

HUMBOLDT-UNIVERSITÄT ZU BERLIN



Forschungsinstitut für Recht und digitale Transformation

Working Paper Series

2019

Digitale Mobilität – Verträge über Nutzerdaten

Prof. Dr. Axel Metzger, LL.M. (Harvard)

Working Paper No. 1

Zitiervorschlag: Axel Metzger, „Digitale Mobilität – Verträge über Nutzerdaten“, Working Paper No. 1 des Forschungsinstituts für Recht und digitale Transformation (2019).

"Digitale Mobilität - Verträge über Nutzerdaten"

erschienen in GRUR 2019, 129-136

Axel Metzger, Berlin*

Die Erhebung, Verwendung und Weitergabe von Mobilitätsdaten erfolgt heute vielfach auf Basis von Verträgen zwischen dem Fahrzeugkäufer oder -nutzer, dem Fahrzeughersteller sowie den weiteren Akteuren auf den nachgelagerten Märkten. Der Beitrag beleuchtet die datenschutz- und vertragsrechtlichen Voraussetzungen und Grenzen eines Marktmodells für Mobilitätsdaten und untersucht erste Beispiele aus der Praxis.

I. Ausgangslage

Für den flüchtigen Betrachter stellt sich die Entwicklung des europäischen Datenrechts der letzten Monate als widersprüchlich dar. Auf der einen Seite hat die EU mit der Datenschutzgrundverordnung (DS-GVO) den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten auf ein nie da gewesenes Niveau angehoben. Ob die zusätzlichen Rechte der Datensubjekte – die DS-GVO spricht von „betroffenen Personen“ – die zusätzlichen Pflichten für große und mittelständische Unternehmen sowie Behörden am Ende wert sind, müssen die kommenden Jahre erst noch zeigen. Die Erfahrungen der ersten Monate mit der DS-GVO nähren durchaus Zweifel, ob sich der bürokratische Aufwand und die erheblichen Rechtsberatungskosten am Ende wirklich in einem höheren Schutzniveau und einem Mehr an Selbstbestimmung niederschlagen werden. Zeitgleich arbeiten auf der anderen Seite die europäischen und nationalen Institutionen an den rechtlichen Rahmenbedingungen für eine funktionsfähige Datenwirtschaft, welche die Entwicklung von international konkurrenzfähigen Produkten und Diensten der Industrie 4.0 in Europa und in Deutschland leisten kann. Smart Cars, Smart Homes, Smart Cities basieren letztlich auf der massenhaften Verarbeitung personenbezogener Daten. Nichts anderes gilt für „selbstlernende Systeme“ und Anwendungen sogenannter künstlicher Intelligenz. Sie benötigen große Datenmengen, um aus deren Verarbeitung Handlungsanweisungen abzuleiten. Die – scheinbare – Widersprüchlichkeit dieser Zielvorstellungen ist Reflex des in der Ökonomie schon lange beschriebenen „Privacy Paradox“²: So wie der

1 Prof. Dr. jur., LL. M. (Harvard); Inhaber des Lehrstuhls für Bürgerliches Recht und Immaterialgüterrecht, insbesondere Gewerblicher Rechtsschutz, Humboldt-Universität zu Berlin; Gründungsdirektor des Weizenbaum-Instituts für die Vernetzte Gesellschaft, Berlin. Der Autor dankt Dr. Zohar Efroni, LL.M. (Cardozo), Jakob Metzger und Lena Mischau von der Forschungsgruppe 4 des Weizenbaum-Instituts für Recherche und Hilfe bei den Nachweisen. Alle Internetquellen wurden zuletzt am 7.11.2018 abgerufen. Der Beitrag beruht auf einem Vortrag, den der Verfasser am 27.9.2018 auf der GRUR-Jahrestagung in Berlin gehalten.

2 Das Konzept des „Privacy Paradox“ wird wohl erstmals beschrieben in *Acquisti/Grossklags*, Losses, Gains and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior, 2003, abrufbar unter: http://people.ischool.berkeley.edu/~jensg/research/paper/acquisti_grossklags.pdf (wenn auch ohne das Phänomen explizit als solches zu bezeichnen). Ausdrücklich vom „Privacy Paradoxon“ sprechen *Norberg/Horne/Horne*, *The Journal of Consumer Affairs*, 2007, 100 ff.

Einzelne nach seinen abstrakten Präferenzen befragt großen Wert auf den Schutz seiner Daten legt, im Alltag aber bereit ist, seine Daten für nur geringe Vorteile preiszugeben, so strebt auch die Legislative einerseits in Richtung mehr Datenschutz, andererseits in Richtung einer Teilhabe an den wirtschaftlichen Chancen der Datenökonomie. Der Widerspruch löst sich bei näherer Betrachtung jedoch auf. Verbraucher haben – in unterschiedlichem Maß und je nach individuellen Präferenzen – ein Interesse an datenintensiven Produkten und Diensten und wollen an der Wertschöpfung teilhaben; sie wollen aber über die Verwendung ihrer Daten entscheiden können, entweder individuell auf Basis von Einwilligungserklärungen und Verträgen oder kollektiv mittels legislativer Festsetzung der Grenzen der Datennutzung. Die Selbstbestimmung im Umgang mit den eigenen Daten und die Teilhabe an der Wertschöpfung aus den Daten sind zwei Seiten derselben Medaille. Dementsprechend setzen alle Bestrebungen der europäischen und nationalen Regulierer – jedenfalls Stand heute – auf den Datenschutzregeln der DS-GVO auf und versuchen auf dieser Basis, eine Marktordnung für die Datenwirtschaft zu entwickeln.

