, Preis und Qualität der Daten verlieren. Dabei müsste jedoch technisch sichergestellt sein, dass es dem Fahrzeughersteller nicht möglich ist, den Datenfluss zwischen Fahrzeug und Datentreuhänder zu beschränken.

Solche oben dargestellten Datentreuhandlösungen können nur im Rahmen einer freiwilligen Selbstverpflichtung der Fahrzeughersteller oder mit einer Regulierung verwirklicht werden, die den Fahrzeugherstellern die Implementierung einer solchen technischen Lösung auferlegt.

c) Offene und interoperable Telematik-Plattform

Die offene und interoperable Telematik-Plattform dagegen wird von vielen Marktakteuren, ausgenommen der Fahrzeughersteller, als mittel- und langfristige Lösung des Datenzugangsproblems gesehen.[204] Dieser direkte, standardisierte, diskriminierungsfreie Zugang zu den Daten im Fahrzeug – mit Zustimmung des Nutzers – gibt auch anderen Marktbeteiligten als den Fahrzeugherstellern die Möglichkeit, mit den Produkten und Diensten des Herstellers zu konkurrieren und neue Dienstleistungen zu entwickeln. Eine Herausforderung für die OTP besteht darin, die IT-Sicherheit des Zugangs über das gesamte Fahrzeugleben zu gewährleisten. Zu berücksichtigen ist zudem, dass die Fahrzeughersteller durch die Monetarisierung von Fahrzeugdaten über ihre Plattformen einen Teil der Entwicklungskosten amortisieren, was bei einer OTP nicht mehr im bisherigen Maße möglich wäre und daher auch Einfluss auf die Innovationskraft von Fahrzeugherstellern haben kann.

Im Hinblick auf einen diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich kann die OTP dazu beitragen, dass die Privilegierung der Fahrzeughersteller durch das Extended Vehicle-Konzept hinsichtlich ihrer Marktchancen mit Blick auf datenbasierten Anschlussdiensten beseitigt werden. Auch bei diesem Konzept würde die derzeit bestehende Gatekeeper-Position der Fahrzeughersteller erst gar nicht entstehen, wodurch mehr Wettbewerb und Innovation gefördert werden kann. Zudem würde auch hier die Möglichkeit des Zugriffes der Fahrzeughersteller auf Geschäftsdaten unabhängiger Drittanbieter vermieden werden können. Eine Umsetzung dieses Konzeptes bedingt ebenfalls eine Zustimmung der

---

[203] Vgl. Stellungnahme des ADAC e.V. zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datengesetz“) aus 05/2022, S. 4, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf

[204] Vgl. Stellungnahme des ADAC e.V. zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datengesetz“) aus 05/2022, S. 4, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf; Gemeinsames Positionspapier verschiedener Verbände aus dem Mobilitätssektor „Sicherer Zugang zum vernetzten Fahrzeug für den Aftermarket“ aus 09/2021, abrufbar unter https://www.gva.de/files/Newsletter/PositionspapierFahrzeugdaten.pdf.

Fahrzeughersteller oder eine Regulierung. Auch das Problem der Interoperabilität für die Erbringung von komplementären Serviceleistungen im Fahrzeug müsste gelöst werden.

IV. Zwischenergebnis

Im Ergebnis gibt es keine umfassenden rechtlichen Regelungen darüber, wie der enorme Umfang an Daten, den moderne Fahrzeuge heutzutage produzieren, konkret von wem verwendet werden darf, wem der Fahrzeugnutzer seine Daten auf welche Weise zur Verfügung stellen kann und wie dabei Transparenz und Sicherheit in Bezug auf die Daten gewährleistet werden kann. Der Zugang zu technischen Daten für Reparaturen und Wartungen ist europarechtlich weitgehend geregelt, er umfasst aber nur einen begrenzten Datensatz über eine bestimmte (analoge) Technik. Daneben gibt es im Sektor Mobilität noch vereinzelte europarechtliche Vorgaben zum Datenteilen auf Basis einer Übermittlungsverpflichtung, wobei die Daten aber den Marktakteuren für den Betrieb oder die Entwicklung von (innovativen) Geschäftsmodellen gar nicht zur Verfügung stehen oder aber nur limitierte Daten zum Nutzen bestimmter Markakteure frei verfügbar sind. Das Kartellrecht scheint für das Thema Datenteilen und Datenzugang mit Bezug zum Mobilitätssektor im Untersuchungskontext eine grundsätzlich geeignete Materie zu sein, jedoch gibt es viele offene Fragen mangels vorhandener Anwendungspraxis und im Ergebnis bietet eine Durchsetzung möglicher Ansprüche den Betroffenen keine ausreichende Abhilfe.

Die privatwirtschaftlichen Konzepte und Projekte zum (zukünftigen) Austausch von Daten in der Automobilwirtschaft zwischen den Marktakteuren lassen sich in zwei sich gegenüberstehende Lager einteilen, die jeweils unterschiedliche technische Ansätze verfolgen und von jeweils unterschiedlichen Interessensvertretern propagiert werden. Zudem unterscheiden sich die Modelle auch hinsichtlich ihres zeitlichen Umsetzungshorizontes.

F. Arbeitspaket 3

I. Grundlegung zur Untersuchung und Bewertung des regulatorischen Rahmens

1. Untersuchungsgang

In der Ausarbeitung zum Arbeitspaket 3 soll der bestehende und in der Diskussion befindliche regulatorische Rahmen daraufhin untersucht werden, welche Auswirkungen sich auf die bestehenden Datenflüsse und Konzepte zum Datenaustausch ergeben. Weiterhin soll analysiert werden, welche regulatorischen Lücken noch identifiziert werden können, und daran anschließend sollen Handlungsempfehlungen abgeleitet werden.

Zunächst soll daher der Vorschlag für ein Datengesetz („DA-E“)[205] daraufhin untersucht werden, wie er sich auf die in Arbeitspaket 1 und Arbeitspaket 2 bereits behandelten Datenflüsse und verschiedenen Konzepte des Datenaustausches beim connected car auswirken würde. In engem Zusammenhang damit ist die Kompatibilität der wichtigsten Modelle mit dem Ansatz des DA-E zu bewerten. Dabei sollen die wichtigen Schnittstellen des DA-E zum Schutz von Betriebs- und Geschäftsgeheimnissen sowie zum Datenschutz behandelt und Möglichkeiten zur Integration der Interessen der Hersteller am Geheimnisschutz sowie der Nutzer am Datenschutz ausgelotet werden. Zu beachten bleibt, dass der Gesetzgebungsprozess zum DA-E zum Zeitpunkt der Erstellung dieser Studie in vollem Gang ist und der ursprüngliche Entwurf mehrmals überarbeitet wurde. Dies wird berücksichtigt, soweit das entsprechende Gesetzesmaterial zugänglich ist.

Des Weiteren sollen die bestehenden sektorspezifischen Regelungen daraufhin untersucht werden, inwieweit diese mit dem Ansatz des DA-E kompatibel sind und bei diesem bestehende Lücken durch die spezifischen Regelungen aufgefüllt werden können. Sodann soll der Vorschlag der EU-Kommission für eine der Entwicklung der Technik angepasste Weiterentwicklung der Typengenehmigungsverordnung (EU) 2018/858 (TypGVO)[206] in gleicher Weise daraufhin analysiert werden, inwieweit die überarbeitete Fassung den regulatorischen Anforderungen nunmehr gerecht wird und ob und welche Defizite hier immer noch verbleiben. Dabei sollen die drei dort von der EU-Kommission angeführten Optionen getrennt betrachtet werden.

Ausgehend von diesem Gesamtbild des sich entwickelnden regulatorischen Rahmens soll abschließend bewertet werden, ob sich bezogen auf die Ziele der Regulierung weitere Regulierungsnotwendigkeiten ergeben und wie und durch welche Maßnahmen diese abgedeckt werden könnten. Am Ende der Untersuchung steht eine daraus abgeleitete Handlungsempfehlung.

2. Ökonomischer Hintergrund und Bewertungskriterien

Die europäische Strategie zum digitalen Binnenmarkt zielt darauf, einen echten Binnenmarkt für Daten zu schaffen und Europa zu einem weltweit führenden Akteur in der datenagilen Wirtschaft durch die Förderung von Wettbewerb und Innovation durch optimalen Zugang zu Daten zu entwickeln.[207] Eines der Kernelemente dieser Strategie ist das geplante Datengesetz. Dieses folgt dem Ziel, eine gerechte Verteilung der Wertschöpfung aus Daten auf die Akteure der Datenwirtschaft zu gewährleisten und den

[205] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM (2022) 68 final, 23.2.2022, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0068.

[206] Verordnung (EU) 2018/858 vom 30. Mai 2018 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG (ABl. L 151 vom 14.6.2018, S. 1),

[207] Mitteilung der Kommission, Eine europäische Datenstrategie, COM(2020) 66 final v. 19.2.2020, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0066.

Datenzugang und die Datennutzung zu fördern. Damit soll dazu beigetragen werden, die Innovations- und Wettbewerbsfähigkeit von EU-Unternehmen sämtlicher Branchen sicherzustellen und die Handlungskompetenz der Menschen in Bezug auf ihre Daten wirksam zu stärken.[208] Diese Zielsetzungen sollen auch der hier durchzuführenden Bewertung des regulatorischen Rahmens zugrunde gelegt werden. Zu beachten bleibt dabei, dass die verschiedenen gesetzgeberischen Initiativen der EU nicht nur einem erkannten Marktversagen abhelfen sollen, sondern auch proaktiv einen rechtlichen Rahmen zur Förderung der Entwicklung innovativer Produkte und Leistungen schaffen soll.

Eine Bewertung der sich entwickelnden Data Governance und der verschiedenen Regulierungsoptionen muss ausgehen von den ökonomischen Gegebenheiten des Ökosystems von connected car und komplementären Produkten und Dienstleistungen.[209] Mit der Investition in das Fahrzeug kann eine lock-in-Situation für den Nutzer entstehen. Der Fahrzeughersteller kann über die Kontrolle des Zugangs zu Daten und Funktionen des Fahrzeugs („in-vehicle data and resources“) den Wettbewerb unabhängiger Diensteanbieter auf den Märkten für nachgelagerte und komplementäre Dienste ausschließen, soweit dieser Zugang für den Marktzutritt notwendig ist.[210] Diese Strategie kann durch Zugangskontrolle aber auch durch vertragliche Koppelung der Dienste umgesetzt werden und in Diskriminierung, Monopolpreisen oder völligem Ausschluss des Zugangs münden.[211]

Entsprechend kann Marktversagen auftreten dadurch, dass

a) durch exklusiven Zugang zu Daten und Fahrzeug der Wettbewerb auf nachgelagerten und komplementären Märkten eingeschränkt wird;
b) ein zu geringes Maß an Interoperabilität eine zu geringe Offenheit des Ökosystems bedingt und dadurch weniger Verbraucherauswahl, Unternutzung der Daten und weniger Innovation zur Folge haben kann.[212]

Die exklusive Datenkontrolle ermöglicht dem Hersteller daher, entweder die komplementären Dienste selbst anzubieten und damit durch vertikale Integration eine Doppelrolle einzunehmen,[213] oder nur einem begrenzten Kreis von Anbietern gegen entsprechende Vergütung Zugang zu gewähren. Weiterhin können sie auch die gesammelten Daten auf Datenmärkten kommerzialisieren. Der eingeschränkte Wettbewerb kann zu höheren Preisen, weniger Verbraucherauswahl und weniger Innovation führen.

Hinzu kommt die zunehmende Einbindung von connected cars in ein Ökosystem vernetzter Mobilität, mit permanentem Datenaustausch zwischen Autos, Straßeninfrastruktur und anderen verbundenen Geräten (vgl. Ziff. D.III.2.a)). Dies erfordert hohe Interkonnektivität und Interoperabilität mit weitgehender Standardisierung von Datenformaten, Datenqualität, Schnittstellen und Sicherheitsmaßnahmen.[214]

---

[208] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz), COM (2022) 68 final, 23.2.2022, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0068, Begründung, S. 3.

[209] Vgl. *Kerber*, 2019 J Comp. L&E 1, 6 ff. Vgl. auch *Kerber*, Jipitec 2018, 310, 316 ff.; *Kerber/Frank*, Data Governance Regimes in the Digital Economy: The Example of connected cars, Working Paper 2017; *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 14 ff., mit einer differenzierten Bewertung der innovationsfördernden Wirkung verschiedener Modelle des Datenzugangs in der Automobilindustrie.

[210] *Kerber*, 2019 J Comp. L&E, 1, 7: “de facto bundling strategy”. Vgl. auch *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 64: Gatekeeper-Position.

[211] Vgl. *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 4 f.

[212] Vgl. *Kerber*, Jipitec 2018, 310, 316 ff. Letzter Aspekt ist insbesondere für die Nutzung als KI-Trainingsdaten relevant.

[213] Aftermarket Alliance, Creating a level playing field for vehicle data access: Secure on-board Telematics Platform Approach, 2021, S. 10.

[214] *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 5.

Schon 2016 hat die EU-Kommission eine Initiative ins Leben gerufen, um mit allen Stakeholdern eine Lösung für die wichtigsten Probleme des vernetzten und autonomen Fahrens zu finden.[215] Dabei hat man sich auf fünf Leitprinzipien verständigt, die für den Zugang zu Daten gelten sollen:

1. Zustimmung des Fahrzeughalters,
2. fairer und nicht-diskriminierender Wettbewerb,
3. Datenschutz für den Fahrer,
4. keine Beeinträchtigung der sicheren Funktionsweise und Haftung des Herstellers,
5. Interoperabilität zwischen Anwendungen durch standardisierten Zugang.[216]

Diese Prinzipien wurden auch der folgenden Studie der EU zu „access to in-vehicle Data and resources" von 2017 zugrunde gelegt, in der die drei wichtigsten technischen Konzepte im Mobilitätssektor verglichen wurden.[217] Diese sollen den Rahmen für vorliegende Untersuchung bilden. Entsprechend der Zielsetzung vor allem die Aspekte des fairen und diskriminierungsfreien Wettbewerbs sowie der Interoperabilität von zentraler Bedeutung. Diese sollen im Folgenden bei der Bewertung im Einzelnen herangezogen und konkretisiert werden.

II. Auswirkungen des Vorschlags für ein Datengesetz auf Datenflüsse und Konzepte

Zunächst sollen die Kernpunkte des DA-E dargestellt und die Auswirkungen auf bestehende Datenflüsse und Konzepte analysiert werden.

1. Kernelemente des Datenzugangs im DA-E und Auswirkungen

a) Räumlicher Anwendungsbereich

In räumlicher Hinsicht ist der Anwendungsbereich nach Art. 1(2) DA-E ähnlich weit gefasst wie bei der DSGVO. Er erstreckt sich auf die Vermarktung von Produkten in der EU sowie Datenzugang für Empfänger sowie Dienstangebote an Kunden in der EU. So erscheint jedenfalls sichergestellt, dass auf dem EU-Markt gleiche Regeln herrschen.

b) Einschränkung auf Rohdaten

aa) Maschinendaten und DA-E

Im Ausgangspunkt wurde die dem DA-E vorausgehende Diskussion mit Bezug auf maschinengenerierte Daten („MGD") bzw. Maschinendaten geführt. Diese Diskussion wurde unter strikter Trennung und Ausblendung der Regelungen für den Schutz personenbezogener Daten geführt, insbesondere durch die DSGVO. Das Konzept der MGD bezieht sich auf die Art der Erzeugung der Daten, sodass auch personenbezogene Daten von der Regelung betroffen sein können, bei deren Bestimmung es inhaltlich auf den Personenbezug ankommt.

Zu beachten ist zunächst, dass der DA-E nicht alle Arten von Maschinendaten erfasst. Dazu zählen Daten, die ohne direkte und wirtschaftlich relevante menschliche Intervention aufgezeichnet, gesammelt oder generiert wurden, und zwar Informationen, die durch Sensoren aus Softwareprozessen

---

[215] C-IST-Initiative Directive 2010/40/EU; C-ITS Platform, Final Report, 2016, abrufbar unter https://transport.ec.europa.eu/system/files/2016-09/c-its-platform-final-report-january-2016.pdf.

[216] C-ITS Platform, Final Report, 2016, S. 75 f., abrufbar unter https://transport.ec.europa.eu/system/files/2016-09/c-its-platform-final-report-january-2016.pdf.

[217] TRL, Studie „Access to In-vehicle Data and Resources – Final Report" im Auftrag der EU-Kommission, 2017, abrufbar unter https://transport.ec.europa.eu/system/files/2016-09/c-its-platform-final-report-january-2016.pdf. Vgl. Dazu auch *Specht/Kerber*, Gutachten Projekt ABIDA, 2017, S. 174 f.

oder Maschinenoperationen oder direkt aus Computerprozessen, Anwendungen oder Diensten erlangt wurden. In einer IoT-Umgebung gehören zu den sensorgenerierten Daten solche über die Maschine selbst, solche aus der Beobachtung der Umgebung und solche, die durch Aggregierung und Verarbeitung der zuvor angeführten Daten erlangt wurden.[218]

Hinsichtlich der Eingrenzung von MGD ist nicht ganz klar, wie weit der zulässige Grad menschlicher Intervention gehen soll. Für das vorliegende Thema besonders von Bedeutung ist vor allem, dass in der Praxis in vielen Fällen der eigentliche Vorgang der Datengenerierung und eine unmittelbar damit verbundene erste Aufbereitung der Daten durch Kompression, Kodierung, Formatierung etc. (Datenaufbereitung, -vorbearbeitung) sich faktisch nicht voneinander trennen lassen.

Für den vom DA-E erfassten Bereich ist die in Art. 2(1) DA-E enthaltende Definition von Daten entscheidend, die auch mit Art. 2(1) Data Governance Act[219] und Art. 2(24) Digital Markets Act[220] identisch ist und sich für die Datengesetzgebung als Standard herauskristallisiert:

> *"jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material"*

Der sachliche Anwendungsbereich wird dann abgegrenzt durch Art. 1 DA-E, wonach das Gesetz Anwendung findet auf

> *„Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden".*[221]

Ein connected car und die damit verbundenen Dienste wäre davon eindeutig erfasst.

Eine wichtige Einschränkung ergibt sich dabei aus den Erwägungsgründen 14 und 17 des DA-E. Danach erstreckt sich der Anwendungsbereich nicht auf abgeleitete oder aggregierte Daten („aus den Daten abgeleitete und gefolgerte Informationen"). Ebenso sollen aus Softwareprozessen entstandene abgeleitete Daten ausgeschlossen sein. Damit ist ein wichtiger Teil der oben definierten MGD aus dem Anwendungsbereich herausgenommen worden.

Insoweit ergeben zwei wichtige Problembereiche hinsichtlich des Anwendungsbereichs: zum einen die mögliche Ausgrenzung von unmittelbar bearbeiteten generierten Daten, zum anderen der Ausschluss abgeleiteter und aggregierter Daten.

Von Bedeutung ist darüber hinaus noch eine dritte Einschränkung. Innerhalb der oben angeführten Definition von MGD liegen auch Daten, die durch interne Geschäftssysteme produziert wurden (CRM) und Daten enthalten zu Produkten, Logistik, Vertrieb etc. Weiterhin gehören dazu auch Daten aus der Interaktion mit dem Nutzer (Cookies, Webtracking etc. sowie aus der internetgestützten

---

[218] Zum Ganzen s. die Begleitstudie zum DA-E, *De Michiel u.a.*, Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022, S. 32 ff. Ähnlich Erwägungsgrund 14 DA-E: „Physische Produkte, die mittels ihrer Komponenten Daten über ihre Leistung, Nutzung oder Umgebung erlangen, erzeugen oder sammeln und die diese Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln können (häufig als Internet der Dinge bezeichnet), sollten unter diese Verordnung fallen.".

[219] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. L 152/1 v. 30.5.2022.

[220] Verordnung (EU) 2022/1925 vom 14. 9. 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. L 265/1 v. 12.10.2022.

[221] Vgl. insoweit auch Art. 2 DA-E:

´ 2. „Produkt" [bezeichnet] einen körperlichen beweglichen Gegenstand, der auch in einem unbeweglichen Gegenstand enthalten sein kann, Daten über seine Nutzung oder Umgebung erlangt, erzeugt oder sammelt und Daten über einen öffentlich zugänglichen elektronischen Kommunikationsdienst übermitteln kann und dessen Hauptfunktion nicht die Speicherung und Verarbeitung von Daten ist;

3. „verbundener Dienst" einen digitalen Dienst, einschließlich Software, der so in ein Produkt integriert oder so mit ihm verbunden ist, dass das Produkt ohne ihn eine seiner Funktionen nicht ausführen könnte;´

Kollaboration.[222] Diese Daten sind aber wohl vom DA-E erfasst, da dieser auch auf die bei der Nutzung eines verbundenen Dienstes erzeugten Daten Anwendung findet. Relevant wird dies vor allem für die interaktiven Dienste im Auto und die von diesen generierten Daten, etwa Infotainment und Entertainment. Hier geht also der Anwendungsbereich des DA-E scheinbar über das in Bezug auf menschliche Intervention restriktive Konzept der Maschinendaten hinaus. Allerdings nimmt Art 2(2) DA-E i.V.m. Erwägungsgrund 15 solche Produkte wieder aus, die in erster Linie dazu bestimmt sind, Inhalte anzuzeigen oder abzuspielen oder diese – unter anderem für die Nutzung durch einen Online-Dienst – aufzuzeichnen und zu übertragen. Insofern ist es denkbar, dass einzelne abgrenzbare Teile des Fahrzeugs und die von diesem erzeugten Nutzungsdaten wieder aus dem Anwendungsbereich herausfallen. Näher liegt es aber, das connected car als Ganzes zu betrachten und nicht einzelne Elemente, die etwa dem Infotainment dienen, auszugliedern.

bb) Folgerungen für die Datengenerierung im connected car

Die fehlende Berücksichtigung der Datenaufbereitung im ursprünglichen Entwurf des DA-E ist für dessen Anwendung auf die im Fahrzeug erzeugten internen und externen Daten unmittelbar relevant. Die technische Aufbereitung ist für die Weiterverarbeitung essentiell. Da häufig eine unmittelbare technische Bearbeitung der Rohdaten untrennbar mit dem Generierungsprozess verbunden ist, sollte dies eigentlich als einheitlicher Prozess gesehen und die erstbearbeiteten Rohdaten mit vom Anwendungsbereich umfasst sein. Diese Quelle von Unsicherheit wurde im zweiten Kompromisstext der tschechischen Präsidentschaft vom Oktober 2022 beseitigt, indem klargestellt wird, dass auch für die weitere Nutzung technisch „aufbereitete Daten“ mit umfasst sind, wobei nach Erwägungsgrund 14 dies weit interpretiert werden soll und dazu auch Metadaten sowie Daten gehören, die in ein übliches Format reformatiert wurden.[223] Der vierte Kompromisstext vom 24.1. 2023 enthält insofern eine weitere Klarstellung, als der Begriff der „Aufbereitung“ durch „preprocessed“ ersetzt wurde und damit noch treffender auf die hier angesprochen technische Aufbereitung abgestellt wird.[224]

Von noch größerer Bedeutung ist der Ausschluss abgeleiteter und aggregierter Daten, der eine der wesentlichen Lücken des DA-E darstellt. Als abgeleitet werden solche Daten angesehen, die durch Verarbeitung mit weiteren Daten zusätzlichen Wert erlangen, gefolgerte Daten entstehen durch den Einsatz statistischer Datenanalyse.[225] Aggregierte und abgeleitete Daten können für die Entstehung von innovativen Produkten und Dienstleistungen auf Sekundärmärkten sogar von größerer Bedeutung sein als Rohdaten, da häufig nur der Hersteller die wertsteigernden Prozesse durchführen kann.[226] Daher wird die entsprechende Eingrenzung des Anwendungsbereichs stark kritisiert.[227] Nicht zuletzt gilt dies auch für die Verwendung als Trainingsdaten für Künstliche Intelligenz (KI).

In Bezug zu der in den vorhergehenden Arbeitspaketen aufgeführten Datenerzeugung im connected car (vgl. Ziff. D.I) lässt sich allgemein sagen, dass die Aggregierung und Ableitung von Daten vor allem für das Angebot von Services von Bedeutung ist, obwohl diese eigentlich vom DA-E erfasst sind. Die gilt etwa für die Profilbildung als Teil der Analyse der Nutzung. Gleiches gilt beim Driver Monitoring,

---

[222] *Everis Benelux*, Study on data sharing between companies in Europe, carried out for the European Commission, Final Report, Brussels, 2018, abrufbar unter https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en.

[223] Proposal for a Data Act, Second Presidency compromise text, 21 Oct. 2022, 2022/0047 (COD), abrufbar unter https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.

[224] Eine eingehende Abgrenzung ist jetzt enthalten in Erwägungsgrund 14a des Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Fourth Presidency compromise text, 24.1.2023, abrufbar unter https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

[225] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 24.

[226] Vgl. das Beispiel bei *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 24.

[227] *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 6; *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 24 ff.; *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 85; *Geiregat*, The Data Act: Start of a New Era for Data Ownership?, 2022, Rn. 20.

aber auch für weitere Dienste, wie sie unter Ziff. D.III aufgeführt sind. Grundsätzlich lässt sich aber sagen, dass bei einer Aggregierung von Daten die Schwelle von der Datenerhebung zur Verarbeitung im Rahmen konkreter Dienste überschritten sein kann, welche dann auch vom Hersteller selbst angeboten werden können, aber schon dem Sekundärmarkt der abgeleiteten Dienste zuzuordnen wären. Die Bewertung wird auch dadurch schwieriger, dass in Zukunft die Abgrenzung von Primär- und Sekundärmarkt vor allem deswegen verschwimmen wird, weil viele Dienste zukünftig direkt ins connected car integriert sein werden und dann dort direkt vom Diensteanbieter angeboten werden können.

Eine Beschränkung des Anwendungsbereichs auf Rohdaten unter Ausschluss der Aggregierung bzw. Ableitung wäre nur insoweit sinnvoll, als man insoweit auch die Grenze zwischen Primär- und Sekundärmarkt für Daten ziehen könnte. Hier ließe sich argumentieren, dass die Verarbeitung von Daten für das Anbieten von Diensten im Sekundärmarkt durch den Hersteller im Wettbewerb zu anderen Dienstanbietern steht und diese nicht von den entsprechenden Bemühungen des Herstellers unfair profitieren sollen.[228]

In vielen Fällen ist aber schon die Aggregierung so untrennbar mit der Datengenerierung verbunden, dass eine Separierung technisch und wirtschaftlich problematisch ist.[229] Weiterhin zeigt der Trend zur herstellerseitigen Integration neuer Funktionen, dass ein Wettbewerb auf der Diensteebene durch die Kontrollmöglichkeiten des Herstellers erschwert wird, was die oben angeführte Grenzziehung von Rohdaten/Diensten in Frage stellt. Schließlich wird auch eine generelle Ausgrenzung aggregierter Daten den Besonderheiten der einzelnen Dienste nicht gerecht.[230] So ist für Predictive Maintenance (vgl. Ziff. D.III.2.e)) ein Echtzeitzugang zu den Rohdaten erforderlich, aber auch zu aggregierten Daten. Für Versicherungen sind die Daten zur Nutzungsintensität als Input relevant, die bereits auf einer Aggregierung und Weiterverarbeitung basieren. Damit erweist sich die Begrenzung auf Rohdaten im DA-E als relevante und zu starke Einschränkung für den notwendigen Datenzugang.[231]

Problematisch ist weiterhin der Ausschluss der weiteren Kategorien von MGD durch Art. 2(2) DA-E, insbesondere solcher, die sich aus der Interaktion mit dem Nutzer ergeben. Die Gefahr ist hier, dass dadurch auch Komponenten des Autos erfasst werden, die für die zukünftige Entwicklung zentrale Bedeutung haben. Sieht man im Rahmen von Entertainment das gesamte Interieur des Fahrzeugs als Human-Machine-Interface („HMI“), so könnte dies zu einem Ausschluss nach Art. 2(2) DA-E vom Anwendungsbereich führen.[232]

Im laufenden Gesetzgebungsprozess wurde nunmehr auch auf den letzten Punkt reagiert und im vierten Kompromissvorschlag vom Januar 2023[233] die Definition von Daten in Art. 2(1af) und Produkt in Art. 2(2) geändert und stärker auf die Funktionalitäten der Daten abgestellt. Danach sind nur noch wesentliche Modifizierungen der Daten ausgeschlossen sowie Daten über die Nutzung zum Zugang zu Anwendungen, Daten über die Aufzeichnung und das Darbieten von Inhalten und die Inhalte selbst.[234]

---

[228] Auch unabhängige Diensteanbieter haben in einem frühen Statement vor allem Bedarf an unverarbeiteten Rohdaten angemeldet, FIGIEFA, Commission Communication on “Free Flow of Data” - Input from the Independent Automotive Aftermarket, 2016, S. 13.

[229] S.a. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 24, wonach ein Zugang zu aggregierten Daten zur Erbringung weiterführender Dienste fast immer erforderlich ist.

[230] Vgl. auch ADAC e.V., Stellungnahme zum „Datengesetz“, 2022, S. 2.

[231] *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 30 f., wollen einen Zugang für aggregierte und abgeleitete Daten nur im Hinblick auf die Verwendung für Mehrwert schaffende Zwecke zulassen und daher nur für Art. 4 und 5 DA-E öffnen, dagegen Art. 3 DA-E auf die erste Enkodierung beschränken.

[232] Vgl. auch *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 58, der stattdessen für einen Ausschluss inhaltsbezogener Daten aus dem Datenbegriff des DA-E plädiert.

[233] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Fourth Presidency compromise text v. 24.1.2023, abrufbar unter https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

[234] Siehe Erwägungsgründe 14a und 15 des Fourth Presidency compromise text v. 24.1.2023, abrufbar unter https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

Daten, die automatisch durch Sensoren oder „embedded“ Anwendungen generiert werden, sollen eingeschlossen sein und zur weiteren Verwertung auf Sekundärmärkten zur Verfügung stehen. Daten hinsichtlich des Aufzeichnens oder der Darbietung von Inhalten und die Inhalte selbst sollen ausgeschlossen bleiben. Märkte für Software und Inhalte sollen insoweit nicht bedient werden. Es bleibt daher derzeit nur bei dem Ausschluss von aggregierten und abgeleiteten Daten.

c) Regeln über Datenzugang und Datenverwendung durch Nutzer und Dritte (Art. 3-12 DA-E).

aa) Überblick

Der DA-E etabliert Zugangsrechte, die im Rahmen vertraglicher Beziehungen zur Geltung gebracht werden. Der Entwurf geht von einem nutzerzentrierten Modell aus, dass die Zugangskontrolle im Kern dem Nutzer zuordnet. Dabei erfolgt eine Rollenverteilung auf Dateninhaber, Nutzer und Dritten vor, die das Bestehen vertraglicher Beziehungen voraussetzt und deren rechtliche Ausgestaltung in verschiedener Hinsicht in Art. 3-12 konkretisiert wird. Es gibt noch eine Reihe von Unklarheiten, so dass an einigen Stellen eine erste Auslegung erfolgen muss.

Als den Anwendungsbereich des DA-E faktisch weiter einschränkende Bedingung beschränken Art. 3 bis 5 DA-E i.d.F. des vierten Kompromisstextes[235] die Zugangsgewährung auf solche Daten, die „readily available“ sind. Letzteres wird konkretisiert in Art. 2 Nr. 1(ae) als solche Daten, die der Dateninhaber „ohne unverhältnismäßigen Aufwand“ erlangen kann, der über eine „einfache Operation“ hinausgehen würde. Das soll nach Erwägungsgrund 19 solche Daten ausschließen, die von Design her nicht dazu vorgesehen sind, gespeichert oder übertragen zu werden. Es ist unklar, inwieweit diese Einschränkung für den Datenzugang durch Drittanbieter relevant ist. Nahe liegt eine Interpretation, dass solche Daten, die der Hersteller selbst nicht weiter nutzt, auch nicht gesondert gespeichert werden sollen, nur um den Zugangsrechten des DA-E gerecht zu werden.

Den Hersteller trifft dann zunächst gem. Art. 3 DA-E die Verpflichtung, das Produkt von Werk aus so herzustellen, dass die vom Produkt oder einem verbundenen Dienst erzeugten Daten standardmäßig für den Nutzer direkt zugänglich sind, verbunden mit vorvertraglichen Informationspflichten. Soweit dies nicht erfolgt, sind die Daten gem. Art. 4(1) DA-E dem Nutzer vom Dateninhaber direkt und in Echtzeit zur Verfügung zu stellen, und auch auf elektronischem Wege, soweit machbar. Schließlich trifft den Dateninhaber gem. Art. 5(1) DA-E auch die Pflicht, auf Verlangen des Nutzers die Daten an Dritte weiterzugeben. Dies hat auch diskriminierungsfrei zu geschehen. Dafür kann der Dateninhaber nach Art. 9 DA-E eine angemessene Vergütung verlangen.

Der DA-E sieht für die verschiedenen Beteiligten Einschränkungen in der Nutzungsmöglichkeit hinsichtlich der erlangten Daten vor. Der Dateninhaber selbst ist in der Nutzung der Daten nach Art. 4(6) insoweit beschränkt, dass er die Daten nur im Rahmen einer vertraglichen Vereinbarung mit dem Nutzer verwenden darf. Er darf auch die Daten nicht dazu verwenden, um daraus Einblicke in die wirtschaftliche Lage, Vermögenswerte und Produktionsmethoden des Nutzers oder in die Nutzung durch den Nutzer sowie der entsprechenden Lage oder Nutzung des Dritten zu erlangen, wenn dies die gewerbliche Position des Nutzers oder des Dritten auf den Märkten, auf denen dieser tätig ist, untergraben könnte. Der Dritte kann nach Art. 5(5) einer solchen Nutzung zustimmen.

Der Nutzer darf nach Art. 4(4) die erlangten Daten nicht zur Entwicklung eines Produktes nutzen, das mit dem Produkt, von dem die Daten stammen, im Wettbewerb steht.

---

[235] Fourth Presidency compromise text, 24.1.2023, abrufbar unter https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

Der Dritte ist in der Verarbeitung der erlangten Daten in mehrfacher Hinsicht beschränkt. Er darf die bereitgestellten Daten nur für die Zwecke und unter den Bedingungen nutzen, die er mit dem Nutzer vereinbart hat. Daraus ergibt sich eines der Kernprobleme bei der Abgrenzung der Zugangsrechte nach dem DA-E. Die Zweckbestimmung obliegt allein den Parteien, die dies über den Kopf des Dateninhabers hinweg bestimmen können. Art. 6(2)(d) DA-E beschränkt dann die Bereitstellung für den Dritten aber auf solche Daten, die für die Erbringung des vom Nutzers bestimmten Dienstes erforderlich sind. Interessanterweise ist hier auch die Weitergabe von aggregierten und abgeleiteten Daten erfasst, die eigentlich vom Anwendungsbereich des DA-E ausgeklammert sind. Erwägungsgrund 28a gibt eine entsprechende Linie vor. Einerseits soll der Wettbewerb in Anschlussmärkten gefördert werden und daher auch eine Datenverwendung durch Dritte zur Entwicklung von Konkurrenzprodukten auf diesen Märkten im Interesse der Innovation gefördert werden. Andererseits sollen die Daten aber nicht zur Entwicklung von Konkurrenzprodukten auf dem Primärmarkt verwendet werden, was Art. 6(2)(e) entspricht.

Ergänzt werden die Einschränkungen für Dritte durch Art. 11(2) DA-E, wonach bei unerlaubter Nutzung eine Verpflichtung zur Löschung der Daten und zur Beendigung der Vermarktung von Produkten, abgeleiteten Daten und Diensten besteht, es sei denn, es ist kein erheblicher Schaden entstanden oder es wäre unverhältnismäßig.[236] Gleiches gilt bei Weitergabe an Dritte ohne die Genehmigung des Dateninhabers. Während danach die Zustimmung des Dateninhabers immer notwendig zu sein scheint, kann die Regelung im Zusammenspiel mit Art. 5 und 6 DA-E nur so interpretiert werden, dass sich der Dateninhaber gegen die zwischen Nutzer und Drittem vereinbarten Zwecke nicht sperren kann.

Andererseits stellt das Vertragserfordernis der Nutzung der Daten durch den Dateninhaber selbst nach Art. 4(6) DA-E eine erhebliche Einschränkung von dessen Verfügungsmacht über die Daten dar. Deren Bewertung hängt auch von der Umsetzbarkeit des grundlegenden Konzepts der Datensouveränität des Nutzers ab. Probleme können sich hier insbesondere für die Hersteller von Zulieferteilen ergeben, die gezwungen sein können, Daten zu liefern, die ihre Wettbewerbsposition auf deren Primärmarkt beeinträchtigen können. Ob Art. 6(2)(e) DA-E effektiv dagegen wirken kann, bleibt abzuwarten.

bb) Auswirkungen auf Datenflüsse und Geschäftsmodelle

(1) Rollenzuweisung

Um die Auswirkungen der Zugangsregeln näher bestimmen zu können, muss man die Rollenzuweisung näher beleuchten und dann auf die Situation bei connected cars anwenden. „Dateninhaber“ ist nach Art. 2 Nr. 6 eine juristische oder natürliche Person, die rechtlich verpflichtet ist oder bei Maschinendaten durch die Kontrolle über die technische Konzeption des Produktes und damit verbundener Dienste in der Lage ist, bestimmte Daten bereitzustellen.Die Definition scheint bei personenbezogenen Daten auf die Position des Verantwortlichen abzustellen, bei Maschinendaten auf die Kontrolle über die Konzeption des Produkts und damit die tatsächliche Möglichkeit zur Bereitstellung der Daten. Für das connected car scheint diese Definition nur auf den Hersteller zu passen. Dieser bestimmt die Konzeption des Fahrzeugs und der IT-Bestandteile und kontrolliert den Zugang zu den Daten.

„Nutzer“ ist nach Art. 2 Nr. 5 eine natürliche oder juristische Person, die ein Produkt besitzt, mietet oder least oder eine Dienstleistung in Anspruch nimmt. Als Nutzer gelten der Käufer, Leasingnehmer und Entleiher, auf der Basis eines „Rechtstitels“. Das kann der Halter sein. Aber auch der Fahrer ist gemeint,

[236] In Art. 11(2) des Second Presidency compromise text v. 21.10.2022 ist dies abgeändert in ein Recht des Dateninhabers, den Empfänger zu den entsprechenden Unterlassungs- und Beseitigungshandlungen aufzufordern; Art. 11(2a) erweitert diese Rechte teilweise auf die Nutzer, vgl. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.

da auch der Besitz und die Generierung von Daten durch Nutzung von Diensten in die Definition einbezogen ist und dies auch auf jeden Fahrer zutrifft.[237]

„Datenempfänger“ ist nach Art. 2 Nr. 7 eine juristische oder natürliche Person, die zu gewerblichen oder beruflichen Zwecken handelt, und der vom Dateninhaber Daten bereitgestellt werden, einschl. eines Dritten, dem auf Verlangen des Nutzers die Daten bereitgestellt werden.

Die Rollenverteilung scheint zunächst mit der Situation bei connected cars kompatibel. Die Bestimmung des Nutzers kann in Zukunft schwieriger werden, wenn etwa Mobility-on-demand zunimmt und es oft wechselnde Fahrer gibt (vgl. Ziff. D.III.2.b)). Erwägungsgrund 20 des vierten Kompromisstextes führt nunmehr die Möglichkeit des Anlegens separater Accounts für jeden Nutzer als mögliche Lösung an.[238] Die Zuordnung der Rolle des Dateninhabers kann sich dadurch verändern, dass zunehmend externe Dienste in das connected car integriert werden, bei denen die generierten Daten nicht im Auto gespeichert werden, sondern an die Diensteanbieter übermittelt werden. Dies könnte dazu führen, die Diensteanbieter als Dateninhaber anzusehen sind, sodass Nutzer und Dritte mit den Diensteanbietern in vertragliche Beziehungen hinsichtlich des Datenzugangs treten müssten statt mit dem Hersteller.

(2) Zugangsrechte für Nutzer und Dritte

Im Folgenden sollen die oben dargestellten Konzepte daraufhin untersucht werden, inwieweit sie mit den Zugangsregeln des DA-E kompatibel sind. Nicht ganz klar ist, wie die Default-Einstellung in Art. 3 DA-E für das connected car umzusetzen wären. Erwägungsgrund 19 des vierten Kompromisstextes führt dazu aus, dass keine Verpflichtung zum Einbau zusätzlicher Speicher für diesen Zweck begründet werden soll. Eine standardmäßige direkte Zugänglichkeit für den Nutzer wäre jedenfalls durch das Konzept des OTP gewährleistet, weil hier der Nutzer selbst die Kontrolle über die generierten Daten ausübt. Gleiches gilt für die Datenplattform nach dem Data Shared Server-Prinzip. Fraglich ist, ob dies auch für das extended-vehicle-Konzept und insbesondere das ADAXO-Konzept gilt, wenn der Zugang für den Nutzer generell freigeschaltet wird, auch wenn hier der Fahrzeughersteller die ausschließliche Kontrolle behält. Nach Erwägungsgrund 21 ist sowohl die Zugänglichkeit auf dem Produkt als auch remote umfasst.

Unklar ist das Verhältnis des Direktzugangs nach Art. 3 zu den Zugangsansprüchen nach Art. 4, 5 DA-E. Nach einer Interpretation sollen Art. 4 DA-E nur eingreifen, wenn ein Zugang nach Art. 3 gar nicht gewährt wird, vor allem aus technischen Gründen. Zum anderen kann man Art. 4 DA-E auf Situationen beziehen, wo kein Zugang on device, sondern nur remote gewährt wird.[239] Bei letzterem kann man wiederum unterscheiden, ob der Zugang über eine Schnittstelle im Auto gewährt wird oder Zugriff auf externe Server notwendig ist, was bei den extended vehicle-Konzepten der Fall zu sein scheint (anders OTP). Es lässt sich aber erwarten, dass auch bei diesen Konzepten ein Zugriff für den Nutzer direkt im Auto ermöglicht werden kann, der die Daten als „readily available“ wie durch Art. 3 gefordert, erscheinen lässt (Erwägungsgrund 21). Jedenfalls ist davon auszugehen, dass Art. 5 DA-E unabhängig davon eingreift, ob und in welcher Form der Zugriff nach Art. 3 DA-E gewährt wird.[240] Nur dann ist der Zweck der Ermöglichung des Zugriffs für Dritte gewahrt.

Was die Bereitstellung der Daten für Dritte angeht, so ermöglicht der DA-E sowohl die Weitergabe der vom Nutzer im Rahmen von Art. 3 oder 4 DA-E erlangten Daten an Dritte, als auch eine Zurverfügungstellung an Dritte auf Verlangen des Nutzers nach Art. 5 DA-E. Dies ist zunächst als

---

[237] Für eine engere Definition des Nutzers *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 59 f., die bloße Nutzer ohne Rechte am Auto ausgeschlossen sehen.

[238] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Fourth Presidency compromise text v. 24.1.2023, abrufbar unter https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

[239] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 79.

[240] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 80.

indirekter Zugang des Dritten auf Veranlassung des Nutzers konzipiert. Es sollte aber auch ein Zugangsverlangen des Dritten im Auftrag und mit Autorisierung des Nutzers einschließen, um weitere Transaktionskosten zu vermeiden.[241] Nach dem extended vehicle-Prinzip behält jedoch der Hersteller die vollständige Kontrolle über den Datenzugang.[242] Einige Hersteller eröffnen den Datenzugriff für Dritte über API-Schnittstellen, die aber nicht standardisiert sind. Hier ist offen, ob dies für die Erfüllung von Art. 5 DA-E ausreicht oder eine standardisierte Schnittstelle anzubieten ist. Für letzteres spricht, dass Art. 5 DA-E nun ein „allgemein gebräuchliches" Format vorschreibt.

In diesen Kontext gehört auch das Anbieten von Datenpaketen über Marktplätze wie BMW CarData oder Caruso. Problematisch ist insoweit, dass dabei die Daten nicht gezielt auf Veranlassung des Nutzers einem Dritten bereitgestellt werden. Sofern allerdings die Dritten Zugang zu dem Marktplatz bekommen und die angeforderten Daten dort bereitgestellt werden, sollte dies ausreichen, um die Anforderungen von Art. 5 DA-E zu erfüllen. Problematisch bleibt insoweit aber, dass der geforderte Echtzeitzugriff dadurch nicht gewährleistet ist.

Der bei ADAXO zugrunde gelegte Abschluss eines Vertrags zwischen Hersteller und Drittem entspricht der Vorstellung des DA-E, ebenso wie die Gewährung diskriminierungsfreien Zugangs zu allen Daten, die die Hersteller auch selbst nutzen. Hinzukommen muss ein Vertrag zwischen Nutzer und Drittem. Beim OTP-Konzept räumt der Nutzer selbst Dritten den Zugang ein, was eher in den Rahmen von Art. 4 DA-E passt. Gleiches gilt wohl auch für das Data Shared Server-Prinzip, wobei es keinen Unterschied macht, ob der Server unter Kontrolle eines Datentreuhänders steht.

(3) Art der Zugangsgewährung

Die Daten sind in einem gebräuchlichen maschinenlesbaren Format bereitzustellen. Außerdem soll der Zugang sicher und einfach sein, und die Datenqualität jedenfalls im Rahmen von Art. 4 DA-E möglichst gleichwertig sein.[243] Fraglich ist, ob im Rahmen von Art. 3 oder Art. 4,5 ein bloßer in-situ-Zugang in einer vom Hersteller kontrollierten Umgebung ausreichend ist. Hier enthält der DA-E etwas unterschiedliche Begrifflichkeiten.[244] Erwägungsgrund 21 lässt die Möglichkeit offen, die Daten auf einem Server des Herstellers zugänglich zu machen. Der vierte Kompromissvorschlag hat das um die Möglichkeit ergänzt, die Daten in einem IT-Umfeld zugänglich zu machen, das vom Nutzer oder dem Dritten ausgewählt wurde. Zur effektiven Erreichung des Zwecks erscheint nur eine Interpretation sinnvoll, die auch die Erlangung bzw. Übermittlung der Daten umfasst und eine Angleichung an die Datenportabilität nach Art. 20 DSGVO beinhaltet.[245] Ein in-situ-Zugang sollte auf Verlangen des Nutzers möglich sein, aber der Zugang nicht darauf begrenzt sein.

Nach Art. 4 und 5 DA-E sind die Daten „gegebenenfalls" in Echtzeit zur Verfügung zu stellen sind, Soweit die Daten vom Hersteller kontinuierlich und in Echtzeit gespeichert werden, ist auch ein entsprechender Zugang zu gewähren.[246] Beim extended vehicle-Konzept ebenso wie beim Data Shared Server-Konzept ist dies derzeit nicht der Fall. Nur beim OTP-Konzept wird derzeit diese Möglichkeit angeboten.

---

[241] Vgl. *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 14, der auf Art. 35, 36 der Zweiten ZahlungsdiensteRL 2015/2366 mit einer ähnlichen Regelung verweist.

[242] *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 16, weist darauf hin, dass auch die Regeln in Ch. III DA-E insgesamt im Einklang mit dem extended vehicle-Konzept stehen.

[243] Nach dem Fourth Presidency compromise text v. 24.1.2023 sind im Rahmen von Art. 4 und 5 DA-E die Daten bereitzustellen: "without undue delay, free of charge, easily, securely, in a structured, commonly used and machine-readable format and, where applicable, of the same quality as is available to the data holder, continuously and in real-time", vgl. https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

[244] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, 65.

[245] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 66; *Geiregat*, The Data Act: Start of a New Era for Data Ownership?, 2022, Rn. 21.

[246] *Geiregat*, The Data Act: Start of a New Era for Data Ownership?, 2022, Rn. 21.

Weiterhin wird in Bezug auf Art. 5, 6 DA-E die Gefahr gesehen, dass der Dateninhaber nach der derzeitigen Ausgestaltung über die Kontrolle der Datenströme Informationen erlangt, die ihm einen Wettbewerbsvorteil verschaffen (Business Monitoring). Dieses Problem wird durch den Ansatz des DA-E nicht gelöst. Hiernach behält der Dateninhaber grundsätzlich die technische Kontrolle über den Datenzugang, den er lediglich dem Nutzer bzw. dem Dritten gewähren muss. Jedenfalls kann der Hersteller bei der Zugangsgewährung über die eigenen Server im Rahmen des extended vehicle-Konzepts Informationen über die Geschäftstätigkeit der Nutzer und Dritte erlangen. Dies wäre beim Data Shared Server-Konzept sowie bei OTP anders. Gegen die aus dieser Gatekeeper-Position entstehenden Risiken sollen die Regelungen in Art. 4(6) und Art. 5(3)S. 2 und (5) DA-E über die zulässige Speicherung und Nichtverwendung solcher Informationen zu Wettbewerbszwecken schützen, auf die im Folgenden näher eingegangen wird. Ob dies angesichts der Nachweisprobleme ausreicht, erscheint zweifelhaft. Vorzugswürdig erscheint ein struktureller Ausschluss der Gatekeeper-Funktion.

(4) Weiterverwendung

(a) Nutzer

Die Verwendung der Daten durch den Nutzer nach Art. 3 und 4 DA-E unterliegt keinen ausdrücklichen Beschränkungen (Erwägungsgrund 28).[247]

(b) Dateninhaber

Hinsichtlich der Nutzung der Daten durch den Dateninhaber selbst ist die Regelung des Art. 4(6) DA-E problematisch. Sollte die Regelung bedeuten, dass jede Nutzung der Daten ohne Zustimmung des Nutzers ausgeschlossen wäre, würde das eine ernste Beschränkung für den Dateninhaber, aber auch für Dritte, an die der Dateninhaber die Daten ohne Veranlassung durch den Nutzer weitergibt, bedeuten. Damit wären marktbedingte Zugriffe durch dritte Diensteanbieter ohne „Umweg“ über den Nutzer erschwert.

Dies hätte auch Konsequenzen für die Ausgestaltung der entsprechenden Geschäftsmodelle. Es müsste sichergestellt werden, dass die Bereitstellung der Daten durch den Hersteller immer nur mit Zustimmung des Nutzers erfolgt. Dies ließe sich natürlich bei der Überlassung des Produkts vertraglich regeln. Wahrscheinlich ist, dass der Nutzer in diesem Fall in breitem Umfang der Nutzung durch den Dateninhaber zustimmen soll.[248] Es müsste sichergestellt werden, dass in jedem Fall ein Vertrag geschlossen wird, alle potenziellen Nutzer eingeschlossen sind und dieser Vertrag auch wirksam ist. Letzteres könnte etwa bei einer vorab abgegebenen breiten Einwilligung problematisch sein. Insoweit ist insbesondere die Erfüllung der vorvertraglichen Informationspflichten von Art. 3(2) DA-E von Bedeutung. Deren Verletzung kann u.a. nach § 3a UWG sowie §§ 5a Abs. 1, 5b Abs. 4 UWG sanktioniert werden. Weiterhin sind die AGB-Kontrolle gegenüber Verbrauchern sowie die Fairness-Regeln von Art. 13 DA-E für die AGB-Kontrolle im Verhältnis zwischen Unternehmen (B2B) von Bedeutung. Alternativ oder ergänzend könnten hier technische Datenmanagementsysteme eingesetzt werden, wie sie auch für das Datenschutzrecht diskutiert werden.[249]

---

[247] Kritisch dazu aus ökonomischer Sicht *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, S. 19, 40.

[248] *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 10; *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S.S. 20 f., *Specht-Riemenschneider*, MMR 2022, 809, 817, warnt vor einem „totalen Buy-Out“ des Nutzers.

[249] Zu verschiedenen Einwilligungstypen und der technischen Umsetzung eingehend *Stiemerling/Weiß/Wendehorst*, Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, 2021, abrufbar unter https://www.ecambria-experts.de/it-sachverstaendiger/wp-content/uploads/2022/01/211216-Gutachten_fuer_Bundesministerium_fuer_Wirtschaft_und_Energie_p-os37621.pdf. Vgl. ferner *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 29 ff.

Eine technische Implementierung der Zustimmung wäre hilfreich, um dem dritten Datenempfänger Rechtssicherheit zu verschaffen. Es können hier aber erhebliche Transaktionskosten entstehen, bis hin zu der Frage, welche Daten jeweils von welchem Nutzer generiert worden sind, was insbesondere bei häufigem Fahrerwechsel noch verschärft wird. Das Zustimmungserfordernis lässt sich nur schwer mit Erwägungsgrund 6 DA-E vereinbaren, wonach es sich bei den Zugangsrechten nicht um exklusive Rechte handelt.[250] Wegen der erheblichen Auswirkungen dieser Regelung auf die Bereitstellung von Daten sollte die Regelung in Art. 4(6) DA-E gestrichen werden.[251]

(c) Dritte

Die Regelung der Verwendungsmöglichkeiten der Daten durch den Dritten weist ebenfalls Unklarheiten auf. Zwar besteht nach Art. 6(1) eine Zweckbegrenzung durch die Vereinbarung mit dem Nutzer. Allerdings ist der Nutzer in der Verwendung der Daten frei, so dass er entsprechende breite Zweckverwendungen auch mit dem Dritten vereinbaren kann. Damit scheint auch die Kommerzialisierung der Daten, z.B. auf Datenplattformen, ohne weitere Zweckeingrenzung möglich. Der DA-E enthält vor allem Rahmenbedingungen für die weitere Verwendung durch den Dritten.

Das betrifft nach Art. 6(2)(c) DA-E die Weitergabe von Rohdaten, aggregierten und abgeleiteten Daten, die vom Dritten nur für den Dienst verwendet werden dürfen, den der Nutzer vorgegeben hat. Auch dürfen die Dritten nach Art. 6(2)(e) DA-E die Daten nicht zur Entwicklung eines Konkurrenzprodukts auf dem Primärmarkt nutzen oder zu diesem Zweck weitergeben. Damit ist im Ausgangspunkt die Weiterverwendung von Daten durch den Diensteanbieter auf die vereinbarten Zwecke beschränkt, was eine Benachteiligung gegenüber dem Dateninhaber begründen kann, der sich vom Nutzer eine breite Zustimmung vertraglich einholen kann.[252].

Diese Verpflichtungen gelten aber vom Wortlaut her nur für eine Zugänglichmachung nach Art. 5 DA-E, sodass bei Weitergabe durch den Nutzer selbst die Beschränkungen von Art. 6 nicht zu greifen scheinen. Dies Verständnis wäre aber problematisch, da es von der jeweiligen technischen Ausgestaltung abhängen würde, ob die Daten dem Dritten direkt vom Nutzer oder vom Dateninhaber nach Art. 5 bereitgestellt werden. Auch entstehen Probleme entlang der Wertschöpfungskette, wenn der Ursprung der Daten nicht mehr geklärt werden kann.

Das gilt insbesondere bei der Verwertung der Daten auf Datenmärkten. Hier wäre eine Klarstellung sinnvoll. Man könnte das Weitergabeverbot von Art. 6(2)(c) DA-E um eine Ausnahme für Weitergabe an Danteintermediäre nach dem DGS erweitern.[253] Erwägungsgrund 28a idF des vierten Kompromisstextes nennt als Zweck des DA-E die Überwindung des „vendor lock-in“ und die Förderung von Wettbewerb und Innovation auf den Folgemärkten. Das schließt auch die Entwicklung völlig neuartiger Dienste unter Nutzung der Daten ein, was auf eine Verwendungsmöglichkeit auch im Rahmen einer zweckfreien Datenweitergabe hindeutet, einschließlich des Verkaufs auf Datenmärkten.[254] Dann wäre aber eine Zweckbindung nicht mehr sinnvoll und auch nicht kontrollierbar.

Es stellt sich insoweit auch im Rahmen von Art. 5 DA-E die Frage, wie eine mögliche Zweckbindung der Daten überwacht und durchgesetzt werden kann. Diese Aufgabe ist nach dem DA-E der vertraglichen Beziehung zwischen Nutzer und Drittem überlassen. Allerdings regelt Art. 8 DA-E auch die Datenherausgabe nach Art. 5 DA-E an den Dritten im Rahmen eines B2B-Vertrages. Erwägungsgrund 38 hebt aber gleichzeitig hervor, dass ein Vertrag nicht zwingend notwendig sei,

---

[250] Für Einordnung als gesetzlicher Zugangsverpflichtung *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 44.

[251] So auch *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 53 f.

[252] *Graef/Husovec*, Seven Things to Improve in the Data Act, 2022, S. 2, weisen auch auf die Gefahr hin, dass Nutzer und Dritte durch falsche Behauptungen Herkunft der Daten von einem Dienst im Sekundärmarkt der wettbewerblichen Verwendung von der Verwendung der Daten abgehalten werden.

[253] *Schweitzer u.a.*, Data access and sharing in Germany and in the EU, Final Report, 2022, S. 299.

[254] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 15 f.

sondern das Zugangsrecht auch isoliert vor nationalen Gerichten eingeklagt werden kann. Die Durchsetzung der Maßnahmen bei Pflichtverletzung des Dritten nach Art. 11(2) DA-E obliegt auch primär dem Dateninhaber. Die durch den vierten Kompromisstext eingefügte Berechtigung des Nutzers, gegen den Dritten vorzugehen, beschränkt sich auf die Verletzung von Art. 6(2)(a) und (b) DA-E.

Von besonderer Bedeutung ist der ausdrückliche Bezug auf die FRAND-Bedingungen in Art. 8(1) i.V.m. Erwägungsgrund 38 DA-E, wo auch auf die nicht bindenden Modellverträge verwiesen wird, die im Auftrag der EU-Kommission entwickelt werden sollen. Die Einhaltung der Bedingungen von Fairness, Nichtdiskriminierung und Transparenz ist ein wesentliches Element einer wettbewerbsfördernden Gestaltung der Zugangsrechte.[255]

Die Regeln zur Weiterverwendung im DA-E scheinen grundsätzlich mit den bestehenden Geschäftsmodellen und Konzepten im Mobilitätssektor kompatibel zu sein. Allerdings wäre eine Interpretation von Art. 4(6) DA-E, welche die eigene Datenverwendung des Herstellers von der Zustimmung des Nutzers abhängig macht, zumindest mit den extended-vehicle-Konzepten nur schwer zu vereinbaren. Entsprechende vertragliche Regelungen wären dann in ihrer Wirksamkeit nicht unproblematisch, vor allem wenn sie dem Dateninhaber völlige Freiheit bei der Verwendung lassen. Hier könnte eine AGB-Kontrolle zur Annahme einer unangemessenen Benachteiligung wegen Abweichens vom nutzerzentrierten Modell des DA-E führen.

Der Kern einer möglichen Unverträglichkeit mit bestehenden Konzepten liegt aber darin, dass der Nutzer die Zwecke von Zugang und Weiterverwendung frei bestimmen kann. Dies ist schon im Ansatz nicht mit dem extended-vehicle-Konzept vereinbar. Das gilt in gleicher Weise für neue Konzepte wie Catena-X und Mobility Data Space, bei denen ebenfalls der Fahrzeughersteller die Kontrolle behält. Sollte die Interpretation vertretbar sein, dass der Nutzer frei ist in der Zweckbestimmung, so würde dies bedeuten, dass der Hersteller die Kontrolle über den Adressaten und den Umfang der Weitergabe der Daten insoweit verliert und diese durch den Nutzer ausgeübt wird. Es bliebe ein Restbestand an technischer Kontrolle, das Kernelement der Zugangskontrolle durch den Hersteller ginge aber verloren. Auch die im Rahmen von ADAXO eingeführte teilweise Nutzerbeteiligung ändert an der Beibehaltung der Kontrolle durch den Hersteller nichts.

Dies ändert sich, wenn man bei den sich entwickelnden Datenmärkten wie Catena-X und MobilityDataSpace auch den Nutzer einbeziehen würde, so dass dieser die von ihm generierten Daten dort verwerten und insoweit auch die Bedingungen bestimmen könnte. Dabei könnten Datenintermediäre im Auftrag des Nutzers aktiv werden, wie es auch Erwägungsgrund 29 des vierten Kompromisstextes zum DA-E ausdrücklich anführt. Auch dafür wäre eine Klarstellung wichtig, ob der Nutzer in der Zweckbestimmung frei ist und damit auch die Daten für multiple Zwecke weitergeben kann.

Für die Konzepte von OTP und Data Shared Server bestünde insoweit kein Problem, da bei diesen die Kontrolle bereits durch den Nutzer ausgeübt wird. Aufgrund der direkten Kontrolle der Nutzer im Rahmen von OTP sowie Shared Server müsste man allerdings diese dann in der Rolle des Dateninhabers sehen, was dazu führen würde, dass die gesamte Rollenverteilung des DA-E nicht mehr passen würde. Der Zweck des DA-E würde aber durch die direkte Kontrollmöglichkeit des Nutzers erfüllt. Alternativ könnte man dann einen Fall von Art. 3 DA-E sehen, nämlich der direkten Zugänglichkeit der Daten für den Nutzer.

[255] Zu den Problemen bei der Umsetzung vgl. *Ducuing/Margoni/Schirru*, White Paper on the Data Act Proposal, CiTiP Working Paper 2022, 26 October 2022, S. 35, abrufbar unter .https://openfuture.eu/wp-content/uploads/2022/10/CiTiP_WhitePaperDataAct.pdf.

2. Erste Bewertung des DA-E und seiner Folgewirkungen

a) Zugang zu Daten und Ressourcen/Funktionen

Um die Ziele von Wettbewerb und Innovation im Bereich der connected cars zu erreichen, ist ein offenes System mit dem zentralen Merkmal des „access to in-vehicle data and resources“ erforderlich.[256] Der Zugang zu Daten und derjenige zu Funktionen und Ressourcen sind getrennt zu betrachten. Bei letzterem geht es um den Zugang zum IT-System des Fahrzeugs, um Daten herunterzuladen (Lesezugriff) oder Daten hochzuladen oder Dienste im Fahrzeug anzubieten (Schreibzugriff). Angesichts der unter Ziff. D.III dargestellten Ausgestaltung der Dienste ist auch ein Angebot direkt im Fahrzeug notwendig, etwa functions-on-demand oder Infotainment. Ergänzend ist dazu ein Zugriff auf die Benutzerschnittstelle im Auto („HMI“) notwendig, um die direkte Kommunikation zwischen Dienst und Nutzer zu ermöglichen.[257]

Im Hinblick auf den Datenzugang ist die Verankerung des Nutzers und indirekt auch Dritter unter FRAND-Bedingungen ein wichtiger Baustein. Von Bedeutung ist auch, dass nach Art. 4 und 5 DA-E der Hersteller alle Daten zur Verfügung stellen muss, die ihm ohne weiteres verfügbar sind. Dies schließt auch solche Daten ein, die der Hersteller nicht selbst auf dem Sekundärmarkt nutzt, die aber für die Entwicklung weiterer innovativer Leistungen essentiell sein können.

Viele Dienste auf dem Sekundärmarkt bedürfen eines Zugriffs auf die Rohdaten, was durch den DA-E jetzt vorgesehen ist. Problematisch bleibt der Ausschluss aggregierter bzw. abgeleiteter Daten vom Anwendungsbereich des DA-E, was dazu führen kann, dass bestimmte komplementäre Dienste nicht betrieben werden können. Dies ist auch im Hinblick auf KI-Einsatz von Bedeutung. Die Gewährung eines Echtzeitzugangs ist für den Datenzugang essentiell, aber auch hier ist die Regelung im DA-E zu unklar, wann dieser zu gewähren ist. Gleiches gilt einerseits für die Frage, ob eine Begrenzung auf einen in-situ-Zugang nach dem DA-E zulässig ist, andererseits ist fraglich, ob dies für einen effektiven Datenzugang ausreichend ist. Mit der Zuweisung der rechtlichen Kontrolle über den Datenzugang für Dritte an den Nutzer wird ein wesentliches Merkmal der Datenkontrolle der Fahrzeughersteller aufgebrochen. Die Frage, inwieweit die vom Nutzer zu bestimmenden Zwecke begrenzt sind, ist aber noch nicht endgültig geklärt.

Die unklare Reichweite möglicher Zwecke der Datenverwendung erzeugt auch Unsicherheiten hinsichtlich der Weiterverwendung der Daten. Sollte auch die Kommerzialisierung auf Datenmärkten durch den Nutzer und/oder den Dritten zulässig sein, so würde dies einen freien Datenzugang aller Beteiligten auf dem abgeleiteten Markt zur Folge haben, der im Sinne des Wettbewerbs positiv zu bewerten wäre.[258] Sollte nach dem Wortlaut von Art. 4(6) DA-E auch der Hersteller selbst eine Zustimmung des Nutzers zur Verwertung der Daten benötigen, so wäre in Bezug auf den Datenzugang ein vollständiges Level-Playing-Field aller Beteiligten auf Sekundärmärkten hergestellt. Einschränkungen bestünden dann nur für die Nutzung der Daten zur Erstellung von Konkurrenzprodukten auf dem Primärmarkt.

Der DA-E erfasst aber nur den ersten Aspekt des Datenzugangs. Der zweite Aspekt des Zugangs zu Ressourcen und Funktionen erfordert einen Schreibzugriff, um Daten hochzuladen und Funktionen

---

[256] *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 5, und *Kerber*, 2019 Journal of Competition Law & Economics, 381, 390, diskutiert auch die Frage, ob statt offener Systeme ein Wettbewerb der geschlossenen Systeme positive Ergebnisse bringen kann, lehnt dies aber wegen der Langlebigkeit der Fahrzeuge und der Komplexität der Produkte mit hohen Wechselkosten für die Nutzer ab.

[257] Vgl. zum Ganzen TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 75 ff.; *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 7 ff.; *Kerber*, 2019 Journal of Competition Law & Economics, 381 Fn. 27.

[258] Zu Netzwerkeffekten und economies of scope auf Datenplattformen, die auch durch markenübergreifende Aggregierung von Daten entstehen können, *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 22.

direkt im Auto anzubieten. Weiterhin ist für verschiedene Dienste der direkte Kommunikationskanal zum Nutzer essentiell, durch Zugriff auf die Benutzerschnittstelle (HMI).[259] Diese Frage wird vom DA-E nicht geregelt, und damit ist ein wichtiger Teil des Zugangs zum Angebot von ergänzenden und abgeleiteten Diensten nicht erfasst. Auf diese Weise behielte der Fahrzeugersteller eine wichtige faktische Position, um in bestimmten Fällen den Wettbewerb von Diensten zu behindern, vor allem wenn dieser einen direkten Zugang zu den Funktionen und Ressourcen des Fahrzeugs voraussetzen. Ergänzt wird das Problem durch die sich aus der verbleibenden Gatekeeper-Position der Hersteller ergebende faktische Möglichkeit, Daten über die Zugriffe der Wettbewerber zu erfassen (Business Monitoring) und strategisch zu nutzen, auch wenn dies rechtlich durch den DA-E untersagt wird.

Die zuletzt angesprochene Problematik stellt sich insbesondere, wenn der Hersteller ebenfalls im Sekundärmarkt aktiv ist und damit zugleich Wettbewerber ist. Dies ermöglicht Bundling-Strategien. Der DA-E schützt zwar den Primärmarkt vor Datennutzung aus dem Sekundärmarkt, nicht aber den Sekundärmarkt für Datennutzung durch Wettbewerb im Primärmarkt. Ein möglicher Weg zur Vermeidung der Gatekeeper-Problematik unter gleichzeitiger Herstellung von IT-Sicherheit ist die Funktionstrennung („separation of duties").[260] Dies lässt sich etwa beim Ferndiagnosezugriff dadurch verwirklichen, dass die Funktionen von Zugriff zum Fahrzeug durch den Hersteller, Identifikation des Eigentümers und Autorisierung des Dienstezugriffs getrennt werden und die letzten beiden durch einen Treuhänder übernommen werden.[261]

Ein Sonderproblem besteht in Bezug auf die Datenabhängigkeit von Komponentenherstellern von den Fahrzeugherstellern upstream, also in der Lieferkette aufwärts. Erstere haben ein großes Interesse am Zugang zu Daten über die Performanz der Komponenten, wenn sie im Auto eingebaut sind. Diese Daten liegen beim Hersteller als Dateninhaber. Jedoch passen die Komponentenhersteller nicht in das Rollenschema des DA-E. Man kann sie zwar als Drittanbieter ansehen, das Konzept des DA-E stellt insoweit aber auf den Sekundärmarkt ab und entsprechende Dienste für den Nutzer. Der Komponentenhersteller bedient aber den Primärmarkt mit Produktteilen. Insofern liegt diese Problematik allein im Bereich vertraglicher Vereinbarungen. Wegen möglicher wirtschaftlicher Ungleichgewichte ist aber nicht sichergestellt, dass die Komponentenhersteller hinreichend mit Daten versorgt wird. Auch diese stehen im Wettbewerb, und der Hersteller kann diesen Wettbewerb durch entsprechende Vertragsgestaltung stark behindern. Daher wäre auch insoweit an eine eigenes Zugangsrecht der Komponentenhersteller zu denken, wobei allerdings weitere ökonomische Forschung über die Situation in dem Bereich und die Auswirkungen von Datenzugangsrechten notwendig erscheinen.[262]

Insgesamt wird der DA-E die Datenströme insoweit verändern, als die Kontrolle auf den Nutzer verlagert wird. Allerdings muss man unterscheiden zwischen der rechtlichen und der technisch-strukturellen Zugangskontrolle. Letztere verbleibt beim Hersteller. Daraus ergibt sich zum einen, dass wegen der Rolle des Nutzers eine Inkompatibilität mit den Konzepten des extended vehicle besteht. Wegen der verbleibenden technischen Kontrolle durch den Hersteller und den sich daraus ergebenden Möglichkeiten des Business Monitoring besteht andererseits eine Unverträglichkeit mit den Konzepten von OTP und Data Shared Server.

---

[259] Zur Bedeutung der HMI für den Wettbewerb *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 25.

[260] Vgl. etwa Aftermarket Alliance, Creating a level playing field for vehicle data access: Secure on-board Telematics Platform Approach, 2021, https://www.fiaregion1.com/wp-content/uploads/2021/03/2021-02-S-OTP-Paper-vFin.pdf, S. 32 f.

[261] Vgl. etwa Stellungnahme des ADAC e.V. zum Vorschlag für ein „Datengesetz" aus 05/2022, S. 4, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf,

[262] Vgl. auch *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 37; Gill, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 12.

b) Interoperabilität

Technische Standardisierung und Interoperabilität sind essentiell für Wettbewerb in digitalen Ökosystemen. Der Aspekt der Interoperabilität lässt sich unterteilen in datenbezogene Interoperabilität, die Datenportabilität und Protokollinteroperabilität beinhaltet und Voraussetzung für Datenzugang und Datenteilen ist, und „voller Protokollinteroperabilität", die es ermöglicht, dass unabhängige Diensteanbieter mit dem IT-System des Fahrzeugs interagieren können.[263] Die aufgezeigte Zweiteilung in Daten und Ressourcen zeigt sich auch hier.

Anforderungen an die Interoperabilität sind in den Zugangsregeln nicht spezifisch enthalten. Die in Art. 3 bis 5 DA-E enthaltenen Anforderungen an das Format der Datenbereitstellung beinhaltet eine gewisse Standardisierungsnotwendigkeit im Hinblick auf Datenportabilität und Protokollinteroperabilität. Allerdings wird zu Recht kritisiert, dass keine weitergehenden Anforderungen zur Förderung von Standardisierung und Interoperabilität einbezogen wurden.[264] Art. 28 DA-E sieht entsprechende Regelungen hinsichtlich Interoperabilität für die Betreiber von Datenräumen vor. Dies kann für die Hersteller im Rahmen eines Common European Mobility Data Space relevant werden. Für die Erreichung der Ziele des DA ist die Interoperabilität unerlässlich und sollte daher regulatorisch stärker berücksichtigt werden. Dies sollte auch die oben angesprochene volle Protokollinteroperabilität umfassen, auch wenn diese wesentlich schwerer zu erreichen ist.[265]

c) Probleme des nutzerzentrierten Ansatzes des DA-E

Allgemein erscheint das Modell des DA-E unterkomplex, und es ist fraglich, ob es den komplexen und differenzierten Datenflüssen im Mobilitätssektor gerecht werden kann.[266] Positiv sind die Anforderungen an die Transparenz hinsichtlich der verfügbaren Daten, deren Zugänglichkeit für die Nutzer und die Einbeziehung von FRAND-Bedingungen zu sehen.[267] Grundsätzlich problematisch ist aber das nutzerzentrierte Modell, das von einer effektiven Vermarktung der Daten durch die Nutzer ausgeht, um Innovation auf Sekundärmärkten zu fördern, bei gleichzeitiger Beibehaltung der Datenkontrolle beim Dateninhaber. Gegen dessen Funktionieren sprechen Motivation und tatsächliche Verwertungsmöglichkeiten des Nutzers, die durch Transaktionskosten und Informationsasymmetrien eingeschränkt sein können. Weiterhin erscheint die Verhandlungsposition des Nutzers nicht stark genug, auch wenn Art. 13 DA-E dem im Bereich von B2B entgegenwirken sollen. Für den Nutzer als Verbraucher greift das bestehende AGB-Recht ein. Aufgrund der zentralen Rolle der Nutzer sowie der Notwendigkeit eingehender vertraglicher Regelungen entstehen hohe Transaktionskosten für den Nutzer, aber auch für die anderen Beteiligten, welche die Funktionsweise des Modells stark beeinträchtigen können.[268] Die Notwendigkeit individueller Verträge zwischen den Beteiligten stärkt die Position des Dateninhabers. Denkbar ist beispielsweise auch, dass unabhängige Dienste den Nutzer für den Erhalt der Daten entschädigen müssen, während die Hersteller diese Kosten bei Tätigkeit auf dem Sekundärmarkt nicht haben.[269] Allerdings setzt Art. 9 insoweit einen detaillierten Rahmen für die Bestimmung der Angemessenheit von Vergütungen, ergänzt um zu erarbeitende Richtlinien von Seiten der EU-Kommission.

---

[263] *Cremer/de Montjoye/Schweitzer*, Competition Policy for the Digital Era, 2019, S. 83 ff.
[264] *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 13.
[265] Vgl. *Cremer/de Montjoye/Schweitzer*, Competition Policy for the Digital Era, 2019, S. 83 ff.
[266] Von Herstellerseite wurde in den Stellungahmen eher eine ablehnende Haltung eingenommen und auf die resultierende Unsicherheit, die Vorteile freiwilligen Datenteilens und die Notwendigkeit der Amortisation der Investitionen verwiesen, vgl. FIGIEFA, 2022; BDI, EU-Data-Act, 2022. Demgegenüber geht den unabhängigen Diensteanbietern der DA-E nicht weit genug, und sie fordern ergänzende sektorspezifische Regelungen, vgl. zum Ganzen *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, 6 f., m.w.N.
[267] Vgl. auch *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 24.
[268] Vgl. *Kerber/Gilll*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 10.
[269] Vgl. *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 13.

Die Schwäche des Ansatzes könnte sich dann relativieren, wenn der Nutzer direkten Zugang zu Datenmärkten wie Catena-X und MobilityDataSpace erhält und die Bedingungen selbst bestimmen kann. Das könnte die Transaktionskosten senken und die Verwertung und Aggregierung der Daten erleichtern, gleichzeitig die Kontrolle der Hersteller reduzieren. Man käme dann der tatsächlichen Implementierung des Modells des DA-E näher. Weiterhin wäre an eine zentrale Rolle für Datenintermediäre zu denken, deren Tätigkeit durch Art. 9 ff. des Data Governance Acts[270] gestärkt werden soll. Auch hier ist aber zu beachten, dass diese nicht neue Monopolstellungen aufbauen, wobei hier ein Anwendungsfeld für das Kartellrecht mit den neuen spezifisch datenbezogenen Regelungen besteht, aber auch für den Digital Markets Act.[271]

Trotzdem wäre angesichts der Schwächen ein direkter Datenzugang der dritten Diensteanbieter vorzuziehen, den diese direkt gegenüber den Dateninhabern geltend machen könnten.[272] Soweit Hersteller weiterhin frei in der eigenen Verwertung sein sollten, kann hier der Markt für einen Interessenausgleich sorgen.[273]

Letztendlich kann der DA-E zwar dazu führen, dass dem Nutzer stärkere Kontrolle über den Datenzugang zu gewähren ist, und Der DA-E damit im Ansatz geeignet ist, die in den Strukturen vor allem des extended vehicle-Konzepts angelegte Kontrolle des Herstellers zu einem gewissen Grade aufzubrechen.[274] Die aufgeführten Defizite können aber dazu führen, dass das Modell nicht so funktioniert wie beabsichtigt und damit auch die erstrebten Wirkungen des Datenzugangs für Wettbewerb und Innovation auf nachgelagerten Märkte nicht wie beabsichtigt erreichbar erscheinen.[275]

3. Sicherung von Betriebs- und Geschäftsgeheimnissen gegenüber Zugangsrechten

Der Schutz von Betriebs- und Geschäftsgeheimnissen spielt für die Data Governance allgemein und die Datenzugangsrechte im Besonderen eine wichtige Rolle und begründet ein zu berücksichtigendes Gegeninteresse vor allem der Hersteller gegen den Datenzugang. Ziel der Datenzugangsrechte ist das Aufbrechen der faktischen Kontrolle von Unternehmen über Daten, deren Zugang für Wettbewerb und Innovation von Bedeutung sind. Darunter können auch vertrauliche Informationen der unterschiedlichsten Art sein. Das können zum einen bereits bestehende Geheimnisse mit geschäftlichen Informationen oder Informationen über technische Aspekte und Verfahren sein, die in den Datensätzen enthalten oder daraus erschließbar sind. Zum anderen können die maschinengenerierten Daten selbst geschützte Betriebs- und Geschäftsgeheimnisse darstellen.

Dies kann bereits für einzelne Datensätze der Fall sein. Hier ist auf das Potenzial abzustellen, das für Datenanalyse bereits im Hinblick auf einzelne Datensätze bestehen kann, die dann mit anderen Daten zur Analyse herangezogen werden, aber durch die Nichtoffenkundigkeit auch wirtschaftlichen Wert erlangen. Das Potenzial steigt mit dem Einsatz von Aggregierung und Datenanalyse entlang der Wertschöpfungskette in Bezug auf die daraus resultierenden Datensätze.[276] Neben der Nichtoffenkundigkeit müssen auch die weiteren Voraussetzungen des Geheimnisschutzes erfüllt sein. Dies ist auch für maschinengenerierte Daten grundsätzlich möglich.[277] Der Geheimnisinhaber muss organisatorische, vertragliche und technische Instrumente zum Schutz der Nichtoffenkundigkeit

[270] Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. L 152/1 v. 30.5.2022.
[271] Vgl. etwa *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. S. 29.
[272] So in der Tat die Forderung von AFCAR, The Data Act – Analysis from the perspective of the Automotive Aftermarket & Mobility Services Sector AFCAR Position paper, 9th May 2022, S. 5.
[273] Vgl. auch *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 33, 35.
[274] *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 9 f., sieht in der Ausgestaltung eher eine Stärkung der Position des Herstellers und eine rechtliche Anerkennung dessen faktischer Kontrollposition.
[275] Skeptisch auch *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. S. 13 ff.; s.a. *Kerber*, 2019 Journal of Competition Law & Economics 381, 390 ff.
[276] Vgl. *Drexl*, Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation BEUC, 2018, S. 94.
[277] Vgl. eingehend dazu *Wiebe*, GRUR 2023, 227 ff.

einsetzen. In technischer Hinsicht kommt Verschlüsselungstechniken eine besondere Bedeutung zu, die heute eine Übermittlung von Daten ermöglichen, ohne dass auf dem Transportweg Zugriff auf den Inhalt möglich ist.[278]

Mit dem Ansatz der Gewährung von Zugangsrechten durch den DA-E sind Konflikte mit dem Geheimnisschutz vorprogrammiert. Von großer Bedeutung für die Effektivität der Zugangsrechte, ist, dass der DA-E einen grundsätzlichen Vorrang der Zugangsrechte begründet, da sonst die Zugangsrechte durch die Geltendmachung von Geheimnisschutz auch in den Fällen ausgehebelt werden könnten, in denen dieser gar nicht besteht. Forderungen der Industrie nach einer gänzlichen Herausnahme von Geheimnissen aus den Zugangsrechten sind daher unrealistisch und im Übrigen wegen der davon ausgehenden Anreizwirkung auch nicht sinnvoll.

Das Problem könnte sich relativieren dadurch, dass aggregierte und abgeleitete Daten aus dem Anwendungsbereich des DA-E ausgeschlossen sind und damit ein wichtiger Bereich des Geheimnisschutzes den Zugangsrechten nicht unterworfen wird. Hier bleiben aber die bereits angesprochenen Probleme der Abgrenzung gegenüber Rohdaten, vor allem in praktischer Hinsicht. Weiterhin würde das Problem wieder virulent, wenn die entsprechenden Datensätze – wie hier befürwortet - wieder in den Anwendungsbereich einbezogen würden.

Der DA-E versucht, diesen Vorrang abzumildern durch ein größtmögliches Maß an Maßnahmen zur Erhaltung des Geheimnisschutzes. Die vom DA-E eingezogenen Sicherheitslinien sind zum einen in Art. 4(3) DA-E enthalten, wonach ein Zugang zu Geheimnissen nur dann gewährt werden soll, wenn zuvor alle notwendigen Maßnahmen zu deren Schutz getroffen worden sind. Der Kompromisstext vom Oktober 2022 erweiterte diese Pflicht auf Dateninhaber und Nutzer.[279] Soweit diese Maßnahmen nicht ausreichen, sollen Dateninhaber und Nutzer sich auf weitere Schutzmaßnahmen verständigen, insbesondere gegenüber Dritten. Dies dürfte auch den Fall abdecken, dass der Nutzer vom Dateninhaber erlangte Daten direkt an Dritte weitergibt. Der vierte Kompromisstext vom Januar 2023 flankiert dies in Art. 4(4) DA-E dadurch, dass die Weitergabe durch den Nutzer an Dritte zur Entwicklung eines Konkurrenzprodukts ausgeschlossen sein soll.[280] Auch kann der Dateninhaber nach Erwägungsgrund 28a verlangen, dass Nutzer und von ihm benannte Dritte die Vertraulichkeit bei der Offenlegung sicherstellen.

Kernelemente des Geheimnisschutzes sind die Schutzmaßnahmen, die der Dateninhaber und der Dritte vertraglich vereinbaren, worauf auch Art. 5(8) DA-E Bezug nimmt.[281] In der Fassung des vierten Kompromisstexts kann der Dateninhaber nachweisen, dass die vereinbarten Maßnahmen nicht ausreichen, und weitere Schutzmaßnahmen vom Dritten verlangen. Weiterhin wird die Offenlegungspflicht gegenüber Dritten nach Art. 5(8) DA-E strikt auf den Zweck begrenzt. Auch begrenzen die Verpflichtungen des Nutzers aus Art. 4(4) DA-E und sowie des Dritten aus Art. 6 DA-E die Verwertung der so erlangten Informationen.[282] Interessanterweise umfasst das Verbot der Weitergabe an Dritte nach Art. 6(2)(c) DA-E auch aggregierte und abgeleitete Daten. Art. 11 und 11(2)(a) DA-E in der Fassung des vierten Kompromisstextes fügen noch eine ausdrückliche Haftung

---

[278] Vgl. *Wiebe/Schur*, Protection of trade secrets in a data-driven, networked environment – Is the update already out-dated?, 14 Journal of Intellectual Property Law & Practice (2019) 814, 820, abrufbar unter https://academic.oup.com/jiplp/article/14/10/814/5572178.

[279] Art. 4(3), Second Presidency compromise text v. 21.10.2022, abrufbar unter https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.

[280] Fourth Presidency compromise text, v. 23.1.2023, abrufbar unter https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

[281] Im Fourth Presidency compromise text v. 24.1.2023 wird die Möglichkeit der Vereinbarung zusätzlicher Sicherungsmaßnahmen zwischen Dateninhaber und Drittem in Art. 5(6) eingefügt, vgl. https://table.media/europe/wp-content/uploads/sites/9/2023/01/20230124_Data-Act_4th_Compromise_Text.pdf.

[282] Kritisch *Lorenzen* ZGE 2022, 251, 262; *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 88 f.

des Nutzers bei Verletzung von Geheimhaltungspflichten in Bezug auf die Entwicklung von Konkurrenzprodukten ein.

Von Bedeutung für den Geheimnisschutz kann die Art der Zugangsgewährung sein. Sollte ein in-situ-Zugang als ausreichend angesehen werden, könnte dies den Schutz stärken, soweit eine Weiterverwendung der Daten dabei stärker unter der Kontrolle des Dateninhabers bleiben würde. Jedoch würde dies im Widerspruch zum Zweck des DA-E stehen und könnte umgekehrt auch Zugriffsmöglichkeiten des Dateninhabers auf vertrauliche Informationen der Dritten eröffnen, die sich aus Art und Umfang der genutzten Daten ergeben könnten und damit wiederum das Problem des Business Monitoring berühren. Hier wäre ein durch den Hersteller nicht kontrollierbarer Datenzugang vorzuziehen.

Weitere Probleme können sich ergeben, wenn Dateninhaber und Geheimnisinhaber nicht identisch sind. Die Definition in Art. 2(6) DA-E knüpft an die Kontrolle des technischen Designs oder der Zugangsmittel an, so dass man in der Praxis von einer häufigen Übereinstimmung der Rollen des Dateninhaber und Geheimnisinhabers ausgehen kann, soweit es um maschinengenerierte Daten selbst geht. Anders kann es sein, wenn vorbestehende Geheimnisse in den zugangspflichtigen Daten enthalten sind. Hier muss sich der Geheimnisinhaber bereits im Vorfeld gegenüber dem Dateninhaber durch entsprechende Schutzmechanismen absichern. Dies ist aber wohl bei connected cars, anders als etwa bei Smart Factories, weniger relevant.

Die im DA-E verankerte Priorität der Zugangsrechte über den Geheimnisschutz kann die Bereitschaft zum Data Sharing beeinträchtigen. Bereits die bei der Nutzung des Fahrzeugs generierten Rohdaten und aufbereiteten Daten können Geheimnisqualität haben, soweit sie etwa die Performanz des Fahrzeugs oder sonstige technische Funktionen betreffen, die der Hersteller vertraulich halten wollte. Dies steigert sich mit der Aggregierung und weiteren Bearbeitung. Auch wenn aus diesen Bearbeitungsvorgängen resultierenden Daten derzeit aus dem Anwendungsbereich ausgeschlossen sind, können sich in der Praxis Schwierigkeiten ergeben, diese aus einem gewährten Datenzugang auszunehmen. Der Einsatz von Verschlüsselungsmethoden kann zwar den Übertragungsweg sichern, verhindert aber nicht den Datenzugang beim Empfänger. Hier sollten dessen Verwendungsbeschränkungen zusätzliche Sicherheit schaffen.

Art. 28a des Kompromisstextes zum DA-E vom Oktober 2022 bekräftigt noch einmal, dass der Dateninhaber vom Dritten und vom Nutzer technische Maßnahmen und Wahrung der Vertraulichkeit verlangen kann. Allerdings stellen sich hier nicht nur Kontrollprobleme, sondern die nicht eindeutige Bestimmung des Herausgabezwecks, die jedenfalls auch das Angebot der Daten auf Datenmärkten ohne konkret benannten Dritten nicht grundsätzlich ausschließt, kann den Einsatz hinreichender Kontrollmechanismen in der weiteren Wertschöpfungskette erschweren. Insbesondere wird hier der Einsatz von vertraglichen Sicherungsmaßnahmen an seine Grenzen stoßen. Andererseits scheint die Relevanz des Geheimnisschutzes im Bereich der generierten Daten nicht so gravierend zu sein, während andererseits die Notwendigkeit des Datenzugangs für die nachgelagerten Märkte enorm sein kann. Daher stellt sich hier vor allem das Problem der Vermeidung von „overclaiming“, also der Geltendmachung von Geheimnisschutz auch in Fällen, in denen dieser gar nicht besteht.[283]

Insofern ist die Einfügung der Verpflichtung des Dateninhabers, die Daten zu identifizieren, die Geheimnisse enthalten, in Art. 5(8) DA-E zentral. Diese Identifizierungspflicht kann eine zentrale Bedeutung für die Effektivierung des Geheimnisschutzes erlangen, aber umgekehrt auch der Gefahr entgegenwirken, dass die Hersteller den Geheimnisschutz als Vorwand benutzen, um der Zugangsgewährung zu entgehen. Wie genau die Identifizierung durchgeführt werden soll, ist offengelassen.

[283] *Radauer u.a.*, Study on the Legal Protection of Trade Secrets in the Context of the Data Economy, Final Report, Brussels 2022, S. 84.

Dagegen ist die nunmehr aktuell im fünften Kompromisstext zum DA-E vom 21.2.2023 in Art. 4(3a) und Art. 5 (8a) eingeführte ausnahmsweise Verweigerung des Zugangs aus Gründen des Geheimnisschutzes kritisch zu bewerten.[284] Zwar soll diese Ausnahme nur „unter außergewöhnlichen Umständen“ eingreifen, in denen der Dateninhaber nachweisen kann, dass „ernsthafter Schaden“ aus einer Geheimnisverletzung „sehr wahrscheinlich“ ist. Dies wird in Erwägungsgrund 28a dahin konkretisiert, dass der ökonomische Schaden für den Dateninhaber aus einer Geheimnisverletzung von einer Größenordnung ist, die eine Ablehnung des Zugangsbegehrens rechtfertigt. Dies ist aber so vage formuliert, dass damit einem „overclaiming“ Tür und Tor geöffnet ist und die Gefahr besteht, dass die Effektivität der Zugangsrechte durch deren Aufweichen erheblich beeinträchtigt wird. Hier scheint ein „harter“ Vorrang zur Erreichung der Ziele des DA-E sinnvoller, natürlich unter Anwendung aller Möglichkeiten zum Schutz der Geheimnisse.

Der dargestellte Konflikt betrifft alle hier behandelten Geschäftsmodelle und Konzepte im Bereich des connected cars in gleicher Weise. Mit der im Kompromisstext vom Oktober 2022 zusätzlich eingeführten Spezifizierungspflicht des Herstellers verbessern sich die Möglichkeiten des Interessenausgleichs bei Einsatz von OTP und Data Shared Server-Konzept. Soweit dabei der Nutzer den Zugang gewährt, ist durch die Spezifizierung ein konkreter Schutz der Geheimnisse erleichtert und damit auch die Anreize für den Hersteller vermindert, durch zu weitgehende Zurückhaltung von Daten die eigenen Geheimnisse zu schützen. Zum anderen erleichtert dies die Möglichkeit, die Geheimniseigenschaft durch neutrale Dritte überprüfen zu lassen. Hier wäre dann ein weiteres Anwendungsfeld für eine Datentreuhandschaft gegeben. Erwägungsgrund 29 des vierten Kompromisstextes führt in diesem Kontext selbst die Einschaltung vertrauenswürdiger Vermittlerdienste an und scheint damit eine Abkehr von entsprechend anders strukturierten extended vehicle-Konzepten zu befürworten.

4. Anforderungen an Datenschutz-Compliance beim Datenzugang

a) Verhältnis des DA-E zur DSVGO

Man kann davon ausgehen, dass die meisten wenn nicht sogar fast alle der im connected car generierten Daten personenbezogenen Charakter aufweisen, da mit einfachen Kennungen wie Kennzeichen oder sonstige Kfz-Identifikationsdaten ebenso wie bei Übertragung über Mobilfunkschnittstelle eine Verknüpfung zumindest zum Halter oder Fahrer hergestellt werden kann.[285] Das umfasst nicht nur vom Fahrer selbst bei der Nutzung generierte Daten, sondern auch solche, die das technische Funktionieren oder die Umgebung betreffen und Auskunft über Verhalten oder Fahreigenschaften des Fahrers oder Halters geben können.

Data Sharing steht in einem grundsätzlichen Konflikt mit dem Datenschutzrecht, das die Datensouveränität des Betroffenen sichern will und auf dem Prinzip der Datenminimierung basiert.[286] Es ist daher zu beleuchten, inwieweit das Datenschutzrecht dem Datenzugang kritische Grenzen setzt. Der DA-E enthält insoweit nur die Bestimmung, dass das Datenschutzrecht unberührt bleiben soll (Art. 1(3) DA-E; Erwägungsgrund 7 S. 4). Jedoch findet man ergänzende Bestimmungen, die auch auf personenbezogene Daten Anwendung finden, und beide Regelungen sind parallel anwendbar.[287] Damit stellt sich die Frage nach der Auflösung von Konfliktsituationen. Der Europäische Datenschutzausschuss („European Data Protection Board“ (EDPD) empfiehlt insoweit die Aufnahme

[284] Fifth Presidency compromise text, v. 21.2.2023, geleakte Version, noch nicht im Internet verfügbar.
[285] Vgl. *Karsten/Wienröder*, RAW 2022, 99, 102.
[286] Vgl. *Specht-Riemenschneider/Blankertz*, ‘Lösungsoption Datentreuhand: Datennutzbarkeit und Datenschutz zusammen denken’, MMR 2021, 369; *Specht-Riemenschneider*, ‘Das Verhältnis möglicher Datenrechte zum Datenschutzrecht‘ GRUR Int. 2017, 1040, 1041f; *Schweitzer*, ‘Datenzugang in der Datenökonomie: Eckpfeiler einer Informationsordnung‘, GRUR 2019, 569, 571.
[287] *Specht-Riemenschneider*, MMR 2022, 809, 811; *Hennemann/Steinrötter*, NJW 1481, 1482.

spezifischer klarstellender Regelungen in den DA-E für diese Fälle.[288] Das Problem ist insofern besonders relevant, als häufig personen- und nicht-personenbezogene Daten in einem Datensatz enthalten oder sonst nicht trennbar sind. Dann wären die datenschutzrechtlichen Regelungen jedenfalls parallel einzuhalten.

b) Kompatibilität der DSGVO mit dem DA-E

Die Informationspflichten nach Art. 13, 14 DSGVO ergänzen die Pflichten des Dateninhabers gegenüber dem Nutzer nach Art. 3(2) DA-E. Auch die Zugangsrechte aus Art. 4 und 5 DA-E und das Recht auf Datenportabilität nach Art. 20 DSGVO laufen parallel.[289] Insofern sind das Recht auf direkte Übertragung nach Art. 20(2) DSGVO und das Zugangsrecht nach Art. 5(1) DA-E kongruent. Art. 4 und 5 DA-E gehen über die DSGVO insoweit hinaus, als nicht nur einmalige Datenherausgabe verlangt werden kann, sondern diese fortdauernd und möglichst in Echtzeit zu erfolgen hat. Auch gibt es nach dem DA-E keinen Vorbehalt der technischen Machbarkeit wie in Art. 20 DSGVO.[290] In Ergänzung zu Art. 17 DSVGO muss der Datenempfänger die Daten nach Art. 6(1) DA-E löschen, sobald diese für den vereinbarten Zweck nicht mehr erforderlich sind.

Nach Erwägungsgrund 21 DA-E soll der Zugang auch in-situ möglich sein.[291] Die DSGVO geht hier für den Nutzer weiter, da Art. 15(3) DSGVO auch die Möglichkeit vorsieht, dass der Berechtigte eine „Kopie“ der gespeicherten Daten erhält. Art und Umfang dieses Anspruchs sind allerdings derzeit unklar und stark umstritten.[292]

c) Datenschutzrechtliche Verarbeitungsgrundlagen

Art. 20 DSGVO begründet für den Betroffenen ein Recht auf Datenportabilität, das ebenfalls für Mobilitätsdaten mit Personenbezug nutzbar gemacht werden kann, nun aber durch die Zugangsrechte des DA-E ergänzt wird. Art. 20 DSGVO basiert auf der Prämisse, dass die Daten vom Betroffenen selbst bereitgestellt werden und insoweit eine Einwilligung oder ein Vertragsverhältnis als rechtliche Grundlage für die Verarbeitung in Betracht kommt. Dies lässt sich für Art. 3 bis 5 DA-E ähnlich bewerten. Die Initiative geht vom Nutzer aus, er veranlasst die Bereitstellung der Daten durch den Dateninhaber an einen Dritten, so dass man eine (zumindest konkludente) Einwilligung nach Art. 6 Abs. 1 lit. a) DSGVO als Rechtsgrundlage für die Übermittlung annehmen kann.[293] Auch bestehen zwischen Nutzer, Dateninhaber und Drittem Vertragsverhältnisse, so dass auch Art. 6 Abs. 1 lit. b) DSGVO als Rechtsgrundlage in Betracht kommt. Hier wäre die Verarbeitung auf die zwischen Nutzer und Drittem vereinbarten Zwecke begrenzt. Nutzer und Dritter wäre als gemeinsam Verantwortliche anzusehen, und sie müssten in ihren Vertrag eine Verteilung der Verantwortlichkeiten nach Art. 26 DSGVO einbeziehen.[294] Problematisch für die Anwendung von Art. 6 Abs. 1 lit. b) DSGVO ist aber, dass dieser Erlaubnistatbestand überwiegend nicht für anwendbar gehalten wird, wenn die Gestattung der Datenverarbeitung selbst Vertragsgegenstand ist, da dann nur die Einwilligung in Frage kommen soll.[295]

---

[288] EDPB, EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted 4 May 2022, Rn. 26; ebenso Specht-Riemenschneider, MMR 2022, 809, 810.
[289] *Klink-Straub/Straub*, ZD-Aktuell 2022, 01076.
[290] Vgl. *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 300 ff, die vorschlagen, die Interoperabilitätsverpflichtung auf Dateninhaber auszudehnen.
[291] See *Kerber*, Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, 2022, S. 9; *Specht-Riemenschneider*, MMR 2022, 809, 816.
[292] Vgl. nur BGH, Urt. v. 15.06.2021 – VI ZR 576/19; EDSA, Richtlinie 1/2022, Rn. 141 ff.; BAG, Urt. v. 16.12.2021 – 2 AZR 235/21; VG Potsdam, Urt. v. 24.08. 2022 – 9 K 114/21; 186/22; OLG Karlsruhe, v. 29.11.2022 – 12 U 305/21; 20 U 295/21; OLG Celle, v. 15.12.2022 – 8 U 165/22. Beim EuGH – C-487/21 sowie C-307/22 – laufen Vorlageverfahren, ob die Dokumente oder nur Auszüge auszuhändigen sind.
[293] *Specht-Riemenschneider*, MMR 2022, 809, 810.
[294] Vgl. *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. S. 90.
[295] Vgl. Kühling/Buchner/*Buchner/Petri*, DS-GVO, Art. 6 Rn 41.

Auch wird es häufig schwer sein, die Verarbeitung isoliert jeweils auf die datenbasierten Zusatzleistungen zu beziehen und insoweit die Erforderlichkeit zu beurteilen.[296]

Ist der Nutzer nicht der Betroffene, etwa weil es mehrere Fahrer gibt, wie z.B. beim Carsharing, und diese auch anhand der Daten oder durch Verknüpfung identifizierbar sind, könnte sich eine Rechtsgrundlage aus Art. 6 (1)(c) DSVGO ergeben. Bereits aus dem Verweis von Art. 4(5) DA-E auf die DSGVO ist davon auszugehen, dass der DA selbst keine entsprechende Rechtsgrundlage darstellt (Erwägungsgrund 24). Daher kann man insoweit die Zugangsrechte nach dem DA-E nicht als Regelungen im Sinne von Art. 6 (1) (c) oder Art. 9 (1)(g) DSGVO heranziehen.[297]

Es bliebe dann noch eine allgemeine Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO. Insoweit wäre auch die Regelung in Art. 6 Abs. 2 lit. b) DSGVO relevant, die das Profiling auf das für die Erfüllung der Dienste notwendige Maß beschränkt. Dies lässt sich als Konkretisierung von Art. 6 Abs. 1 lit. f) DSGVO ansehen. Darüber hinaus ist der Prozess der Abwägung mit erheblichen Unsicherheiten für die Datenverwendung verbunden. Denkbar wäre die Anwendung als tragfähige Rechtsgrundlage etwa dann, wenn beim pay-as-you-drive oder pay-when-you-drive ein Dritter das Fahrzeug führt.[298]

Ansonsten bliebe nur der Weg über eine wirksame Einwilligung. Dies ist in verschiedener Hinsicht problematisch. Die Einwilligung muss nach Art. 7 DSGVO freiwillig und informiert sein. Dies bedeutet auch, dass bei Ablehnung der Einwilligung der Nutzer die Dienste weiter vollumfänglich nutzen können muss. Weiterhin ist die Einwilligung frei widerruflich, was aber teilweise auf bestimmte Fälle eingeschränkt wird, vor allem, wenn diese unverzichtbare Voraussetzung für das Vertragsverhältnis war.[299] Vor allem ist die Informiertheit der Einwilligung ein Problem, da über die Verarbeitungszwecke und die Übermittlung der Daten informiert werden muss.[300] Solange es um Herausgabe der Daten an vom Nutzer benannte Dienste geht und dieser der Betroffene ist, lässt sich eine wirksame Einwilligung begründen. Zu beachten bleibt dabei, dass sich ein Personenbezug auch erst bei der späteren Verarbeitung und Verknüpfung von Daten ergeben kann. Bei einer weiten Zweckbestimmung oder gar einer Kommerzialisierung auf Datenmärkten käme nur noch ein „broad consent“ in Betracht, bei dem eine Vorab-Einwilligung für alle folgenden Verarbeitungsvorgänge ohne konkrete Bezeichnung oder Kenntnis davon. Ein solcher wird teilweise im medizinischen Bereich als Verarbeitungsgrundlage für Gesundheitsdaten eingesetzt, was aber sehr umstritten ist.[301] Er kommt auch für die Verarbeitung von Mobilitätsdaten nicht in Betracht, weil der Nutzer gar nicht alle weiteren Verarbeitungsmöglichkeiten und -zwecke überblicken kann.

Soweit sensible Daten als besondere Kategorien betroffen sind, was auch bei der Datenverarbeitung im connected car möglich ist, kommt nach Art. 9 Abs. 2 lit. a) SGVO nur eine explizite Einwilligung als Rechtsgrundlage in Betracht, die sich aber im Rahmen der Gewährung des Datenzugangs umsetzen ließe. Ansonsten käme noch Art. 9 Abs. 2 lit. g) DSGVO in Betracht, was aber ein erhebliches öffentliches Interesse voraussetzt und sich allenfalls im Hinblick auf die Bedeutung des Datenzugangs für Innovation begründen ließe.[302]

Neben den im Fahrzeug generierten Daten geht es weiter um den Schutz der Zugangsdaten der Zugangsberechtigten. Art. 4(3) und 5(3) DA-E beschränkt deren Nutzung auf das für den Zweck

---

[296] Vgl. *Reiter/Methner/Schenkel,* Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 15.
[297] *Specht-Riemenschneider*, MMR 2022, 809, 811; *Metzger/Schweitzer*, ZEuP 2023, 82. Zweifelnd auch *Karsten/Wienröder*, RAW 2022, 99, 105.
[298] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 15.
[299] Kühling/Buchner/*Buchner/Kühling*, DS-GVO, Art. 7 Rn. 38; Gola/*Schulz*, DS-GVO, Art. 7 Rn. 56.
[300] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 18, weisen auch auf eine mögliche „Informationsüberlastung“ des Nutzers hin.
[301] Vgl. Gola/*Schulz*, DS-GVO, Art. 7 Rn. 35; *Weichert*, Big Data im Gesundheitsbereich, Gutachten ABIDA, 2018, S. 126.
[302] So *Specht-Riemenschneider*, MMR 2022, 809, 811.

Notwendige, die Sicherheit sowie die Verifizierung der Nutzereigenschaft sicherzustellen. Art. 6(1) DA-E enthält eine vergleichbare Regelung für den zugangsberechtigten Dritten, wobei Art. 6(2)(b) DA-E noch einmal ausdrücklich ein mögliches Profiling strikt auf den vorgesehenen Zweck der Diensteerbringung begrenzt. Die Regelungen des DA-E dienen hier dem Datenschutz des Betroffenen und setzen die datenschutzrechtlichen Prinzipien der Zweckbindung und Datenminimierung um.

Ein möglicher Ausweg für das Problem einer tragfähigen Rechtsgrundlage wäre, Art 4 und 5 DA-E ausdrücklich als Regelungen im Sinne von Art. 6 Abs. 1 lit. c) DSGVO anzuerkennen, etwa durch Ergänzung von Erwägungsgrund 24.[303] Damit hätte man eine Konkordanz zwischen personenbezogenen und nicht-personenbezogenen Daten erreicht, und der Nutzer hätte als Verantwortlicher auch die Kontrolle über die Verarbeitung. Jedoch ergäbe sich daraus die Gefahr, dass es zur extensiven Verarbeitung personenbezogener Daten kommt, deren Umfang auch durch die vom DA-E bei der Verarbeitung durch Dritte gesetzten Grenzen nicht datenschutzkonform eingehalten werden können.[304] Angesichts der Unsicherheiten bei der Zweckbestimmung und -begrenzung zwischen Nutzer und Drittem ist es nicht unwahrscheinlich, dass die Daten entgegen der ursprünglichen Zweckbestimmung weiterverwendet werden. Insoweit wäre eine allgemeine, unspezifische Einwilligung („broad consent“) des Betroffenen im Rahmen der Zugangsgewährung nicht ausreichend, da die zukünftigen Verarbeitungsvorgänge und -möglichkeiten dann nicht vorhersehbar und bestimmt sind.

d) Folgerungen für den Datenzugang

Als Schlussfolgerungen ergeben sich insoweit zum einen, soweit und so früh wie möglich Anonymisierungstechniken einzusetzen, möglichst vor dem Datenteilen.[305] Der Einsatz von Anonymisierung und Pseudonymisierung fließt auch in eine mögliche Interessenabwägung nach Art. 6 Abs. 1 lit. f) DSGVO als Abwägungsfaktor ein. Die Anforderungen an eine wirksame Anonymisierung in der DSGVO stehen auch in Beziehung zu der Zumutbarkeit in wirtschaftlicher Hinsicht.[306] Auch wenn sich dies bereits aus der DSGVO ergibt, könnte man den größtmöglichen Einsatz von Anonymisierungstechnik noch einmal ausdrücklich im DA-E verankern. Weiterhin wäre es zur Schaffung von Rechtssicherheit sinnvoll, einen konkreten Grad an Anonymisierung gesetzlich als ausreichend festzuschreiben, etwa durch eine gesetzliche Vermutung.

Weiterhin wäre, vergleichbar mit der Diskussion zum Gesundheitsbereich, an die Einholung abgestufter Einwilligungen über Datenmanagementsysteme (PIMS) zu denken, so dass der Betroffene auch für spätere Zugriffe Zustimmungsmöglichkeiten bekommt.[307] Damit wäre auch eine Option geschaffen für Zugriffe auf Daten von Betroffenen, die nicht mit dem Nutzer identisch sind. § 26 TTDSG sieht nunmehr auch für connected devices ein Einwilligungsmanagement über PIMS vor. Die Nutzer können dabei ihre Präferenzen angeben und speichern. Die Dienste sollen unabhängig sein und durch eine unabhängige Stelle anerkannt werden. Von besonderer Bedeutung ist hier die Datensicherheit, die vom Dienst nachzuweisen ist. Eine Ausprägung eines PIMS ist der „Mobilitätsdatenwächter“, der in einem Gutachten des vzbv ausführlich beschrieben wurde.[308] Eine effektive Umsetzung setzt voraus, dass alle datenverarbeitenden Stellen verpflichtet werden, mit dem PIMS zu kooperieren, da eine freiwillige

[303] *Leistner/Antoine*, IPR and the use of open data and data sharing initiatives by public and private actors, 2022, S. 91.
[304] Vgl. *Metzger/Schweitzer*, ZEuP 2023, 82.
[305] Vgl. auch *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 307; *Metzger/Schweitzer*, ZEuP 2023, 82, unter VI.3.
[306] Vgl. EuGH, C-582/14 Breyer / Deutschland ECLI:EU:C:2016:779, [2017] 2 C.M.L.R. 3, Rn. 45-49,
[307] Vgl. Gutachten der Datenethikommission, 2019, S. 22, 126 ff. Zu den Funktionalitäten Krämer, Digitale Selbstbestimmung durch Personal Information Management Systems?, 2022, 5; *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 29 ff.
[308] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 23 ff.

Nutzung wohl in der Praxis nicht funktionieren würde.[309] Die Regelungen des TTDSG reichen dazu nicht aus.[310]

Die fehlende Berücksichtigung der Möglichkeit der Einschaltung von neutralen Dritten, etwa Datentreuhändern, im DA-E wurde bereits bemängelt.[311] Art. 5(1) DA-E lässt die Geltendmachung von Zugangsrechten durch Dritte zu, die im Namen des Nutzers handeln. Erwägungsgrund 29 idF des vierten Kompromisstextes bezieht nun ausdrücklich den Einsatz von Datenvermittlungsdiensten im Sinne der VO 2022/868[312] ein. Erwähnt wird dabei ausdrücklich deren wichtige Funktion bei der Aggregierung der Daten von vielen Nutzern, etwa zu Zwecken des Machine Learning und der Big Data-Analyse, solange die Nutzer in „voller Kontrolle" über das Ob und Wie bleiben. In gleicher Weise sind Intermediäre aber auch zur Effektivierung des Datenschutzes einsetzbar.[313]

III. Verhältnis zu (sektor)spezifischen Regelungen

1. Kompatibilität mit bestehenden sektorspezifischen Regelungen

Nach der Analyse des Data Act und dessen Auswirkungen auf Datenflüsse und Geschäftsmodelle soll die weitergehende Frage behandelt werden, inwieweit die im Arbeitspaket 2 dargestellten sektorspezifischen Regelungen mit dem DA-E kompatibel sind, aber auch, inwieweit die sektorspezifischen Regelungen sowie die ebenfalls bereits dargestellten Geschäftsmodelle und Konzepte die bisher erkannten regulatorischen Lücken schließen können.

a) Eingeschränkter Anwendungsbereich bzgl. Datenarten

Wie aufgezeigt wurde, bietet die genaue Eingrenzung der vom DA-E erfassten Daten theoretische und praktische Probleme. Dies betrifft insbesondere die Unterscheidung zwischen Rohdaten, aufbereiteten Daten sowie abgeleiteten und aggregierten Daten.

In dieser Hinsicht geht die TypGVO andere Wege. Nach Art. 61 i.V.m. Art. 3 Nr. 48 der TypGVO wird der Datenzugang auf Reparatur- und Wartungsinformation bezogen. Damit wird ein funktionsorientierter Ansatz verfolgt.[314] Auch der Zugang zu OBD-Daten nach Art. 3 Nr. 49 TypGVO ist nicht auf Rohdaten i.S. des DA-E beschränkt. Auch insoweit enthält die TypGVO einen funktionalen Ansatz, da dort in Anhang X unter 2.6.1. „einschlägige Informationen, auf deren Grundlage Ersatzteile entwickelt werden können, die für das einwandfreie Funktionieren des OBD-Systems erforderlich sind", und 2.6.2. die Zurverfügungstellung von „Informationen, auf deren Grundlage generische Diagnosegeräte entwickelt werden können" vorgesehen ist.

Die Kfz-GVO 461/2010 erfasst alle im Netzwerk des Herstellers geteilten Informationen. Unabhängige Werkstätten sollen ungehinderten Zugang zu den für Wartung und Instandsetzung notwendigen

[309] Vgl. *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung, 2022, S. 30 ff., dort auch zur Ausgestaltung im Einzelnen.

[310] Vgl. *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 42 ff. Im Bereich der Unfallforschung ist bereits ein Datentreuhändermodell vorgesehen, § 63a StVG.

[311] *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 309.

[312] Verordnung (EU) 2022/868 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. 152/1 v 3.6.2022.

[313] Eingehend zu den rechtlichen Rahmenbedingungen für Datenintermediäre und deren Funktion beim Datenzugang Schweitzer u.a., Data access and sharing in Germany and in the EU Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022, S. 275 ff.

[314] Zustimmend *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 25, 28, die auch zeigen, dass auch die Bearbeitung noch als Teil des in der Diskussion oft gebrauchten Begriffs der Ko-Generierung der Daten durch den Nutzer anzusehen ist; dort auch mit dem Hinweis, dass Ko-Generierung eine graduelle Frage ist und entsprechend auch die Zugangsinteressen abgestuft sein können, Rn. 30 enthält einen entsprechenden Regelungsvorschlag.

Informationen bekommen und folgt auch insoweit einem funktionsbezogenen Ansatz.[315] Der entsprechende Begriff der „technischen Information“ ist bewusst offen gehalten.[316] Hier ist eher weitergehend die Frage, ob auch Rohdaten, die nicht mit dem eigenen Netzwerk des Herstellers geteilt werden, dann Dritten zur Verfügung zu stellen sind, was wiederum nach der Erforderlichkeit für den Zweck zu beurteilen ist, nämlich die Nutzung für Reparaturzwecke.[317] Es bleibt allerdings die wesentliche Einschränkung des Anwendungsbereichs von Art. 101 AEUV und der GVO.

Auch die IVS-RL und die Delegierte Verordnung 2017/1926 basieren auf der Bereitstellung hochwertiger Straßen-, Reise- und Verkehrsdaten, was zumindest eine technische Bearbeitung, aber auch eine wertschöpfende Weiterverarbeitung der Rohdaten beinhaltet, da sie auch der Schaffung neuer Informationsdienste und Geschäftsmodelle dienen sollen. Der Anhang zur Delegierten Verordnung 2017/1926 enthält eine genaue Auflistung der Datenkategorien. Allerdings sollen nur bereits formatierte Daten in maschinenlesbarer Fassung bereitgestellt werden, so dass unbearbeitete Rohdaten herausfallen können. Dies ist aber angesichts des dargestellten Zusammenhangs von Datengenerierung und Aufarbeitung keine wesentliche Einschränkung.

Für das Kartellrecht lässt sich nicht allgemein sagen, auf welche Form der Daten sich die unterschiedlichen Ansprüche jeweils richten. Dies wird auch durch den Schutzzweck bestimmt und ist jedenfalls auch nicht von vornherein auf Rohdaten beschränkt. Umgekehrt ist die Frage, inwieweit auch Rohdaten in Echtzeit vom Zugangsanspruch umfasst sind, offen. Hier sind insbesondere § 19 Abs. 2 Nr. 4 und § 20 Abs. 1a GWB einschlägig, deren konkrete Anwendung abzuwarten ist.[318]

Aus der näheren Analyse ergibt sich zunächst, dass die untersuchten sektorspezifischen Regelungen zwar einen anderen Ansatz hinsichtlich der erfassten Datenarten verfolgen, diese aber als weitergehende Regelungen auf dem engeren DA-E aufbauen können und insoweit auch kompatibel sind. Es stellt sich dann weiter die Frage, inwieweit die weitergehenden sektorspezifischen Regelungen den begrenzten Anwendungsbereich des DA-E, als Defizit verstanden, „kompensieren“ können. Dies ist hinsichtlich der frühen Phase der Datenbearbeitung der Fall, und auch aggregierte und abgeleitete Daten können durch die spezifischen Regelungen erfasst werden. Andererseits ist der DA-E insofern weiter, als er auch auf Rohdaten anwendbar ist, was auch nicht bei allen spezifischen Regelungen der Fall ist. Gleiches gilt für einen möglichen Echtzeitzugriff auf die Daten.

Weiterhin gilt dies natürlich nur für den begrenzten sachlichen Anwendungsbereich der sektorspezifischen Regelungen. Über den Bereich von Wartungs- und Reparaturdaten und Reisedaten hinaus bleibt nur die unsichere Anwendung des Kartellrechts, so dass in Bezug auf den sachlichen Anwendungsbereich die meisten Daten nicht erfasst werden. Der größere Teil der möglichen Dienste (vgl. Ziff. D.III) kann von dem entsprechenden Datenzugang nicht profitieren.

Soweit die sektorspezifischen Regelungen anwendbar sind, ist jedoch der funktionsorientierte Ansatz dem Ansatz des DA-E überlegen, da er grundsätzlich alle Daten unabhängig vom Bearbeitungsstadium umfasst sowie auch aggregierte Daten. Er vermeidet schwierige theoretische und praktische Abgrenzungsprobleme und führt gleichzeitig zu einer zweckbezogenen Begrenzung des Umfangs des Datenzugangs. Allgemein lässt sich hinsichtlich der rechtlichen Ausgestaltung von Zugangsregeln folgern, dass diese auf alle Daten in allen Formen bezogen sein sollten, die für die Erbringung des betreffenden Dienstes des nachgelagerten Markts notwendig sind.[319] Dies ist nunmehr mit dem vierten Kompromisstext zum DA-E soweit verankert, als stärker auf die Funktionalität der sensor-erhobenen Daten abgestellt würde und es nicht um aggregierte Daten geht, so dass hier der DA-E sich den

[315] Ergänzende Leitlinien, ABl C v. 28.5.2010, S. 26 Rn. 63.
[316] Ergänzende Leitlinien, ABl C v. 28.5.2010, S. 26 Rn. 66.
[317] Ergänzende Leitlinien, ABl C v. 28.5.2010, S. 26 Rn. 65.
[318] Zur Anwendung des Kartellrechts auf das Data sharing allgemein vgl. *Schweitzer u.a.*, Data access and sharing in Germany and in the EU Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022, S. 133 ff.
[319] *Drexl u.a.*, Position Statement of the MPI of 25 May 2022 on the Proposal for a Data Act, Rn. 25.

sektorspezifischen Regelungen annähern würde, was nicht nur die Kompatibilität zwischen beiden verbessert, sondern aufgrund des horizontalen Anwendungsbereichs des DA-E eine breitere Anwendung dieses sachgerechten Ansatzes gewährleistet würde.

b) Zugang und Weiterverwendung

Hinsichtlich Zugang und Weiterverwendung der Daten enthalten auch die sektorspezifischen Regelungen Beschränkungen. Art. 61 TypGVO gewährt Zugriff für „unabhängige Wirtschaftsakteure“ und beschränkt den Zugriff bei sicherheitsrelevanten Daten auf autorisierte Betriebe. Die in Art. 3 Nr. 45 TypGVO näher definierten Zugangsberechtigten beschränken sich auf die Beteiligung an Wartung und Reparatur unabhängig vom Hersteller, sowie auf Anbieter von Inspektions- und Prüfdienstleistungen. Ergänzt wird dies durch Zugang zu OBD-Informationen. Die Informationen sollen in verschiedener Form über das Internet bereitgestellt werden. Eine wichtige Neuregelung im Jahr 2018 war die Erstreckung des Zugangs auf solche Informationen, die der Hersteller nicht in seinem Netzwerk zugänglich macht, aber selbst zu Wartungs- und Reparaturzwecken nutzt. Dies ist besonders bei Remote Services von Bedeutung.[320] Die Beschreibung der bereitzustellenden Informationen und der Ausschluss der Möglichkeit des Herstellers, deren Kreis einzuschränken, schützt die Interessen der Diensteanbieter auf Sekundärmärkten und schafft Rechtssicherheit. Eine wichtige Einschränkung ist, dass ein Zugang in Intervallen oder in Echtzeit nicht vorgeschrieben ist, was für viele Dienste aber Voraussetzung wäre. Von Bedeutung ist auch der Einsatz des standardisierten Autorisierungsverfahrens SERMA, das in Anhang X der TypGVO beschrieben ist und mit dessen Einbeziehung ein konkreter Schritt in Richtung Interoperabilität gegangen würde.

Die Weiterverwendung durch die Datenempfänger ist nicht weiter eingeschränkt, aber natürlich auf die Zwecke bezogen (Art. 61 Abs. 2 TypGVO), und der gesamte Zugang in Anhang X hinsichtlich Inhalt und Art des Datenzugangs ist konkret spezifiziert. Nach Zi. 6.1. des Anhangs X muss der Zugangsberechtigte über die „Reproduktion“ und „Republikation“ der Informationen mit dem jeweiligen Hersteller verhandeln.

Die Kfz-GVO 461/2010 ist ebenfalls auf den Zweck des Verkaufs von Ersatzteilen sowie Erbringung von Wartungs- und Instandsetzungsleistungen beschränkt und kommt „unabhängigen Marktbeteiligten“ zugute, deren Kreis an die TypGVO angelehnt ist.[321] Der Anspruch erfasst sämtliche Informationen, die der Hersteller mit dem eigenen Netzwerk teilt.

Nach Art. 4(1) der Delegierten Verordnung 2017/1926 zur IVS-Richtlinie 2010/40/EU sind auskunftspflichtig „Verkehrsbehörden, Verkehrsbetreiber, Infrastrukturbetreiber oder Anbieter von nachfrageorientierten Verkehrsangeboten“. Nach Art. 8 sind Austausch und Weiterverwendung nicht weiter eingeschränkt, aber nach Abs. 2 eine neutrale, diskriminierungsfreie und unvoreingenommen Weiterverwendung vorgeschrieben. Die Nutzungsmodalitäten können in einer Lizenzvereinbarung geregelt werden, die so wenige Einschränkungen der Weiterverwendung wie möglich enthalten soll. Hier ist also Spielraum für die Entwicklung vertraglicher Praxis im vorgegebenen Rahmen.

Das Kartellrecht kann beispielsweise gegen Verträge gerichtet werden, die dazu führen, dass Dritte von strategisch wichtigem Informationszugang ausgeschlossen werden. Das kartellrechtliche Vorgehen ist stark einzelfallbezogen und macht oft komplexe und schwierige Analysen erforderlich.[322] Ein wichtiger Anwendungsbereich ist auch die Standardisierung. Wegen deren Bedeutung für Innovation auch im Mobilitätssektor ist es von großer Bedeutung, dass das Setzen von Interoperabilitätsstandards nicht zu wettbewerbsbeschränkenden Zwecken eingesetzt wird, transparent ist und alle relevanten Interessen

[320] Vgl. *Kerber/Gill*, Jipitec 2019, 244 Rn. 19.
[321] Ergänzende Leitlinien, ABl C v. 28.5.2010, S. 26 Rn. 62.
[322] Vgl. *Schweitzer u.a.*, Data access and sharing in Germany and in the EU Towards a coherent legal framework for the emerging data economy, Final Report, 8 July 2022, S. 135 ff.

berücksichtigt.[323] Ansonsten können Standards, die dem nicht entsprechen, die wettbewerbsfördernden Effekte der Zugangsregeln weitgehend torpedieren.

Allgemein lässt sich feststellen, dass die sektorspezifischen Regelungen hinsichtlich Zugang und Weiterverwendung wiederum einer funktionsorientierten Ausrichtung folgen. Abgestellt wird bei der IVS-Richtlinie auf die Anbieter bestimmter Dienstleistungen als Zugangspflichtige. Beim Zugang nach TypGVO ist der Kreis der Zugangsberechtigten funktionsbezogen eingeschränkt, während der Kreis der Zugangspflichtigen auf die Fahrzeughersteller begrenzt ist, die die Kontrolle über die Daten haben und daher als Dateninhaber i.S. des DA-E anzusehen sind.

Der dienstleistungs- und funktionsbezogene Ansatz kommt ohne die vom DA-E herangezogene rollenbezogene Einordnung aus, was auch die Nutzer ausblendet. Ansonsten enthalten die sektorspezifischen Regelungen geringe Einschränkungen der Weiterverwendung und verweisen im Wesentlichen auf vertragliche Vereinbarungen im FRAND-Rahmen. Allerdings erfolgt eine Eingrenzung ja bereits zweck- und funktionsbezogen. Hier bestehen im Ergebnis keine größeren Unterschiede zu den Beschränkungen des Dritten nach dem DA-E durch die Zweckbestimmung sowie Art. 6 DA-E. Dies wird allerdings relativiert durch die Unsicherheiten beim Verständnis des DA-E hinsichtlich der Frage, ob der Nutzer die Daten an Dritte weitergeben kann, ohne dass diese den Beschränkungen von Art. 6 sowie aus dem Vertrag mit dem Dateninhaber unterliegen, und inwieweit auch eine freie Handelbarkeit auf Marktplätzen als Zweck zulässig sein soll. Sollte der DA-E so zu verstehen sein, würde dieser dann über die spezifischen Regelungen hinausgehen.

Ein großer Unterschied der sektorspezifischen Regelungen zum DA-E ist dessen nutzerzentrierter Ansatz. Dies beeinträchtigt deren Kompatibilität, da die Kontrolle über den Zugang auseinandergeht. Die Nutzer spielen im Rahmen der bestehenden sektorspezifischen Ansätze kaum eine Rolle. Demgegenüber ist der vom DA-E vorgesehene Vertrag zwischen Nutzer und Drittem entscheidend für den Umfang des Anspruchs. Der Nutzer bestimmt den Umfang der herauszugebenen Daten, wobei insoweit auch der DA-E einem zweck- und funktionsbezogenen Ansatz folgt, wie bereits dargestellt. Nur werden die Zugangsberechtigten nicht vom Hersteller ausgesucht bzw. per Gesetz bestimmt, sondern vom Nutzer. Die Nutzung und Weiterverwendung durch den Dritten nach dem DA-E ist auch zweckbezogen eingeschränkt, wobei allerdings die Zweckbestimmung wiederum dem Nutzer obliegt.

c) Verbleibende Lücken der sektorspezifischen Regelungen

Insgesamt ergibt sich, dass die sektorspezifischen Regelungen nur sehr begrenzt die Defizite des DA-E kompensieren können. Das ergibt sich zum einen aus dem begrenzten sachlichen Anwendungsbereich der Regelungen.

Aber auch in sachlicher Hinsicht bleiben gravierende Lücken. Überlegen sind die spezifischen Regelungen im Hinblick auf ihren zweck- und funktionsbezogenen Ansatz hinsichtlich der Daten, zu denen Zugang zu gewähren ist, im Vergleich zum DA-E, der sich auf Rohdaten beschränkt. Hinsichtlich des Zugangs entsprechen die Regelungen – vor allem der TypGVO – nicht mehr dem aktuellen Stand der Technik. In Bezug auf die Gewährung eines Echtzeit-Zugangs bleiben die spezifischen Regelungen hinter dem – etwas unklaren – Ansatz des DA-E zurück. Auch wird kritisiert, dass die TypGVO nicht klar genug ausdrückt, dass unabhängige Anbieter nicht nur die Ferndiagnosesysteme der Hersteller benutzen dürfen, sondern eigene Diagnosesysteme einsetzen dürfen, etwa für Predictive Maintenance, was direkten Datenzugang erforderlich machte.[324] Nur dann sei das Anbieten von Ferndiagnose durch Unabhängige möglich. Auch bedürfte es dazu unter bestimmten Bedingungen eines Schreib-Zugriffs.

---

[323] EU-Kommission, Draft Horizontal Guidelines, ABl C 2011, 1 Rn. 257 ff.; COM (2022) 1159 endg Rn. 462 ff. Vgl. ferner die Anwendung von Art. 101 TFEU auf GAIA-X, European Commission, Letter to Gaia-X of 19.10.2021, abrufbar unter https://gaia-x.eu/wp-content/uploads/files/2021-11/Letter%20to%20Gaia-X_update.pdf.

[324] *Kerber/Gill*, Jipitec 2019, 244 Rn. 22.

Wegen des engen Zwecks der spezifischen Regelungen ist auch kein direkter Zugriff auf die Funktionen und Ressourcen des Fahrzeugs vorgesehen. Auch die Möglichkeit des Herstellers, aufgrund seiner Gatekeeper-Funktion die Zugriffe unabhängiger Dritter zu überwachen und daraus wertvolle Informationen für eigene Geschäftsstrategien zu erlangen, wird durch die TypGVO nicht beschränkt. Diese bleibt insoweit hinter dem DA-E (Art. 4(6), Art. 5(3)) zurück.

Ein spezielles Problem soll hier noch angesprochen werden: der Zugang zu Daten im öffentlichen Interesse. Der DA-E begrenzt in Art. 14, 15 den Zugang öffentlicher Stellen auf Daten bei Unternehmen (G2B) auf Notfälle und ist nicht auf ständigen Datenzugang ausgerichtet. Damit ist der weite Bereich des Zugangs des öffentlichen Bereichs zu Verkehrs- und Mobilitätsdaten im Interesse von Verkehrssicherheit, Verkehrsmanagement und Umweltschutz nur durch die IVS-Gesetzgebung abgedeckt, klammert man einmal die eCall-VO aus. Die Richtlinie basiert auf Datenzugang über die Nationalen Zugangspunkte,[325] die dann durch den European Mobility Data Space verbunden werden sollen, der mit dem europäischen Projekt GAIA-X verbunden ist. Dies kann die Transparenz erhöhen und die Aggregation von Daten erleichtern.[326]

Allerdings basiert dies auf einer freiwilligen Bereitstellung der Daten, und Datenanbieter können die Bedingungen für die weitere Nutzung der Daten technisch festlegen.[327] Die Hersteller behalten insoweit volle Kontrolle über die Daten. Der DA-E hat die Chance verpasst, Datenzugangsrechte im öffentlichen Interesse zu etablieren, die den angeführten Interessen des Mobilitätssektors zur öffentlichen Nutzung gerecht werden könnten. So hat etwa der TÜV gefordert, dass der Zugang zu Fahrzeugdaten zur Erfüllung ihrer Aufgaben für Verkehrssicherheit und Umweltschutz geregelt werden sollte.[328] Die Vorschläge gehen dahin, die Daten in neutralen „Trust Centern“ zu speichern, um sie leicht und schnell zugänglich zu halten, aber auch direkten Zugang zu Fahrzeugdaten und -funktionen zu erlangen.

Damit ergibt sich jedenfalls nach derzeitigem Stand auch, dass der Mobility Data Space[329] keine Alternative zu bestehenden Konzepten darstellt und keine Datenzugangsrechte vorgesehen sind, die die bestehenden Lücken füllen können. Verwiesen sein insoweit aber auf das Beispiel des European Health Data Space, für den bereits ein konkreter Regelungsrahmen als Vorschlag vorliegt. Der VO-Vorschlag vom 3.5. 2022[330] enthält in Art. 33 eine Verpflichtung der Dateninhaber, die Daten verfügbar zu machen und zu in Art. 34 f. bestimmten Zwecken eine Zweitnutzung zu ermöglichen. Der Zugang wird durch eine Gesundheitsdatenzugangseinrichtung verwaltet, und ein entsprechender Antrag kann von jedermann gestellt werden. Öffentliche Einrichtungen benötigen nach Art. 48 keine Erlaubnis. Mit dem so geregelten Verfahren werden auch die im Gesundheitsbereich enorm relevanten datenschutzrechtlichen Interessen der Betroffenen mit abgedeckt. Es lässt sich nicht ausschließen, dass in Zukunft auch für den Mobility Space eine vergleichbare Regelung geschaffen wird.

2. Regelungen zur IT-Sicherheit

Als einem weitergehenden Datenzugang gegenläufiges Interesse wird von Herstellerseite immer wieder die IT- und Cybersicherheit angeführt.[331] Dies ist das Hauptargument, ihr Konzept des „extended vehicle“ zu rechtfertigen. Nach Angaben von Interviewpartnern im Rahmen unserer Untersuchung

[325] § 2 Nr. 11 IVSG, Intelligente Verkehrssysteme Gesetz vom 11. Juni 2013 (BGBl. I S. 1553), zuletzt geändert durch Artikel 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2640).
[326] Vgl. *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 19.
[327] *Pretzsch u.a.*, Mobility Data Space – Secure Data space for the Sovereign and Cross-Platform Utilization of Mobility Data, 2021, S. 2. Eine eingeschränkte Verpflichtung zur Bereitstellung von bestimmten Mobilitätsdaten ergibt sich etwa aus § 3a PBefG i.V.m. Mobilitätsdatenverordnung vom 20.10.2021.
[328] Ähnliche Forderungen kommen von ROADPOL, EVU und DEKRA, vgl. *Gill*, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, 2022, S. 22, m.w.N.
[329] S. unter Punkt XX.
[330] Proposal for a Regulation on European Health Data Space, COM(2022) 197 final v. 3.5.2022, abrufbar unter https://eur-lex.europa.eu/procedure/EN/2022_140.
[331] Vgl. *Specht/Kerber*, Gutachten Projekt ABIDA, 2017, S. 177.

sollen nur 65% der Gateways der Fahrzeughersteller zugänglich sein. Hier soll beispielhaft ein Blick auf die für neue Typenzulassungen geltenden UNECE-Regelungen R155 und R156 geworfen werden. Die Regelungen gelten ab Juli 2022 für alle neuen Fahrzeugtypen und ab Juli 2024 für alle neu zugelassenen Fahrzeuge und ist relevant für Hersteller und Zulieferer.

Nach UNECE R156 ist bei einem Software-Update sicherzustellen, dass für die Typengenehmigung relevante Funktionen (beispielsweise Abgas, Bremsen, Motorsteuerung), so entwickelt und validiert werden, dass sie auch nach dem Update noch gesetzeskonform arbeiten. Dabei soll die Sicherheit gegen Fehlfunktionen der Software (ISO 26262) als auch Manipulationssicherheit beim Update selbst (ISO 21434) gewährleistet werden. Für mögliche Updates über Funkschnittstelle (OTA) gelten zusätzliche Anforderungen.

Bei UNECE R 155 wird von den Fahrzeugherstellern der Nachweis eines funktionierenden Cybersecurity Management Systems (CSMS) für die Typgenehmigung gefordert. Es wird von einem CSMS erwartet, dass die damit etablierten Prozesse neue Bedrohungen identifizieren und Abwehrmaßnahmen entwickeln können. Angriffe und Abwehrmaßnahmen sind beschrieben, auch auf die Backendsysteme der Hersteller, die wohl am meisten bedroht sind. Als Leitlinie für die Umsetzung der UNECE R155 soll die ISO/SAE 21434 dienen und einen Standard in der Fahrzeugindustrie setzen.

Bereits in Art. 61 Abs. 1 S. 3 TypGVO ist vorgesehen, dass für den unabhängigen Zugang zum Sicherheitssystem des Fahrzeugs besondere Vorkehrungen getroffen werden müssen. Mit „SERMA“ wird ein standardisiertes Akkreditierungsverfahren zum herstellerübergreifenden Zugang zu geschützten Informationen eingeführt.[332]

Diese Sicherheitsanforderungen sind als Rahmenbedingungen für den Datenzugang zu beachten. Gleichzeitig wird aus dem Zusammenspiel von gesetzlichen Anforderungen und Entwicklung des SERMI-Schemas deutlich, dass die Interessen an Zugang und Sicherheit vor allem auf technischem Wege zum Ausgleich gebracht werden können. Dies lässt sich verallgemeinern: auch bei direktem Datenzugriff durch Dritte kann die hinreichende Sicherheit gewährleistet werden.[333] Gleichzeitig leistet dies einen Beitrag zur Interoperabilität. Ein verbleibendes Problem ist aber, dass die Gateways herstellerspezifisch sind, so dass hier auch eine Standardisierung notwendig ist und gesetzgeberisch unterstützt werden sollte.

3. Kompensation von Defiziten durch bestehende und mögliche zukünftige Konzepte

Die wichtigsten drei Modelle für die Data Governance im Automobilsektor wurden bereits in der Studie der EU zu „access to in-verhicle Data and resources“ von 2017 verglichen und mögliche Politikmaßnahmen diskutiert.[334] Wesentliche Ergebnisse der Studie waren, dass alle drei Formen technisch und rechtlich machbar sind, alle aber auch im Hinblick auf die fünf Leitprinzipien (Zi. X) Vor- und Nachteile haben und die on-board-application-Lösung letztlich zu bevorzugen sei. Es wurden auch jeweils ergänzende regulatorische Maßnahmen herausgearbeitet.

Die Kompatiblität der verschiedenen Konzepte mit dem DA-E wurde bereits unter C.II. analysiert. Auf dieser Grundlage soll im Folgenden untersucht werden, inwieweit die hinsichtlich des DA-E und der sektorspezifischen Regulierung verbleibenden Defizite und Lücken durch die verschiedenen Konzepte kompensiert werden können.

[332] Vgl. auch die Anforderungen nach TypGVO 2018/858 Anhang X Nr. 6.2. und 6.3.
[333] Vgl. TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 77; *Determann/Perens*, Open Cars, Berkeley Tech L.J. 2017, 915, 939; *Kerber/Gill*, Jipitec 2019, 244, Rn. 23.
[334] TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 148 ff.

a) Extended Vehicle-Konzept

Im Bereich des extended-vehicle-Konzepts haben sich unterschiedliche Geschäftsmodelle herausgebildet.[335] Bei BMW Connected Drive werden z.B. bearbeitete Rohdaten übermittelt und später auf dem Marktplatz BMW CarData angeboten. Die von Mercedes auf Caruso angebotene Datenpakete enthalten möglicherweise bereits aggregierte Daten. Auch im Rahmen von ÁDAXO geht es letztlich um die Bereitstellung aller Daten, die die Hersteller auch für die Erbringung eigener Dienstleistungen nutzen.

Hinsichtlich des Datenzugangs wurde schon festgestellt, dass der DA-E hinsichtlich der nutzerzentrierten Kontrolle über das Extended vehicle-Konzept hinausgeht.[336] Die sektorspezifischen Regelungen schaffen sichere Zugangsansprüche im Rahmen der jeweiligen Zweckbestimmung für Dritte und begrenzen damit ebenfalls die Entscheidung der Fahrzeughersteller, welchem Drittunternehmen Zugang zu gewähren ist.

Trotz (herstellerspezifischer) Zugriffsmöglichkeit über API ist ein für manchen Dienst notwendiger Echtzeit-Lesezugriff ebenso wie ein Schreibzugriff ausgeschlossen.[337] Wie oben angeführt, haben die Hersteller für die Zukunft auch die Einräumung eines Schreibzugriffs angekündigt.[338] Im Konzept von ADAXO ist vorgesehen, dass den Dritten alle Daten bereitzustellen sind, die der Hersteller auch selbst nutzt. Weitergehend soll dies auch für die Funktionen gelten, was damit deutlich weiter geht, als vom DA-E und auch von sektorspezifischen Regelungen vorgesehen. Grundlage ist hier ein Vertrag, was einerseits dem Schutz von Geheimnissen zugutekommt, andererseits aber weitere Beschränkungsmöglichkeiten für die Fahrzeughersteller schafft. Auch können Zutrittsbarrieren über die Preisgestaltung errichtet werden. Es muss sich zeigen, ob dies in der Praxis flächendeckend umgesetzt wird. Derzeit fehlt es an gemeinsamen Standards und Transparenz, vor allem hinsichtlich der anfallenden Daten, die Voraussetzung für eine diskriminierungsfreie Bereitstellung ist.

Auch die partiellen Öffnungen ändern nichts an der grundsätzlichen Problematik, dass es im Rahmen des extended vehicle-Konzepts bei der technischen Zugangskontrolle der Hersteller und ihrer „faktischen Datenhoheit“ bleibt.[339] Abgesehen von den Nutzerrechten nach DA-E und dem eng begrenzten Zugang nach der TypGVO entscheidet der Hersteller über Quantität und Qualität der bereitzustellenden Daten und über den technischen Zugang zum Fahrzeug. Damit besteht die Rolle der Hersteller als Gatekeeper fort, was die Möglichkeit zur Erlangung von Informationen über die Tätigkeit der Wettbewerber im Sekundärmarkt beinhaltet. Auch können daraus Interoperabilitätsprobleme mit Diensten auf dem Sekundärmarkt entstehen.[340] Weiterhin bleibt das datenschutzrechtliche Problem, das über eine „breite“ Einwilligung bei Vertragsschluss meist nicht gelöst werden kann. Grundsätzlich ist auch die Anpassung herstellereigener Systeme an ein nutzergerechtes Einwilligungsmanagement möglich. Ein möglicher Einsatz von PIMS für das Einwilligungsmanagement gerät jedoch in Konflikt mit der Tatsache, dass die meisten Daten einen Personenbezug haben und damit auf diesem Wege die Kontrolle auf den Nutzer verlagert würde, was aber dem grundlegenden Ansatz des extended vehicle-Konzepts und der fehlenden Neutralität des Herstellers widerspricht und insofern nicht in deren Interesse liegt.[341]

---

[335] S. oben unter B.XX

[336] S. oben unter C.II.1.c)bb)4(c).

[337] Vgl. *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 10.

[338] S. oben B.xx

[339] *Reiter/Methner/Schenkel*, Gutachten „Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 10. Zu den Konsequenzen aus ökonomischer Sicht Martens/Mueller-Langer, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 14 ff.

[340] Vgl. auch *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 64.

[341] So auch *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 34. Der Vorschlag, insoweit die Landesdatenschutzbehörden mit der Überwachung der ordnungsgemäßen Umsetzung zu betrauen, erscheint unrealistisch.

b) OTP-Konzept

Auch bei OTP sind alle Fahrzeugdaten einbezogen, so dass die Beschränkung des DA-E auf Rohdaten hier nicht besteht. Entscheidender Unterschied ist aber die vollständige Nutzerkontrolle über den Datenzugang, die strukturell durch die offene und interoperable Telematikplattform abgesichert wird, die ins Fahrzeug integriert wird. Darauf können dritte Hersteller und Diensteanbieter Daten abrufen, aber auch Applikationen ausführen. Damit wären beide Aspekte des Zugangs zu Daten und Funktionen im Interesse eines fairen und unverzerrten Wettbewerbs abgedeckt, und das Konzept ginge durch die technische und strukturelle Implementierung über den bestehenden regulatorischen Rahmen hinaus. Weitergehend soll sogar die Kommunikation mit dritten Anbietern über das interne Display möglich sein. Eine Gatekeeper-Funktion der Fahrzeughersteller besteht nicht, so dass auch das Problem der Verschaffung von Wettbewerbsvorteilen des Herstellers auf dem Sekundärmarkt nicht mehr entsteht.

Es bleibt darauf zu achten, dass die Auflösung der technischen Gatekeeper-Funktion durch die Hersteller nicht durch entsprechende vertragliche Restriktionen kompensiert wird. Angesichts der bisherigen Erfahrungen und Diskussion wird es einer „starken regulatorischen Lösung“[342] bedürfen. Beinhaltet diese eine Verankerung des OTP-Konzepts, so hätte man mit der AGB-Kontrolle ein erstes Instrument in der Hand, das eine vertragliche Aushöhlung verhindern könnte. Die Fairness-Regeln für B2B im DA-E ergänzen diese, wobei die entsprechenden Regeln im deutschen Recht in die AGB-Kontrolle für den Bereich B2B integriert werden können.

Auf der anderen Seite ist auch dem Interesse des Herstellers an der Wahrung von Betriebs- und Geschäftsgeheimnissen Rechnung zu tragen. Für den Übertragungsweg bieten sich Verschlüsselungstechniken an. Soweit etwa die Daten über die Fahrzeugperformanz solche Geheimnisse darstellen, kann man mit vertraglichen Vereinbarungen mit den dritten Diensteanbietern Schutz erreichen, wie es der DA-E vorsieht. Dies kann aber bei Weiterverwendung der Daten auf gravierende Kontrollprobleme stoßen. Verliert der Hersteller die technische Kontrolle über den Datenzugang, so bestehen Anreize zum „overclaiming“. Hier ist der Ansatz des zweiten Kompromisstextes zum DA-E vom Oktober 2022 zu begrüßen, der eine Spezifizierungspflicht der Hersteller vorsieht und auf die Einschaltung eines Datentreuhänders verweist. Allerdings kann die Feststellung der Geheimniseigenschaft noch schwieriger sein als die Überprüfung einer datenschutzrechtlichen Einwilligung. Hier wäre an die Einschaltung eines Sachverständigen neutralen Dritten im Einzelfall zu denken, die man mit einer prozeduralen Lösung verbinden könnte. Solche Verfahrenslösungen sind bereits allgemein aus dem Wirtschaftsverkehr bekannt und auch beim Schutz von Geheimnissen in Gerichtsverfahren in § 20 i.V.m. §§ 16 ff. GeschGehG gesetzlich verankert.

Die Wahrung des Datenschutzes könnte in der OTP-Variante mit dem Datenzugang verbunden werden, weil der Nutzer in die Kontrollposition über die Daten versetzt wird. Insoweit kommt dieses Konzept auch der Erhaltung der Wahlmöglichkeiten des Verbrauchers optimal zugute, als die unabhängigen Anbieter freie Zugangsmöglichkeit zu den Nutzern bekommen, diese dann aber selbst entscheiden können, welchen Dienst sie in Anspruch nehmen wollen. Der darüberhinausgehende Aspekt der Versorgung von öffentlichen Institutionen mit Daten zur Verwendung im öffentlichen Interesse[343] wird mangels ausreichender Anreize vermutlich nicht allein auf freiwilliger Basis funktionieren, so dass die Halter dazu verpflichtet werden müssten. Hier verbliebe eine Funktion für eine Datentreuhand.[344]

Die Offenheit der Plattform hat den Vorteil, dass die Kontrolle dem Hersteller vollständig entzogen wird.[345] Nachteil ist, dass umfangreiche Standardisierung von Schnittstellen erforderlich ist und ein hohes Maß an Interoperabilität notwendig ist. Besondere Probleme wirft die IT- und Datensicherheit auf. Es gibt zwar standardisierte Sicherheitslösungen, die aber wiederum neue Sicherheitsprobleme

[342] *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 70.
[343] S.o. C.III.1.c).
[344] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 76 f.
[345] Vgl. auch *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 75: „technischer Bottleneck“.

aufwerfen.[346] Die Entwicklung eigener Lösungen ist dagegen sehr kostenintensiv. IT-Sicherheit und Zertifizierung bedürfen umfangreicher Entwicklungsarbeit, die regulatorisch zu unterstützen ist. Dies braucht Zeit, scheint aber die langfristig vielversprechendste Ausgestaltung zu sein. Mit dem Konzept des S-OTP wird der IT-Sicherheit hinreichend Rechnung getragen und zugleich ein diskriminierungsfreier Zugang gewährleistet und damit die Voraussetzung für Innovation im Sekundärmarkt geschaffen.

c) Data Shared Server und Datentreuhand

Beim Data Shared Server-Konzept sollen die relevanten Daten auf einer unabhängig betriebenen Plattform verwaltet und zugänglich gemacht werden. Auch hier liegt die Entscheidung allein beim Nutzer bzw. Fahrer, wem welche Daten zugänglich gemacht werden. Der Zugang soll rechtlich und technisch diskriminierungsfrei ausgestaltet werden. Der Unterschied zum OTP-Konzept ist die Zwischenschaltung einer neutralen Plattform, die staatlich oder privat als Treuhand betrieben werden kann.

Zu diesem Zweck wurde die obligatorische Einschaltung eines Datentreuhänders als Host für den Backend-Server vorgeschlagen.[347] Die Nutzung lässt sich nicht auf freiwilliger Basis implementieren, sondern alle datenverarbeitenden Stellen müssen zur Einbeziehung des PIMS verpflichtet werden. Der vzbv hat 2022 das Mobilitätswächtermodell vorgelegt, das zusätzlich eine Aufspaltung der Funktionen zwischen Treuhänder und Mobilitätsdatenwächter vorsieht und letzteren als PIMS ausgestaltet. Damit wäre den datenschutzrechtlichen Problemen in besonderer Weise Rechnung getragen, als ein individuelles Datenmanagement möglich wird und der Datentreuhänder auch für eine möglichst frühzeitige Anonymisierung sorgen kann. Der Datentreuhänder ist für den technischen Zugang und die Gewährleistung der IT- und Datensicherheit zuständig, der Datenwächter als Autorisierungsstelle.[348] Gleichzeitig bewirkt die Funktionstrennung („separation of duties“) einen Verlust der Gatekeeperstellung des Herstellers, der nur noch wie jeder dritte Diensteanbieter behandelt wird und keinen faktischen Zugriff auf die Daten mehr behält. Damit nicht nur der eine Monopolist durch den anderen ausgetauscht wird, sollen mehrere Datentreuhänder in Wettbewerb treten, um auch für die neutrale Stelle die Entstehung neuer Zugangsmonopole zu verhindern.[349] Es werden auch konkrete Vorschläge für die institutionelle Ausgestaltung, Qualitätssicherung und Finanzierung gemacht. Danach ist wird eine Ausgestaltung als staatliche Stelle bevorzugt, aber die Ermöglichung privater Anbieter befürwortet.[350]

Ein entscheidender Nachteil ist, dass ein Echtzeitzugriff sowie auch ein Schreibzugriff und damit ein Zugriff zu Funktionen im Fahrzeug für dritte Diensteanbieter ausgeschlossen ist. Allerdings soll mit dem Mobilitätsdatenwächtermodell auch ein Schreibzugriff möglich werden, etwa für Updates von Software.[351] Mit dem Verlust der Kontrolle des Herstellers geht das Konzept über den DA-E hinaus, bleibt aber hinsichtlich Funktionszugang hinter dem OTP-Konzept zurück, was eine Einschränkung der wettbewerbsfördernden Wirkung des Konzepts darstellt. Zur Interoperabilität lassen sich noch keine klaren Aussagen treffen, da es konkrete Umsetzungen noch nicht gibt.

---

[346] Vgl. *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 13.
[347] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 70 f.
[348] Allgemein zur Datentreuhand *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 59 ff.
[349] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 28; dort, S. 37 ff., auch zur Anwendung des Modells auf pay-as-you-drive und Ferndiagnose. Auch Martens/Mueller-Langer, Access to Digital Car Data and Competition in Aftersales Services, 2018, S. 18, weisen darauf hin, dass bei nur einem neutralen Server dessen Betreiber weiterhin Monopolpreise ansetzen könnte und befürworten ebenfalls ein Wettbewerbsmodell der Server.
[350] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 34 ff.
[351] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 24.

Hinsichtlich der Rahmenbedingungen und der Standardisierung erscheint ebenfalls eine regulatorische Unterstützung notwendig. So wäre die Zugangsmöglichkeit des Datentreuhänders und der Einsatz des Datenwächters durch den Gesetzgeber verpflichtend vorzugeben.[352] Der vzbv hat dazu im Hinblick auf das für 2024 geplante Mobilitätsdatengesetz konkrete Vorschläge gemacht.[353]

IV. Sektorspezifische Regelungsvorschläge der EU

Die EU-Kommission hat 2022 eine Initiative zur Änderung der VO 2007/715 idF VO 2018/858 gestartet. Dahinter steht die Überlegung, dass vor allem durch die Vernetzung der Fahrzeuge und den dadurch ermöglichten Fernzugriff und auf breiter Front die Entwicklung neuer Dienste und Geschäftsmodelle möglich macht.[354] Die bisherige Regelung wird einhellig als technisch veraltet angesehen, erfasst aber auch nur einen engen Bereich des Datenzugangs in der Wertschöpfungskette.

Die Initiative zielt auf eine sektorspezifische Konkretisierung der Anforderungen des DA-E. Als ein Grund für die Notwendigkeit sektorspezifischer Regelung werden die Unterschiede zwischen Fahrzeugmarken bei verfügbaren Daten und Zugangsarten und das enge Zusammenspiel zwischen Zugang und Sicherheitsmaßnahmen mit den jeweiligen Produkten angegeben.[355] In Ergänzung des DA-E wird daher darauf abgezielt, die Standardisierung von Daten zu fördern sowie den Zugriff auf Fahrzeugfunktionen und –ressourcen zu ermöglichen, und weiterhin einen fairen Wettbewerb auf Anschlussmärkten und bei Mobilitätsdiensten zu gewährleisten. Auch der Ausgleich mit Sicherheitsanforderungen ist sinnvoller sektorspezifisch zu regeln.

Die EU-Kommission hat drei Optionen zur Diskussion gestellt, die im Folgenden erläutert und bewertet werden sollen.

1. Option 1

Bei Option 1 geht es um die Ergänzung des DA-E um ein Recht auf gleichberechtigten Zugang zu Funktionen (z. B. der Möglichkeit im Fall gemeinsam genutzter Mobilitätsdienste, die Fahrzeugtür aus der Ferne zu entriegeln) und Ressourcen (z. B. der Möglichkeit für Navigationsdienste, Informationen über Geschwindigkeitsbegrenzungen am Armaturenbrett des Fahrzeugs anzuzeigen, oder der Möglichkeit zum Laden/Entladen von Batterien für auf Elektrofahrzeuge bezogene Dienstleistungen) für alle Beteiligten.[356] Ergänzend soll im Interesse der Transparenz eine Liste der zugänglichen Fahrzeugdaten, -funktionen und -ressourcen eines bestimmten Fahrzeugmodells oder einer bestimmten Fahrzeugversion von den Fahrzeugherstellern veröffentlicht oder auf andere Weise zur Verfügung gestellt und Berichtspflichten für Hersteller gegenüber zuständigen Behörden (z. B. die Typgenehmigungsbehörden und die Kommission) eingeführt werden. Auch das Verhältnis zwischen Zugangsrechten und Cybersicherheit soll geregelt werden.

Die Option greift einen der zentralen Defizite des DA-E auf, nämlich den nicht vorgesehenen Zugang zu Funktionen und Ressourcen. Damit würde der neben dem Datenzugang wichtige zweite Bereich erfasst, der für die Förderung des Wettbewerbs von Diensten auf den abgeleiteten und Anschlussmärkten erforderlich ist, und damit den Zugang von unabhängigen Dienstleistern erheblich in die Breite erweitern. Dies wäre allerdings bei einer Interpretation wieder eingeschränkt, die den „gleichberechtigten“ Zugang auf solche Funktionen beschränkt, die der Hersteller selbst am

[352] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 27, 34 ff. Vgl. auch *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 33 ff., 71, für das Datentreuhand-Modell.
[353] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 45.
[354] Vgl. Aufforderung zur Stellungnahme für eine Folgenabschätzung, Ref. Ares(2022)23022201-29/03/2022.
[355] Aufforderung zur Stellungnahme für eine Folgenabschätzung, Ref. Ares(2022)23022201-29/03/2022.
[356] Aufforderung zur Stellungnahme für eine Folgenabschätzung, Ref. Ares(2022)23022201-29/03/2022.

Anschlussmarkt anbietet.[357] Hier sollte jedenfalls klargestellt werden, dass auf Verlangen auch Zugang für neuartige Funktionen anderer Diensteanbieter zu gewähren wäre. Die Transparenzanforderungen hinsichtlich der zugänglichen Daten, Funktionen und Ressourcen können hilfreich sein, um Marktzutrittsschranken abzubauen. Was sie nicht direkt leisten können, ist die Herstellung von Interoperabilität zwischen den Herstellern. Ob die Anreize dazu ausreichend sind und dies der Markt ohne weitere Regulierung bewirken kann, ist zweifelhaft.

2. Option 2

In Option 2 sollen bei der Typgenehmigung eine Minimalliste von Daten, Funktionen und Ressourcen für den Fernzugang vorgelegt werden, die in einem bestimmten Format vorhanden sind. Eingeschlossen ist die „bidirektionale“ Kommunikation mit dem Fahrer über die Mensch-Maschine-Schnittstelle (HMI) des Fahrzeugs. sowie ein ständiger und sicherer Zugang zur On-Board-Diagnoseschnittstelle. Hinzu kommt die Regelung von Sicherheitsfragen für diese Maßnahmen.

Die zweite Option würde zusätzlich eine Verfügbarkeit eines Grundbestands von Daten, Funktionen und Ressourcen im Fernzugriff und in einem bestimmten Format ermöglichen. Damit wären explizit diejenigen Dienste ermöglicht, die nur im Fernzugriff zu erbringen sind und damit der Kreis der in den Wettbewerb einbezogenen Dienste gegenüber dem bisher auf Kabelzugriff begrenzten Zugang erweitert. Von großer Bedeutung wäre auch das Vorgeben eines bestimmten Formats. Damit wäre regulatorisch ein Teilaspekt der Interoperabilität abgedeckt. Dies kann zusätzlich zu Option 1 das markenübergreifende Angebot von Diensten erleichtern. Wichtig für die Reichweite der Verbesserung ist auch die Frage, ob die Liste herstellerspezifisch sein soll, was zu vermuten steht, oder herstellerübergreifend anzubieten ist, was der Standardisierung weiter förderlich wäre. Jedenfalls würde dem Fahrzeughersteller – anders als bei Option 1 - mit der Vorgabe eines Minimalbestands für den Zugriff auch die Entscheidung darüber abgenommen, welche Daten, Funktionen und Ressourcen der Hersteller anbietet, sondern diese läge bei der Zulassungsbehörde.

Mit dem Zugriff auf das HMI würde ein weiterer wichtiger Baustein für die Ermöglichung bestimmter Dienste einbezogen, die für die Herstellung eines fairen Wettbewerbs eine unabhängige Kommunikation mit dem Nutzer benötigen. Gleiches gilt für den ständigen Zugang zur OBD, was gegenüber dem jetzigen Zustand ebenfalls verbesserte Zugangsmöglichkeiten für unabhängige Diensteanbieter beinhalten würde.

Mit den erweiterten Zugriffsmöglichkeiten und der Minimalliste wäre ein bedeutender Teil der Gatekeeperfunktion der Hersteller aufgebrochen und ein Beitrag zum „Unlocking“ von Daten, Funktionen und Ressourcen geleistet.[358]

3. Option 3

Option 3 würde dies durch Vorschriften über die Verwaltung des Zugangs ergänzen. Dazu würden weitere Spezifikationen für alle Zugangsarten dahingehend aufgenommen, wie der Zugang erfolgen und kontrolliert werden würde.

Auch wenn weitere Einzelheiten insoweit nicht bekannt sind, würde man durch eine konkretere Regelung des Zugangs zur Standardisierung beitragen und noch besser die Umsetzung eines diskriminierungsfreien Zugangs gewährleisten können. Je nach konkreter Ausgestaltung könnte dies einen weiteren Beitrag dazu leisten, die Gatekeeperfunktion der Fahrzeughersteller zu beseitigen, indem deren Spielräume im verbleibenden Bereich der Art und Weise der Zugangsgewährung weiter beschränkt werden. Viel hängt aber von der konkreten Ausgestaltung ab, über die hier keine näheren

[357] Vgl. *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 7.
[358] Vgl. *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 7.

Informationen vorliegen. Zu vermuten steht, dass keine neutrale Plattform oder Verwaltung der Schnittstelle vorgeschrieben wird, so dass die Effekte hinsichtlich der Gatekeeper-Problematik nur beschränkt eintreten würden. Der IT-Sicherheit würde durch konkretere Regelungen gedient. Der bei einer konkreten Regelung entstehende Nachteil der Notwendigkeit häufigerer Aktualisierungen ist allgemein Kennzeichen des Technikrechts.

4. Bewertung des Vorschlags im Lichte des bestehenden Regulierungsrahmens

Ein bedeutender Teil der konstatierten Lücken des DA-E würde durch die verschiedenen Optionen graduell geschlossen. Dazu gehören vor allem der direkte Zugriff auf Funktionen, Ressourcen und das HMI, ebenso wie die Einräumung der Möglichkeit des Fernzugriffs.[359] Die Vorgabe eines Grundbestands in Option 2 erscheint dabei im Interesse der Rechtssicherheit und der effektiven Umsetzung vorteilhaft. Der funktionsbezogene Ansatz der sektorspezifischen Regelungen wurde bereits bei der Bestimmung der zugänglich zu machenden Daten gegenüber der Beschränkung auf Rohdaten im DA-E als vorteilhaft bewertet.[360] In Option 2 würde der funktionsorientierte Ansatz mit einer Konkretisierung kombiniert. Ein konkreter Mindestkatalog an Daten kann für mehr Klarheit und Rechtssicherheit im Einzelfall sorgen und die Durchsetzung erleichtern, soweit er Katalog weit genug gefasst ist. Allerdings geht dies auf Kosten der Flexibilität, so dass hier Updates erforderlich werden. Auch die Vorgabe bestimmter Formate dient der Interoperabilität sowie der Kostensenkung, was wiederum dem Wettbewerb und der Stärkung der Verbraucherstellung zugutekommt. Insoweit wäre Option 2 gegenüber Option 1 zu bevorzugen.

Klarzustellen wäre, dass vergleichbar zum DA-E der Zugang zu Funktionen und Ressourcen nur zu FRAND-Bedingungen zu gewähren ist, um zu verhindern, dass durch Gestaltung von Gebühren und Vertragsbedingungen die positiven Effekte kompensiert werden.[361] Auch sollte konkreter bestimmt werden, dass die behördlichen Vorgaben für die in die Minimalliste einzubeziehenden Daten, Funktionen und Ressourcen nicht nur die bestehenden Dienste abbilden, sondern auch Raum lassen für die Entwicklung neuartiger Dienste, die möglicherweise andersartige Daten und Funktionen benötigen.[362]

Ein weiterer Vorteil der Option 2 wäre, dass der Zugang von Behörden zu einem Mindestbestand konkret bezeichneter Arten von Informationen, die zu Zwecken des Umweltschutzes und der Verkehrssicherheit notwendig sind, gewährleistet wäre. Weiterhin würden detailliertere Regelungen zur Cybersicherheit dem Ausgleich zwischen IT-Sicherheit und Datenzugang zugutekommen. Wie das oben angeführte Beispiel der UNECE R155 und R156 zeigt, ist ein solcher Ausgleich gut möglich, kann aber am besten durch konkrete Anforderungen umgesetzt werden, wofür der die TypGVO der richtige Ort ist. Hier wäre letztlich Option 3 einschlägig.

Unklar bleibt, ob die Zugangsrechte entsprechend dem Ansatz der TypGVO direkt dem Diensteanbieter zustehen sollen, oder ob eine Umstellung auf das nutzerzentrierte Modell des DA-E mit der Kontrolle des Zugangs beim Nutzer erfolgen soll. Auch wenn das nutzerzentrierte Modell zum Aufbrechen der Gatekeeperfunktion der Fahrzeughersteller beitragen kann, ist angesichts dessen oben festgestellter Schwächen und der bereits in der bestehenden TypGVO praktizierten Ausgestaltung ein direkter Zugriff

[359] *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 9, betonen insoweit auch die Notwendigkeit, das Diensteanbieter Software im Fahrzeug installieren können müssen, um neue Dienste anzubieten, was man als Teil des Zugangs zu den Funktionen ansehen kann. Diese müsste sicherheitstechnisch zugelassen werden.
[360] S.oben C.III.1.c).
[361] Vgl. *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 8.
[362] *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 9: „For enabling a flourishing ecosystem of data-driven vehicle-related and mobility services, as much data as possible should be made available for ISPs".

der Diensteanbieter vorzugswürdig, wobei die Datenschutzrechte des Nutzers gewahrt bleiben müssten.[363] Für letzteres ist an die Integration eines herstellereigenen PIMS zu denken.

Ein direkter Zugangsanspruch der Diensteanbieter könnte einerseits den Ansatz des DA-E mit Zugangsansprüchen auch des Nutzers ergänzen, könnte aber in der Praxis zu Abstimmungsproblemen und einer gewissen Komplexität führen. Sinnvoller wäre es, wenn der nutzerorientierte Zugang des DA-E sektorspezifisch durch Direktansprüche der Diensteanbieter verdrängt würde. Damit würden die dargestellten Probleme vermieden, der Nutzer könnte indirekt von den Zugangsrechten der Diensteanbieter profitieren und die Möglichkeit des Zugangs unabhängig von der Initiative des Nutzers öffnet den Sekundärmarkt für weitere innovative Dienste und Produkte. Unabhängig von der Art der Zugangsgewährung blieben die Wahlmöglichkeiten des Nutzers erhalten, als sie oder er selbst bestimmen kann, welchen Dienst sie oder er nutzen will. Aber die Wahlmöglichkeiten könnten erweitert werden.

Offen ist wegen der unklaren Zweckregelung hinsichtlich der Datenverwendung die Frage, inwieweit der DA-E auch den Handel mit Daten auf Datenmärkten zulässt.[364] Dafür sind gute Argumente angeführt worden: die schwierige Abgrenzung zwischen ergänzendem Service und Wettbewerbsprodukt; die Schwierigkeit der Verifizierung der Herkunft der Daten in der weiteren Wertschöpfungskette; die Feststellung des Bestehens von Wettbewerb hinsichtlich der beschränkten Datenverwendung kann aufwändig sein.[365] Eine vollständige Öffnung der Daten auch für direkten Wettbewerb auf dem Sekundärmarkt schafft auch mehr Freiraum für neue Services und Geschäftsmodelle, die nicht vorab benannt und festgelegt werden müssen.[366] Innovation kann sich aus dem Markt heraus entwickeln. Es lässt sich jedoch dann auch nicht ausschließen, dass die Daten für den Wettbewerb auf dem Primärmarkt genutzt werden. Der DA-E möchte das durch die verschiedenen Begrenzungen der Datenverwendung ausschließen. Es ist aber fraglich, ob sich überhaupt noch eine klare Grenze zwischen Sekundär- und Primärmarkt ziehen lässt, geschweige denn, wie sich entsprechende Verwendungen kontrollieren lassen. Dies bedarf weiterer vertiefter ökonomischer Forschung.

Es bleibt weiter das Problem, dass der Zugriff jeweils herstellerspezifisch und dadurch für jeden Hersteller ein separater Zugriff erforderlich ist. Dies erhöht die Kosten wegen unterschiedlicher Formate und Standards und kann zur Konzentration auf einen eingeschränkten Kreis von Herstellern zu Lasten von Konsumentenwahl und Wettbewerb führen. Vor allem wird auch die Gatekeeperfunktion der Hersteller nicht vollständig aufgebrochen. Die Vorschläge zur Überarbeitung der TypGVO bleiben im Rahmen des extended vehicle-Konzepts, aber kombiniert mit stärkerer Regulierung der Zugangsbedingungen, etwa im Rahmen eines FRAND-Ansatzes, sowie der Notwendigkeit des Angebots eines Minimalbestands an Daten, Funktionen und Ressourcen, bestimmt durch die Zulassungsbehörde.[367] Diese Lösung könnte zwar für eine Übergangszeit sinnvoll sein, langfristig wird jedoch ein Aufbrechen der Exklusivkontrolle der Hersteller durch eine unabhängige Datentreuhand

[363] *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 11, weisen auf die Notwendigkeit des Abschlusses eines Vertrags zwischen Nutzer und Hersteller im Rahmen des DA-E hin, und sehen hier die Notwendigkeit der Stärkung des Verbraucherschutzes. Allerdings kann hier die AGB-Kontrolle, vielleicht unter Bezugnahme auf Ch. IV des DA-E, der zwar für B2B gilt, aber eine gewisse ergänzende Leitbildfunktion entfalten kann, schon einen wesentlichen Beitrag leisten.
[364] S.oben unter C.II.1.c)bb)4(c).
[365] *Graef/Husovec*, Seven Things to Improve in the Data Act Proposal, 2022, S. 7.
[366] Für eine entsprechende Freigabe im Interesse der Sicherstellung der Wirksamkeit *Geiregat*, The Data Act: Start of a New Era for Data Ownership?, 2022, Rn. 21.
[367] Vgl. auch *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 6 f. *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 70, verweisen auf das Problem eine zu engen Bestimmung des Datenzugangs auch unter FRAND-Bedingungen ebenso wie hinsichtlich der Interoperabilität.

(data shared server) oder unabhängige OBD-Plattformen als überlegene Lösung im Sinne von Wettbewerb und Innovation anzusehen sein.[368]

Eng damit zusammen hängt die Möglichkeit der Hersteller, den Zugang zumindest technisch zu kontrollieren und gleichzeitig gebündelt Dienste auf dem Sekundärmarkt anzubieten. Um das zu verhindern, ist ein vom Hersteller unabhängiger Zugriff auf Daten und Funktionen sowie eine direkte Kommunikation mit dem Nutzer erforderlich. Letzteres wird zwar von Option 2 schon vorgesehen, allerdings ist nicht gewährleistet, dass diese vom Hersteller nicht mehr überwacht werden kann (Business Monitoring). Gleiches gilt für die Genehmigung einzusetzender Software sowie die sicherheitstechnische Zustimmung zum Zugang von Diensten zum Fahrzeug.

Abhilfe schaffen kann hier der Einsatz des Prinzips der „Separation of Duties".[369] Dabei kann die Identifizierung des Fahrzeugeigentümers und Autorisierung von Dienstleistern durch eine neutrale Stelle, etwa einen Datentreuhänder, vorgenommen werden, während der Zugriff selbst über den Hersteller erfolgt. Gleichfalls kommt eine solche Gestaltung der Lösung der datenschutzrechtlichen Problematik entgegen, die wegen des primär wettbewerbspolitischen Blickwinkels der TypGVO bisher noch nicht hinreichend berücksichtigt wurde. Die Datentreuhand kann dazu mit dem PIMS-Einsatz verknüpft werden.[370]

Flankierend müssen auch die für die Öffnung des Zugangs zu Funktionen und Ressourcen notwendige Standardisierung und Interoperabilität durch weitere Maßnahmen gefördert werden. Dies kann der Integration des Mobilitätssektors sowie Anreizen für innovative Dienste zugutekommen.[371]

V. Regelungsoptionen und Handlungsempfehlung

Die insgesamt sehr komplexe Problemlage konnte im vorliegenden Rahmen nicht in allen Einzelheiten analysiert werden, und auch die Schlussfolgerungen, für die sich ergebenden Regulierungsnotwendigkeiten müssen sich auf Eckpunkte konzentrieren. Sinnvollerweise ist dabei an die verschiedenen im Mittelpunkt der Diskussion stehenden Konzepte anzuknüpfen. Vor dem Hintergrund des Gesamtüberblicks über den regulatorischen Rahmen sollen im Folgenden die drei Konzepte daraufhin untersucht werden, wie die noch bestehenden Defizite durch regulatorische Maßnahmen kompensiert werden können. Darauf aufbauend sollen Handlungsempfehlungen begründet werden.[372]

1. Regelungsoptionen

a) Reguliertes Extended vehicle-Konzept

Die Hersteller bestehen auf dem Ausbau des derzeitigen extended vehicle-Konzept und führen dafür vor allem Sicherheitsprobleme bei offenen Plattformen an.[373] Diese sind nicht ganz von der Hand zu

[368] Vgl. *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 4; TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 171; *Martens/Mueller-Langer*, Access to Digital Car Data and Competition in Aftersales Services, 2018, 2018.

[369] Eine Ausprägung der Funktionstrennung stellt das Modell des Mobilitätsdatenwächters dar, vgl. *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung, 2022, S. 23 ff.

[370] . Vgl. auch *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 73 f.

[371] Vgl. *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 10, die gleichzeitig darauf hinweisen, dass es einen Zielfkonflikt zwischen Produktdifferenzierung und Wettbewerb auf dem Sekundärmarkt gibt.

[372] Vgl. auch TLR, fka, Study on Access to Data -Lot 1 on behalf of the European Commission, 2021, nur verfügbar als Kopie der Präsentation. Diese hatte das Ziel, eine "toolbox" für policy options zu entwickeln, verschiedene Optionen zu bewerten und Empfehlungen auszusprechen. Die beiden herausgearbeiteten Empfehlungen entsprechend den hier empfohlenen Optionen 1 a) und c), wobei sehr detailliert einzelne Maßnahmen spezifiziert werden.

[373] VDA, Position Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten, 2016, S. 1, abrufbar unter https://www.forschungsinformationssystem.de/servlet/is/4741517/.

weisen, und die entsprechenden Sicherheits- und Interoperabilitätsstandards bedürfen weiterer Entwicklungsarbeit.

Für eine bestmögliche Gestaltung im Rahmen dieses Konzepts wäre eine Lösung geeignet, bei der die Hersteller die Daten auf einen externen Server unter ihrer Kontrolle übertragen. Dies würde auch neuere Konzepte wie Mobility Data Space und Catena-X umfassen, bei denen es grundsätzlich bei der Kontrolle durch die Hersteller bleibt. Alternativ bestünde Zugang über eine herstellerkontrollierte Schnittstelle im Fahrzeug, wie bei ADAXO. Zugleich sollte regulatorisch der Zugang zu den Daten unter FRAND-Bedingungen festgelegt werden.[374] Dies ließe sich unter die Überwachung durch eine Aufsichtsbehörde stellen.[375]

Erfasst würde der gesamte Bereich möglicher Dienste auf dem Sekundärmarkt. Des Weiteren wäre auch der technische Zugang (remote access) zu den Funktionen des Fahrzeugs sowie zum HMI zu FRAND-Bedingungen zu gewährleisten. Damit würde auch ein Direktzugriff auf das Fahrzeug verbunden. Dies ist insbesondere von Bedeutung, als durch vorinstallierte Funktionen eine zunehmende Herstellerbindung durchgesetzt werden soll. Die Bedingungen des Zugriffs sollten vom Regulator festgelegt werden und Standardisierung der technischen Schnittstellen und des Sicherheitskonzepts einschließlich Zertifizierung der Diensteanbieter beinhalten.[376] Entsprechend könnte, soweit durch das Sicherheitsinteresse begründet, der Zugang auf autorisierte und zertifizierte Dienste beschränkt werden.

Verfeinert werden könnte dies durch ein standardisiertes Rollenkonzept, das die Tiefe des Zugriffs in vier Stufen reguliert: Lesen, Löschen, Software aufspielen, neue Komponenten aufspielen.[377] Damit ließe sich ein differenzierter Zugang implementieren. Allerdings müsste auch hier die Zuordnung der Zugangsbegehrenden zu den verschiedenen Rollen bestimmt werden. Hier müssten vermieden werden, dass diese Bestimmung den Fahrzeugherstellern zukommt.

Eine entsprechende Regulierung könnte an den Vorschlag zur Erneuerung der TypGVO anknüpfen und eine Liste von zugänglich zu machenden Daten und Funktionen mit einzuräumendem Echtzeitzugriff beinhalten. Die entsprechenden Listen sollten öffentlich verfügbar sein. Es sollte klargestellt werden, dass Zugang jeweils unter FRAND-Bedingungen zu gewährleisten ist und auch für vom Fahrzeughersteller selbst nicht genutzte Daten und Dienste gelten soll, um Innovationen nicht zu behindern. Die Regelungen zur Stärkung fairer Vertragsbedingungen im DA-E im Verhältnis B2B sollten ergänzend Anwendung finden. Wegen der Schwächen des nutzerzentrierten Ansatzes wäre eine Abkehr vom DA-E insoweit sinnvoll, als dem Anbieter auf dem Sekundärmarkt direkte Ansprüche gegen den Hersteller eingeräumt werden sollten.[378] Dies würde auch der Entstehung wettbewerbsrechtlich begründeter Zugangsrechte als komplementärem Regulierungsansatz entsprechen, wie sie bereits durch das GWB-Digitalisierungsgesetz 2021 im deutschen Recht verankert wurden, deren Art und Durchsetzbarkeit allerdings noch abzuwarten bleibt.[379] Insoweit wäre eine sektorspezifische Spezialregelung zum DA-E sinnvoll, wie es oben bereits für die TypGVO empfohlen wurde.

Es bliebe aber auch bei einer entsprechenden Ausgestaltung des extended vehicle-Konzepts bei der grundsätzlichen technischen Zugangskontrolle durch die Fahrzeughersteller. Das damit weiter mögliche Business Monitoring ist zwar im DA-E bereits weitgehend untersagt, wäre aber technisch-strukturell weiterhin nicht ausgeschlossen. Weitergehend wäre daher auch im Rahmen des extended-vehicle-Konzepts an die Einführung einer Funktionstrennung zu denken. Entsprechend dem Modell des

[374] Vgl. eingehend *Specht-Riemenschneider/Kerber*, Designing Data Trustees, S. 68 f.
[375] Vgl. auch TLR 2021, fka, Study on Access to Data - Lot 1 on behalf of the European Commission, 2021, nur verfügbar als Präsentation, Folie 16.
[376] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 69.
[377] Information/Erkenntnis aus dem Interview mit dem ADAC e.V. am 09.01.2023.
[378] Vgl. *Drexl*, Connected Deveices – An Unfair Competition Law Approach to Connected Devices, MPI Research Paper 20-22, S. 38 ff.
[379] S. auch *Kerber*, Journal of Competition Law & Economics 15 (4), 2019, 381 (390 ff.).

„Mobilitätswächters“ wäre der technische Zugang in den Händen eines Datentreuhänders, die Autorisierungsfunktion in den Händen des Mobilitätswächters.[380] Der Datentreuhänder diente dazu, die technische Kontrolle aus der Hand der Fahrzeughersteller zu nehmen und gleichzeitig der IT-Sicherheit zu dienen sowie eine frühzeitige Anonymisierung von Daten im Interesse des Verbrauchers zu bewirken. Der Mobilitätsdatenwächter stellte die Neutralität der Zugangsgewährung sicher und diente gleichzeitig zur Einbindung von PIMS, um Wahrnehmung der datenschutzrechtlichen Befugnisse der Nutzer zu gewährleisten.

Beim Fahrzeughersteller verbliebe noch die Funktion, die Erfüllung der IT-Sicherheitsanforderungen zu überprüfen. Dieser wäre bei positiver Prüfung verpflichtet, den Zugang für den Datentreuhänder freizugeben.[381] Die Sicherheitsanforderungen müssen eindeutig und verhältnismäßig sein. Nach dem Modell würde der Hersteller die Kontrolle über den Datenzugang verlieren. Es müsste aber auch technisch sichergestellt werden, dass der Hersteller keinen direkten Datenzugang mehr hat, sondern wie die anderen Zugangsberechtigten Zugang nur über den Datentreuhänder erhält. Die wesentlichen Punkte dieses Modell müssten regulatorisch verpflichtend festgeschrieben werden.

b) Data Shared Server und Datentreuhand

Das Data Shared Server-Konzept würde dem Nutzer die direkte Kontrolle ermöglichen und aufgrund der Neutralität der Plattform den Herstellern insoweit die Zugangskontrolle entziehen. Diese Lösung könnte auf dem DA-E aufsetzen, wobei die neutrale Instanz bzw. die Datentreuhand, die die Plattform verwaltet und kontrolliert, als Dateninhaber i.S. des DA-E anzusehen wäre. Ein direkter Zugangsanspruch der Diensteanbieter, wie zur Überarbeitung der TypGVO vertreten, wäre hier insoweit nicht zwingend notwendig, als die Initiative zum Zugang hier vor allem von den Diensteanbietern ausgehen würde, nicht vom Nutzer wie im Modell des DA-E, und damit die Schwächen des nutzerzentrierten Modells weitgehend vermieden würden. Dieser behielte aber die Letztentscheidung über die Zugangsgewährung, was zur Vernachlässigung der Zugänglichkeit von Daten im öffentlichen Interesse führen könnte,

Eine eher mit dem Überarbeitungsvorschlag zur TypGVO kompatible Lösung wäre hier die Einschaltung einer Datentreuhand. Diese könnte im Rahmen des Prinzips der Funktionstrennung auch noch einmal in eine Datentreuhand und einen Datenwächter aufgespalten werden, wie es das Modell des vzbv vorsieht. Dabei würde wiederum der Gesetzgeber bzw. die damit beauftragte Regulierungsbehörde über die zugänglich zu machenden Daten und Zwecke entscheiden und Datenzugangsregeln festlegen. Dies schließt nicht grundsätzlich aus, dass auch die Wünsche des Nutzers für einen Datenzugang Dritter berücksichtigt werden. Das müsste auch die Wahrung des Datenschutzes des Nutzers beinhalten. Darüber hinaus ließe sich hier aber unternehmens- und zweckbezogen differenzieren.[382] Für öffentliche Zwecke wie Verkehrssicherheit, Umweltschutz und Unfallforschung könnten anonymisierte Daten bereitgestellt werden. Diese könnten auch auf Datenmärkten frei zur Verfügung gestellt werden. Dem Geheimnisschutz würde durch die im DA-E nunmehr vorgesehen Spezifizierungspflicht der Hersteller Rechnung getragen.

Insoweit besteht Regulierungsbedarf nicht nur hinsichtlich der Verpflichtung zur Einführung eines solchen Konzepts, sondern auch hinsichtlich der Zugangsregeln. Der entscheidende Unterschied zum extended vehicle-Konzept ist die Verlagerung der Datenzugangskontrolle auf eine neutrale Plattform bzw. auf die Datentreuhand. Dies ist in sehr engen Grenzen bereits in der eCall-VO 2015/758 umgesetzt

[380] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S. 23 ff.
[381] *Reiter/Methner/Schenkel*, Gutachten Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung, 2022, S.28.
[382] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 72.

(vgl. Ziff. E.I.3). Nimmt man aber dem Nutzer die Kontrolle über den Datenzugang, wäre diese Ausgestaltung eher mit dem Vorschlag zur TypGVO kompatibel und könnte darauf aufsetzen.

Als entscheidender Nachteil dieser Lösung bleibt, dass kein Zugriff auf die Funktionen des Fahrzeugs sowie das HMI gewährt würde. Zwar ließe sich auch der Zugang entsprechend über die Regulierung einer Treuhandlösung einschließlich der dazu erforderlichen Standardisierung der technischen Schnittstellen sowie der Sicherheitslösungen erreichen. Dies würde aber über die Grundidee der Bereitstellung eines neutral betriebenen externen Servers hinausgehen und direkten Zugriff auf das Fahrzeug beinhalten.

c) OTP

Beim OTP-Modell als Ausprägung des „On-Board Application Platform"-Grundmodells wird die offene und interoperable Plattform in das Fahrzeug selbst integriert, über die die externen Dienstleister nicht nur direkt und gleichberechtigt Zugang zu Daten bekommen, sondern auch zu den Funktionen und dem HMI.[383] Damit wäre die Gatekeeper-Position des Herstellers komplett beseitigt und Nutzer und/oder Diensteanbieter bekämen die direkte Kontrolle auch über die Funktionen sowie einen Echtzeitzugriff auf die Daten. Das vernetzte Fahrzeug würde zum offenen System.[384] Die Funktionstrennung wäre strukturell „eingebaut" und der Fahrzeughersteller auf die technische Ermöglichung der Voraussetzungen für den Zugang beschränkt. Diese Lösung wäre unter den Gesichtspunkten eines fairen und unverzerrten Wettbewerbs und der bestmöglichen Förderung von Innovation vorzugswürdig.

Dies machte für das gesamte System Standardisierung und Interoperabilität von Schnittstellen und Sicherheitsstandards einschl. Zertifizierung notwendig, aufbauend auf UNECE R155.[385] Zu beachten ist auch, dass bei der Standardisierung alle beteiligten Stakeholder angemessen einbezogen werden sollten.[386] Hier wäre auch eine Aufgabe für das Kartellrecht (vgl. Ziff. E.I.5).

Teil des Konzepts wäre ein direkter Zugriff dritter Diensteanbieter auf Daten und Funktionen über API-Schnittstellen. Das sollte die Möglichkeit zur Installierung von Software im Fahrzeug einschließen, nach sicherheitstechnischer Autorisierung von Diensteanbieter und Software durch unabhängige Instanzen, etwa nach dem Modell von SERMI.[387] Die Fahrzeughersteller müssten dabei die Kompatibilitätsvoraussetzungen schaffen. Die Dritt-Software sollte - vom Hersteller ungehindert und ohne Überwachungsmöglichkeit - mit dritten Servern kommunizieren können. Die Zugriffsmöglichkeiten der Software auf interne Ressourcen könnten entsprechend der Funktion des Diensteanbieters abgestuft werden. Eng damit zusammenhängend sollte die direkte Funktion des Drittanbieters mit dem Nutzer über das HMI sichergestellt werden. Das könnte auch Wahlmöglichkeiten des Nutzers hinsichtlich des Verbindungsdiensteanbieters einschließen. Die Förderung der notwendigen Standardentwicklung und –weiterentwicklung wäre eine regulatorische Aufgabe.

Die Entscheidung über den Datenzugang wäre dann dem Nutzer überlassen und würde basieren auf einem klar geregelten Zugangs- und Berechtigungskonzept für Daten, Funktionen und Ressourcen, wie es bei S-OTP vorgesehen ist. Dies lässt sich etwa umsetzen nach dem Prinzip eines App-Stores, wonach dem Nutzer alle zugelassenen Anwendungen angezeigt werden und er auswählen kann. Durch

---

[383] Dies entspräche Policy option 3 bei TRL fka, Study on Access to Data -Lot 1 on behalf of the European Commission, 2021, nur verfügbar als Präsentation, Folie 19 ff.

[384] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 76.

[385] Zur Standardisierung von Daten, Funktionen und HMI vgl. Aftermarket Alliance, Creating a level playing field for vehicle data access: Secure on-board Telematics Platform Approach, 2021, S. 40 ff.

[386] Vgl. *Kerber/Gill*, jipitec 2019, 244, 255 Rn. 29 S. auch TypGVO 2018/858, Erwägungsgrund. 54 S. 3, wonach CEN sicherstellen sollte, dass alle beteiligten Interessen von Herstellern und unabhängigen Diensteanbietern berücksichtigt werden. Zu ergänzen wären noch die Verbraucherinteressen.

[387] Vgl. Nr. 4 Delegierte Verordnung (EU) 2021/1244 zur Änderung des Anhangs X der Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates hinsichtlich des standardisierten Zugangs zu Fahrzeug-OBD-Informationen und zu Reparatur- und Wartungsinformationen sowie der Anforderungen und Verfahren für den Zugang Sicherheitsinformationen des Fahrzeugs, ABl. L 272/16 v. 20.5.2021.

Auswahl der App bucht er den Dienst und kann gleichzeitig der Nutzung seiner Daten datenschutzkonform zustimmen.[388]

Allerdings könnten sich bei vollständiger Überlassung des Zugangs an den Nutzer Nachteile für den Datenzugang zugunsten öffentlicher Interessen ergeben. Ergänzend wäre insoweit der Einsatz eines Datentreuhänders möglich, der das Datenmanagement für den Nutzer übernimmt und diesem entsprechende optimale Wahlmöglichkeiten bereitstellt.[389] Weitergehend könnte dieser auch die Bereitstellung bestimmter Informationen von öffentlichen Interesse Verkehrssicherheit, Umweltschutz) für staatliche Institutionen sicherstellen. Alternativ könnte dieser Zugriff aber auch regulatorisch vorgesehen werden.

Die Eckpunkte müssten regulatorisch verankert werden, einschließlich der Integration der Plattform in das Fahrzeug. Die Regulierung des Konzepts könnte auf dem Vorschlag zur Überarbeitung der TypGVO aufsetzen, etwa im Rahmen einer Konkretisierung von Option 3. Allerdings würde das Konzept darüber hinausgehen, indem den Herstellern jegliche Kontrolle über die Plattform entzogen würde. Beließe man es bei der Nutzerkontrolle, so wäre eine Umsetzung im Rahmen von Art. 3 DA-E denkbar. Dies könnte flankiert werden durch eine inhaltliche Erweiterung des Zugangs öffentlicher Stellen auf Informationen im öffentlichen Interesse in Kapitel V DA-E.

2. Handlungsempfehlung

Im Einklang mit den vorhandenen Studien gelangt auch die vorliegende Untersuchung zu dem Ergebnis, dass langfristig eine Gestaltung nach dem Konzept der offenen „on-board-application“ die besten Ergebnisse für die Förderung des Wettbewerbs auf Sekundärmärkten und Innovation bringen wird.[390] Die bisher ausführlichste Studie der EU-Kommission kam ebenfalls zu dem Ergebnis, dass das OTP-Konzept unter dem Gesichtspunkt „fairer und unverzerrter Wettbewerb“ die beste Lösung darstelle. wobei eine Reihe von möglichen Politikmaßnahmen diskutiert wurde.[391] Die Studie ging auch davon aus, dass ohne weitere regulatorische Maßnahmen das extended vehicle-Konzept von der Automobilindustrie durchgesetzt würde, zumal insoweit auch eine ISO-Standardisierung vorangetrieben wurde.

Die EU-Kommission hatte in der Folge zunächst keine direkte Initiative ergriffen. Der DA-E mit der Öffnung für sektorspezifische Regelungen hat aber eine neue Dynamik erzeugt, die zu einer neuen regulatorischen Initiative genutzt und mit der Initiative zur Erneuerung der TypGVO verbunden werden könnte. Einigkeit herrscht, abgesehen von den Fahrzeugherstellern, insoweit, dass zur Erreichung des Ziels weitergehende gesetzgeberische Maßnahmen erforderlich sind. Offenheit und Sicherheit sind kein Gegensatz.[392]

Da die OTP-Lösung wegen der umfangreichen Standardisierungsnotwendigkeiten und Sicherheitsanforderungen aber nur langfristig zum Einsatz gebracht werden kann, sollte kurzfristig die Lösung C.V.1.a) („Reguliertes Extended vehicle-Konzept“) verfolgt werden, und die Öffnung des Zugangs unter FRAND-Bedingungen von den Daten schrittweise auch auf Funktionen und HMI ausgeweitet werden.[393] Dazu könnte eine den DA-E ergänzende und teilweise verdrängende sektorspezifische Regelung dienen. Diese ließe sich im Rahmen der Überarbeitung der TypGVO

---

[388] Gemeinsames Positionspapier „Sicherer Zugang zum vernetzten Fahrzeug für den Aftermarket, 9/2021, https://www.gva.de/files/dokumente/VernetztesFahrzeug.pdf, S. 2.

[389] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 76 f., gehen von der Kontrollmöglichkeit durch den Nutzer aus und wollen nur für die Verpflichtung zur Bereitstellung bestimmter Daten an öffentliche Institutionen einen Datentreuhänger einsetzen, der dann Aggregierung von Daten durchführen kann.

[390] *Specht-Riemenschneider/Kerber*, Designing Data Trustees,S. 77 ff.;TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 170; *Kerber/Gill*, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, S. 11 f.; TLR 2021, fka, Study on Access to Data -Lot 1 on behalf of the European Commission, 2021, nur verfügbar als Präsentation, Folie 16 ff..

[391] TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 165 ff.

[392] TRL, Access to In-vehicle Data and Resources – Final Report, 2017, S. 8 f.

[393] „Evolution“, *Kerber/Gill*, Jipitec 2019, 244, 256 Rn. 30.

umsetzen. Sollte diese auf europäischer Ebene scheitern, erscheint auch eine entsprechende nationale Regelung möglich. Das würde allerdings eine entsprechende Öffnungsklausel im DA-E voraussetzen.

Offen bleibt auch die Entwicklung und konkrete Umsetzung eines Europäischen Mobilitätsdatenraums als Alternative oder weitergehende Option.[394] Auch insoweit erscheint das Modell der offenen Plattform am besten anschlussfähig.

*****

[394] Aufforderung zur Stellungnahme zu einer Initiative, Mitteilung der Kommission über die Schaffung eines gemeinsamen europäischen Mobilitätsdatenraums, Ref. Ares(2022)7735749 - 09/11/2022, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13566-Verkehrsdaten-Schaffung-eines-gemeinsamen-europaischen-Mobilitatsdatenraums-Mitteilung-_de.

Literaturverzeichnis

Stellungnahmen und Positionspapiere

- Alliance for the Freedom for CAR Repair in the EU, The Data Act – Analysis from the perspective of the Automotive Aftermarket & Mobility Services Sector AFCAR Position paper, 9th May 2022, abrufbar unter https://static1.squarespace.com/static/620fb46a5ce1cb523d888332/t/62947ec7456c296566000e04/1653898952510/Data+Act+-+AFCAR+Position+Paper+-+2022+05+09+-+Fin.pdf
- Bewertungsbericht der Kommission über die Anwendung der Verordnung (EU) Nr. 461/2010 (Kfz-Gruppenfreistellungsverordnung) vom 28.5.2021, COM(2021) 264 final, abrufbar unter https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)264&lang=en.
- COMMISSION STAFF WORKING DOCUMENT on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, SWD(2017) 2 final vom 10.1.2017, abrufbar unter https://op.europa.eu/de/publication-detail/-/publication/30f7e8aa-d808-11e6-ad7c-01aa75ed71a1.
- EDPB, EDPB-EDPS Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted 4 May 2022, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en
- EDPS, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0 vom 9. März 2021, abrufbar unter https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf
- European Data Protection Board, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0 vom 9. März 2021, abrufbar unter: https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf.
- Ergebnispapier „Industrie 4.0 – Kartellrechtliche Betrachtungen“ des Bundesministerium für Wirtschaft und Energie (BMWi) aus 02/2021, S. 22, abrufbar unter https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/Kartellrechtliche-Betrachtungen.pdf?__blob=publicationFile&v=5.
- FIGIEFA, Commission Communication on “Free Flow of Data” - Input from the Independent Automotive Aftermarket, 2016
- Gemeinsames Positionspapier verschiedener Verbände aus dem Mobilitätssektor „Sicherer Zugang zum vernetzten Fahrzeug für den Aftermarket“ aus 09/2021, abrufbar unter https://www.gva.de/files/Newsletter/PositionspapierFahrzeugdaten.pdf.
- Gesamtverband Autoteile Handel, Stellungnahme vom 13.02.2020, Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkung für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), abrufbar unter https://www.gva.de/files/dokumente/GVA-Stellungnahme_Ref_Entw_10__GWB-Novelle_final.pdf
- Konzept „ON-BOARD TELEMATICS PLATFORM SECURITY“ der Fédération Internationale de l’Automobile (FIA) aus 06/2020, abrufbar unter https://www.tuvit.de/en/news/downloads/fia-study/.

- Positionspapier „ACCESS TO VEHICLE DATA, FUNCTIONS AND RESOURCES„ des International Motor Vehicle Inspection Committe (CITA) aus 06/2022, abrufbar unter https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources/F3316299_en.
- Positionspapier „Connected Cars – Der Zugriff auf die Fahrzeugdaten“ des European Automobile Clubs (EAC) aus 11/2016, abrufbar unter https://www.eaclubs.org/de/connected-cars-access-to-vehicle-da.
- Positionspapier „Policy position on car connectivity” der Fédération Internationale de l’Automobile (FIA) aus 04/2016, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf.
- Positionspapier „Sicherer Zugang zum vernetzten Fahrzeug für den Aftermarket“ aus 09/2021, abrufbar unter https://www.gva.de/files/Newsletter/PositionspapierFahrzeugdaten.pdf;
- Positionspapier „Wettbewerb, Sicherheit und Transparenz: Daten im vernetzen Fahrzeug“ des Allgemeinen Deutschen Automobilclubs e.V. (ADAC) aus 12/2020, abrufbar unter https:////www.adac.de/-/media/pdf/motorwelt/positionspapier-daten-im-fahrzeug-final-12-2020.pdf.
- Pressemitteilung „Fragen und Antworten: Intelligente Verkehrssysteme“ der EU-Kommission vom 14.12.2021, abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/qanda_21_6727.
- Salesforce, Metastudie – Die Mobilität von morgen – Eine Herausforderung für die Automobilindustrie, 2020, abrufbar unter https://www.salesforce.com/content/dam/web/de_de/www/PDF/de-automotive-whitepaper-metastudies.pdf.
- Stellungnahme „Eingeschränkter Zugang zur OBD (On-Board-Diagnose) bei neueren Modellen“ des Allgemeinen Deutschen Automobilclubs e.V. (ADAC) aus 1/2022.
- Stellungnahme „Rechtsfragen der digitalisierten Wirtschaft: Datenrechte“ des Bitkom e.V. aus 09/2019, abrufbar unter https://www.bitkom.org/sites/default/files/2019-09/bitkom-stellungnahme-zu-datenrechten_langfassung_final_0.pdf.
- Stellungnahme des Allgemeinen Deutschen Automobilclubs e.V. (ADAC) zum Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung („Datengesetz“) aus 05/2022, abrufbar unter https://assets.adac.de/image/upload/v1660828122/ADAC-eV/KOR/Text/PDF/202205_ADAC_Stellungnahme_VO_Datengesetz_final_sxj2t8.pdf.
- Stricker, K./Wegener, R./Anding, M., Big Data revolutioniert die Automobilindustrie. München: Bain & Company, abrufbar unter http://www.bain.de/Images/Bain-Studie_Big%20Data%20revolutioniert%20die%20Automobilindustrie_FINAL_ES.pdf.
- VDA-Konzept für den Zugriff auf fahrzeuggenerierte Daten aus 01/2022, abrufbar unter https://www.vda.de/dam/jcr:2026d593-4515-4c7c-8eef-7bae3597ad78/VDA_5690_Positionspapier_ADAXO_RZ.pdf?mode=view.
- VDA. Position Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten, 2016, https://www.forschungsinformationssystem.de/servlet/is/474151/
- Vogt, Joerg Oliver, Geschäftsmodelle für das vernetzte Fahrzeug – Klassifikation, Angebot und Nutzen für das mobile Arbeiten, HNU Working Paper Nr. 30, 2014.

Juristische Fachliteratur

- Aftermarket Alliance, Creating a level playing field for vehicle data access: Secure on-board Telematics Platform Approach, 2021, abrufbar unter https://www.fiaregion1.com/wp-content/uploads/2021/03/2021-02-S-OTP-Paper-vFin.pdf

- Arzt, Clemens / Kleemann, Steven / Plappert, Christian / Rieke, Roland / Zelle, Daniel: Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung, MMR 2022, S. 593 ff.
- Crémer, Jacques/de Montjoye, Yves-Alxandre/Schweitzer, Heike: Competition Policy for the Digital Era, Report for the EU Commission, Final Report, 2019, abrufbar unter https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.
- Drexl, Josef: Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation BEUC, Brussels, 2018, abrufbar unter https://www.beuc.eu/sites/default/files/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.
- Drexl, Josef, u.a: Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), abrufbar unter https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content.
- Drexl, Josef: Neue Regeln für die Europäische Datenwirtschaft?, NZKart 2017, S. 415 ff.
- Ducuing, Charlotte/Margoni, Thomas/Schirru, Luca: White Paper on the Data Act Proposal, CiTiP Working Paper 2022, 26 October 2022, abrufbar unter https://openfuture.eu/wp-content/uploads/2022/10/CiTiP_WhitePaperDataAct.pdf.
- Gatzke, M. / Motzek, C. / Schneider, M. / Weigelin, L. / Sommer, C. / Stahl, K. / Engels, G. / Gries, S. / Gruhn, V. / Hesenius, M. / Ollesch, J. / Patalas, M. / Ide, C. / Wietfeld, C.: Fahrzeugvernetzung revolutioniert Mobilität. Perspektiven, Chancen und Herausforderungen für NRW. Institut SIkoM+; Bergische Universität Wuppertal, abrufbar unter http://ikt.nrw.de/fileadmin/user_upload/Dokumente/Fahrzeugvernetzung_revolutioniert_Mobilitaet_gestaltet.pdf.
- Geiregat, Simon: The Data Act: Start of a New Era for Data Ownership? (September 8, 2022), abrufbar unter https://ssrn.com/abstract=4214704.
- Gill, Daniel: The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources (May 16, 2022), abrufbar unter https://ssrn.com/abstract=4115443.
- Graef, Inge and Husovec, Martin: Seven Things to Improve in the Data Act (March 7, 2022), abrufbar unter https://ssrn.com/abstract=4051793.
- Greß, Sebastian / Springborn, Florian: Datenschutz bei der Fahrzeugentwicklung – Was hat der Datenschutzbeauftragte mit „Design" zu tun?, in: Stiftung Datenschutz (Hrsg.), Datenschutz im vernetzen Fahrzeug, 2020, S. 55 ff.
- Hansen, Sven: Kampf um die Datenhoheit, c´t 1/2022, 2.
- Hennemann, Moritz/Steinrötter, Bernd: Data Act – Fundament des neuen EU-Datenwirtschaftsrechts? NJW 2022, S. 1481 ff.
- Hoeren, Thomas / Böckers, Michael: § 63a StVG und der Umgang mit Fahrzeugdaten beim hoch- bzw. vollautomatisierten Fahren, JurPC Web-Dok. 21/2020, Abs. 1 – 148, abrufbar unter https://www.jurpc.de/jurpc/show?id=20200021#fn3.
- Höppner, Thomas / Weber, Jan Markus: Die Modernisierung der Missbrauchskontrolle nach dem Referentenentwurf für eine 10. GWB-Novelle, K&R 2020, S. 24 ff.
- Huerkamp, Florian / Nuys, Marcel: Datenzugang nach § 19 Abs. 2 Nr. 4 GWB n.F. – Geglückte „Klarstellung"?, NZKart 2021, S. 327 ff.
- Karsten, Benedikt / Wienroeder, Marie, Der Entwurf des Data Act – Auswirkungen auf die Automobilindustrie, RAW 2022, S. 99 ff.
- Käseberg, Thorsten: Wettbewerbspolitik in dieser Legislaturperiode: 10. GWB-Novelle und Kommission Wettbewerbsrecht 4.0, NZKart 2018, S. 441 ff.

- Kerber, Wolfgang / Gill, Daniel: Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC), 2019, 10(2), S. 244 ff.
- Kerber, Wolfgang: Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, Jipitec 2018, S. 310 ff.
- Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives (Second Version) (July 18, 2022). Available (revised) at: GRUR International, ikac107, abrufbar unter https://ssrn.com/abstract=4080436.
- Kerber, Wolfgang: Data-sharing in IoT Ecosystems and Competition Law: The Example of Connected Cars, Journal of Competition Law & Economics, Volume 15, Issue 4, December 2019, S. 381 ff.
- Kerber, Wolfgang / Frank, Jonas Severin: Data Governance Regimes in the Digital Economy: The Example of connected cars, Working Paper 2017, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064794.
- Kerber, Wolfgang / Gill, Daniel: Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, Jipitec 2019, S. 244 ff.
- Kerber, Wolfgang / Gill, Daniel: Revision of the Motor Vehicle Type Approval Regulation: Analysis and Recommendations (July 27, 2022), abrufbar unter https://ssrn.com/abstract=4174028 oder http://dx.doi.org/10.2139/ssrn.4174028.
- Klink-Straub, Judith / Straub, Tobias: Data Act als Rahmen für gemeinsame Datennutzung, ZD-Aktuell 2022, 01076.
- Körber, Torsten: „Ist Wissen Marktmacht?“ Überlegungen zum Verhältnis von Datenschutz, „Datenmacht“ und Kartellrecht – Teil 1, NZKart 2016, S. 303 ff.
- Krämer, Jan: Digitale Selbstbestimmung durch Personal Information Management Systems?, 2022, abrufbar unter https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-4-kraemer-digitale-selbstbestimmung-durch-personal-information-management-systems.pdf.
- Kreutzer, Till / Lahmann, Henning / Schallaböck, Jan: Big Data. Eine Untersuchung des iRights.Lab im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), 2016, abrufbar unter https://www.divsi.de/wp-content/uploads/2016/01/Big-Data.pdf.
- Lorenzen, Birte: Geschäftsgeheimnisschutz und Data Act, ZGE 2022, S. 251 ff.
- Martens, Bertin / Mueller-Langer, Frank: Access to Digital Car Data and Competition in Aftersales Services (October 1, 2018), abrufbar unter: https://ssrn.com/abstract=3262807 oder http://dx.doi.org/10.2139/ssrn.3262807.
- Martens, Bertin / Mueller-Langer, Frank: Access to digital car data and competition in aftersales markets, JRC Digital Economy Working Paper, 2018-6, abrufbar unter: https://joint-research-centre.ec.europa.eu/system/files/2018-10/jrc112634.pdf.
- Metzger, Axel / Schweitzer, Heike: Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, S. 82 ff.
- Metzger, Jakob / Mischau, Lena: Neutrale Server – Datenschutz und Datenwirtschaft im vernetzten Fahrzeug, in: Stiftung Datenschutz (Hrsg.), Datenschutz im vernetzen Fahrzeug, 2020, S. 135 ff.
- Öksüz / Schulze / Rusch-Rodosthemnous / Scheibel: Connected Car nimmt Fahrt auf – Wohin steuert das Auto der Zukunft?, Verbraucherzentrale NRW, 2017, abrufbar unter https://www.bvdw.org/fileadmin/bvdw/upload/publikationen/digitale_transformation/Diskussionspapier_Connected_Cars_Geschaeftsmodelle.pdf.

- Peitz, Martin / Schweitzer, Heike: Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018, S. 275 ff.
- Rehbinder, Manfred: Rechtssoziologie, 8. Aufl., 2014.
- Reiter, Julius / Methner, Olaf / Schenkel, Bénédict / Kinzler, Sarah: „Neutrale Server“ für Fahrzeugdaten: Garant für Datenschutz und Datensicherheit am Beispiel des Fahrmodusspeichers, in: Stiftung Datenschutz, Datenschutz im vernetzten Fahrzeug, 2020, S. 153 ff.
- Roßnagel, Alexander/Hornung, Gerrit: Grundrechtsschutz im Smart Car, Wiesbaden 2019.
- Roßnagel, Alexander: Fahrzeugdaten – wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung, Zeitschrift für die Praxis der Verkehrsjuristen, 2014, S. 281 ff.
- Schmid, Alexander / Wessels, Ferdinand: Event Data Recording für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG, NZV 2017, S. 357 ff.
- Schönfeld, M., in: Hoeren, T. / Kolany-Raiser, B.: Big Data zwischen Kausalität und Korrelation, S. 63 ff.
- Schweitzer, Heike: Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, S. 569 ff.
- Louven, Sebastian: Datenmacht und Zugang zu Daten, NZKart 2018, S. 217 ff.
- Louven, Sebastian: Marktmacht durch Daten: Eine Analyse aus rechtswissenschaftlicher Perspektive, in: Specht-Riemenschneider, Louisa / Werry, Nikola /Werry, Susanne (Hrsg.), Datenrecht in der Digitalisierung, 2020, S. 779 ff.
- Specht-Riemenschneider, Louisa: Der Entwurf des Data Act, MMR 2022, S. 809 ff.
- Specht-Riemenschneider, Louisa: Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, S. 1040 ff.
- Specht-Riemenschneider, Louisa / Blankertz, Aline: Lösungsoption Datentreuhand: Datennutzbarkeit und Datenschutz zusammen denken, MMR 2021, S. 369 ff.
- Specht-Riemenschneider / Kerber, Wolfgang: Designing Data Trusteees – A Purpose-Based Approach, Berlin 2022, abrufbar unter https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d.
- Telle, Sebastian: Konditionenmissbrauch durch Ausplünderung von Plattform-Nutzerdaten, WRP 2016, S. 814 ff.
- Weber, Henri: Datenzugang nach dem Referentenentwurf der 10. GWB-Novelle, WRP 2020, S. 559 ff.
- Weisser, R. / Färber, C.: Rechtliche Rahmenbedingungen bei Connected Car. Überblick über die Rechtsprobleme der automobilen Zukunft, MMR 2015, S. 506 ff.
- Wegner, Anne C.: Neue Kfz-GVO (VO 461/2010) - des Kaisers neue Kleider? - Teil 1: die Anschlussmärkte, BB 2010, S. 1803 ff.
- Wegner, Anne C.: Neue Kfz-GVO (VO 461/2010) – Teil 2: Individuelle Beurteilung von Verträgen außerhalb der GVO auf den Anschlussmärkten, BB 2010, S. 1867 ff.
- Wendehorst, Christiane / Schwamberger, Sebastian: Zugang zu Kfz-Nutzerdaten im (zukünftigen) europäischen Datenrecht, DAR 2022, S. 541 ff.
- Wendt, Kai: Autonomes Fahren und Datenschutz – eine Bestandsaufnahme, ZD-Aktuell, 06034.
- Wiebe, Andreas: Data Act Proposal. Access Rights at the Intersection with Database Rights and Trade Secret Protection, GRUR 2023, S. 227 ff.

- Wiebe, Andreas / Schur, Nico: Protection of trade secrets in a data-driven, networked environment – Is the update already out-dated?, 14 Journal of Intellectual Property Law & Practice (2019) 814, abrufbar unter https://doi.org/10.1093/jiplp/jpz119.
- Wolf, Maik / Westermann, Kathrin, in: Frank Montag, Frank / Säcker, Franz Jürgen / Bien, Florian / Meier-Beck, Peter (Hrsg.): Münchener Kommentar zum Wettbewerbsrecht, Band 2: Deutsches Wettbewerbsrecht Gesetz gegen Wettbewerbsbeschränkungen (GWB), 4. Aufl. 2022.

Weitere Fachliteratur

- Fast, Victoria / Schnurr, Daniel / Wohlfarth, Michael: Marktmacht durch Daten: Eine Analyse aus ökonomischer Perspektive, in: Specht-Riemenschneider, Louisa /Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, 2020, S. 745 ff.
- Flügge, Barabara: Smart Mobility in der Praxis: Das Auto – unverzichtbar für den intermodalen Verkehr?, 2018.
- Fuchslocher, Götz: Entertainment im Fahrzeug – So mutieren Autos zu Spieleplattformen und Kinosälen, 13. Okt. 2020, abrufbar unter https://www.automotiveit.eu/technology/so-mutieren-autos-zu-spieleplattformen-und-kinosaelen-315.html.
- Holland, Heinrich / Zand-Niapour, Sam: Einflussfaktoren der Adoption von "Connected Cars" durch Endnutzer in Deutschland: Eine empirische Untersuchung, University of Applied Sciences Mainz 2017.
- Johanning, Volker/ Mildner, Roman: Car IT kompakt. Das Auto der Zukunft – Vernetzt und autonom fahren, 2015.
- Kerber, Wolfgang / Gill, Daniel: Datenzugang und Datenschutz im vernetzen Fahrzeug: eine ökonomische Perspektive, in: Stiftung Datenschutz (Hrsg.), Datenschutz im vernetzen Fahrzeug, 2020, S. 85 ff.
- Kielmann, C. / Detting, J.: Mit Big Data zum Connetced Car der Zukunft. Computerwoche, abrufbar unter https://www.computerwoche.de/a/mit-big-data-zum-connected-car-der-zukunft,3094413.
- Knorre, Susanne / Müller-Peters, Horst / Wagner, Fred: Die Big Data Debatte. Chancen und Risiken der digitalen vernetzten Gesellschaft, 2020.
- Niederländer, Ursula / Katzlinger, Elisabeth: Connected Cars – Profiteure, Risiken und Geschäftsfelder, in: Höller, Johann / Illetits-Motta, Tanja / Küll, Stefan / Niederländer, Ursula / Stabauer, Martin: Digital Business für Verkehr und Mobilität. Ist die Zukunft autonom und digital?, 2020, Teil 7, abrufbar unter https://www.idb.edu/wp-content/uploads/2021/01/CONNECTED-CARS-–-PROFITEURE-RISIKEN-UND-GESCHAeFTSFELDER.pdf.
- Proff, Heike / Fojcik, Thomas: Mobilität und digitake Transformation, Technische und betriebswirtschaftliche Aspekte, 2018.
- Reif, K.: Sensoren im Kraftfahrzeug, 3. Aufl., Wiesbaden 2016.
- Vieweg, C: Der Arzt fährt mit. Zeit Online 2015, abrufbar unter http://www.zeit.de/maobilitaet/2015-05/autofahrer-gesundheit-sensoren-autotechnik.

Forschungsstudien und Gutachten

- Bericht „C-ITS Platform“, Final Report, 2016, abrufbar unter https://www.polisnetwork.eu/wp-content/uploads/2019/09/c-its-platform-final-report-january-2016.pdf.

- C-IST-Initiative Directive 2010/40/EU; C-ITS Platform, Final Report, 2016, abrufbar unter https://transport.ec.europa.eu/system/files/2016-09/c-its-platform-final-report-january-2016.pdf.
- De Michiel, Federico, u.a.: Study to support an impact assessment for the review of the Database Directive, Final Report, Brussels, 2022.
- Everis Benelux, Study on data sharing between companies in Europe, carried out for the European Commission, Final Report, Brussels, 2018, abrufbar unter https://data.europa.eu/doi/10.2759/354943.
- Gutachten der Datenethikkommission, 2019, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=E9822C131C92FCCDF0D8C234444E5A06.2_cid295?__blob=publicationFile&v=7.
- Kienbaum, Connected-Car-Studie, 2016, abrufbar unter https://media.kienbaum.com/wp-content/uploads/sites/13/2019/05/New_Kienbaum_Connected_Car_Studie_2016.pdf.
- Leistner, Matthias / Antoine, Lucie: IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by the JURI committee of the European Parliament, May 2022, abrufbar unter https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266.
- McKinsey & Company, Monetizing car data. New service business opportunities to create new customer beneftis, 2016, abrufbar unter http://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%data/Monetizing-car-data.ashx
- Pretzsch, Sebastian / Drees, Holger / Rittershaus, Lutz / Schlueter Langdon, Christoph / Lange, Christoph / Weiers, Christian: Mobility Data Space, Secure Data Space for the sovereign and cross-platform utilization of mobility data, 2. Aufl. 2021, abrufbar unter https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/documents/Mobility_Data_Space_2022_EN.pdf
- Radauer, Alfred / Bader, Martin / Aplin, Tanya / Konopka, Ute / Searle, Nicola / Altenburger, Reinhard / Bachner, Christine: Study on the Legal Protection of Trade Secrets in the Context of the Data Economy, Final Report, Brussels 2022, abrufbar unter https://op.europa.eu/de/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en/format-PDF/source-267469968.
- Reiter, Julius / Methner, Olaf / Schenkel, Bénédict: Gutachten „Einführung eines „Mobilitätsdatenwächters“ für eine verbrauchergerechte Datennutzung - Notwendigkeit, Modell, gesetzliche Grundlagen“ im Auftrag des Verbraucherzentrale Bundesverband e.V. vom 15.11.2022, abrufbar unter https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilitätsdatenwächter_BRC_2022-15-11_Clean_Finalversion.pdf.
- Schweitzer, Heike / Metzger, Axel / Blind, Knut / Richter, Heiko / Niebel, Crispin / Gutmann, Frederik: Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy - A legal, economic and competition policy angle, Stand 8.7.2022, abrufbar unter https://pure.mpg.de/rest/items/item_3457829_2/component/file_3457831/content.
- Schweitzer, Heike / Metzger, Axel / Blind, Knut / Richter, Heiko / Niebel, Crispin / Gutmann, Frederik: Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy (July 8, 2022), abrufbar unter https://ssrn.com/abstract=4270272.
- Specht, Louisa / Kerber, Wolfgang: Datenrechte – Eine rechts- und sozialwissenschaftliche Untersuchung Deutschland-USA, Gutachten Projekt ABIDA, 2017, abrufbar unter https://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf.

- Stiemerling, Oliver / Weiß, Steffen / Wendehorst, Christiane: Forschungsgutachten zum Einwilligungsmanagement nach § 26 TTDSG, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, 16.12.2021, abrufbar unter https://www.ecambria-experts.de/it-sachverstaendiger/wp-content/uploads/2022/01/211216-Gutachten_fuer_Bundesministerium_fuer_Wirtschaft_und_Energie_p-os37621.pdf.
- Studie „Datenarchitekturen fahrzeuggenerierter Daten - Eine Use-Case-basierte Bewertung“ des Deutschen Zentrums für Luft- und Raumfahrt (DLR) vom 29.2.2020, abrufbar unter https://www.bmwk.de/Redaktion/DE/Publikationen/Technologie/studie-zu-datenarchitekturen-fahrzeuggenerierter-daten.pdf?__blob=publicationFile&v=6.
- TRL, Studie „Access to In-vehicle Data and Resources – Final Report” im Auftrag der EU-Kommission, durchgeführt von TRL aus 05/2017, abrufbar unter https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf.

Anlage - Fragebogen zu den moderierten Experten-Interviews

Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft

Hintergrund

Das Forschungsvorhaben untersucht übergeordnet die Notwendigkeit von Fahrzeugdatenzugangsregelungen entlang der Wertschöpfungskette der Automobilwirtschaft am Beispiel des vernetzten Fahrzeugs zur Steigerung von Innovation und Wettbewerb in dem Industriesektor der Automobil- und Mobilitätswirtschaft.

Wir möchten gerne die Expertise und Erkenntnisse der Automobil- und Mobilitätswirtschaft in die Untersuchung einbauen und hierfür Experteninterviews durchführen. Nur auf diese Weise lassen sich die langfristigen Entwicklungsziele der Automobil- und Mobilitätswirtschaft als Ganzes sowie datenbasierter Dienste und Geschäftsmodelle sowie entsprechende Datenzugangskonzepte und Datenaustauschmodelle im Einzelnen adäquat ermitteln.

Unsere Fragen an Ihre Experten

Frage 1:

Beschreiben Sie bitte die Datenerzeugung im vernetzten Fahrzeug. Welche (personenbezogen und nicht personenbezogen) Daten werden im vernetzten Fahrzeug heute und gegenwärtig erzeugt?

Frage 2:

Denkt man entlang der Wertschöpfungskette der Automobil- und Mobilitätswirtschaft, für welche Marktakteure sind nach Ihrer Einschätzung die Daten im Rahmen der Entwicklung innovativer Dienste und Geschäftsmodelle von Bedeutung?

Frage 3:

Beschreiben Sie bitte die von Ihnen angebotenen und in Zukunft zu erwartenden datenbasierten Dienste und Geschäftsmodelle.

Frage 4:

Welche Konzepte und Projekte zum Datenzugang und -austausch im Mobilitätsbereich sind Ihnen bekannt und wie bewerten Sie diese mit Blick auf verschiedene Marktteilnehmer?

Frage 5:

Führen bestehende gesetzliche Regelungen sowie die zuvor genannten Konzepte und Projekte aus Ihrer Sicht zu einem diskriminierungsfreien, chancengleichen Wettbewerb zwischen den verschiedenen Marktakteuren im Mobilitätsdatenbereich? Wenn ja bzw. nein, warum?

Frage 6:

Welche Bedeutung haben Betriebs- und Geschäftsgeheimnisse bei der Datengenerierung und –weitergabe in Ihrem Unternehmen und mit welchen Maßnahmen kann man diese trotz der kommenden Verpflichtungen zum Data Sharing bewahren?

*****