Die beschriebenen Entwicklungen zeigen sich am Beispiel der Automobilindustrie wie in einem Brennglas. Moderne Kraftfahrzeuge sammeln und verarbeiten vielfältige, zumeist auch personenbezogene Daten, insbesondere:³

- Daten für Wartungs- und Reparaturzwecke, die zum Teil auch nur lokal und offline im Fahrzeug gespeichert werden,
- Daten über das Fahrzeug und seine Komponenten zum Zweck der Verbesserung und Weiterentwicklung,
- Daten für vernetzte Verkehrssysteme (bspw. C-ITS: Cooperative Intelligent Traffic-Systems⁴) und für andere vernetzte Dienste, die das Fahrzeug und seinen Betrieb im Straßenverkehr selbst betreffen,
- Daten, die in einem ggf. vorhandenen Unfalldatenspeicher abgelegt werden,
- Medien- und Telekommunikationsdienste im Fahrzeug, Karten- Verkehrs- und Wetterdienste, Daten für Mautsysteme bei Privatstraßen, für Versicherungen etc.

Je nach Fahrzeughersteller und Verwendungskontext ließe sich die Liste noch fortsetzen. Wer als Verbraucher einen Neuwagen erwirbt, leaset, mietet oder einfach nur fährt, wird einige, wenn nicht alle der genannten datenbasierten Fähigkeiten und Dienste des Fahrzeugs nutzen wollen und ist bereit, der hierfür notwendigen Verarbeitung seiner personenbezogenen Daten zuzustimmen, sofern die Zustimmung aufgrund der gesetzlichen Erlaubnistatbestände des Datenschutzrechts nicht obsolet ist. Werden Daten jenseits des hierfür erforderlichen Maßes genutzt, etwa durch Weitergabe von (nicht) anonymisierten „Big Data“-Sammlungen an Dritte, stellt sich erneut die Frage nach der Einwilligung des Fahrers und auch nach der Partizipation an dieser zusätzlichen Wertschöpfung. Jenseits der individuellen Entscheidung über die Datenverarbeitung können auch Entscheidungen des Gesetzgebers über die Grenzen der zulässigen

3 Zum Folgenden auch eingehend *Hansen*, DuD 2015, 367 (367 f.); *Krauß/Waidner*, DuD 2015, 383 ff.; *von Schönfeld*, DAR 2015, 617 (619).

4 *Europäische Kommission*, COM(2016) 766 final; *C-ITS Platform*, Final report Phase II, September 2017, 27 ff., abrufbar unter: <https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf>; *Artikel-29-Datenschutzgruppe*, Stellungnahme 03/2017 zur Verarbeitung personenbezogener Daten im Kontext Kooperativer, Intelligenter Verkehrssysteme (C-ITS), WP 252, vom 04.10.2017, abrufbar unter: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

Datennutzung erforderlich sein, um kollektive Systeme – etwa Mautgebühren, autonomes Fahren oder vernetzte Verkehrssysteme – überhaupt funktionsfähig aufbauen zu können. Kollektive Entscheidungen können auch erforderlich werden, um den Zugang zu Datensammlungen im Interesse des Wettbewerbs zu eröffnen. Der Bereich der digitalen Mobilität bietet also reichlich Anschauungsmaterial für die Voraussetzungen, die Möglichkeiten und die Grenzen der Datenökonomie.

Im Folgenden sollen entsprechend der Gesamtkonzeption des Themenschwerpunkts dieser Ausgabe der GRUR die Vertragsverhältnisse der Beteiligten beleuchtet werden. Nach dem vorläufigen Scheitern der Pläne für die Einführung eines geistigen Eigentumsrechts an Daten auf europäischer Ebene, dürfte sich die im Entstehen begriffene Marktordnung der digitalen Mobilität vor allem auf die Instrumente der Einwilligung und des Vertrags stützen – flankiert durch die verschiedenen Instrumente der (vor allem datenschutzrechtlichen) Regulierung und des Wettbewerbsrechts. Dass sich die Akteure privatautonom durch Verträge organisieren, entspricht dem Konzept der Marktwirtschaft und lässt jedenfalls bei einer modellhaften Betrachtung auch eine effiziente Verteilung von Gütern und gesamtwirtschaftliche Wohlfahrtsmaximierung erwarten, sofern die Voraussetzungen für eine solche Marktordnung gegeben sind (Wettbewerb, Fehlen von Informationsasymmetrien, niedrige Transaktionskosten etc.).⁵ Insofern gebührt dem Vertragsrecht besondere Aufmerksamkeit. Zur Vereinfachung des ohnehin schon komplexen Interessengefüges wird im Folgenden allein die Datenverarbeitung durch den Hersteller betrachtet, einschließlich sogenannter „Extended vehicle“-Modelle, bei denen die Daten auf unternehmenseigenen Servern des jeweiligen Herstellers verarbeitet werden.⁶ Treuhandmodelle, bei denen neutrale Dritte die Daten gegebenenfalls auch verschiedener Hersteller sammeln, werden im Folgenden dagegen nicht untersucht, da diese – soweit ersichtlich – zwar von manchen Akteuren gefordert, bislang in der Praxis aber nicht umgesetzt werden.⁷ Ausgeblendet bleiben auch direkt im Fahrzeug installierte Apps Dritter, die eigenständig Daten sammeln.⁸ Auf diese sind die nachfolgenden Überlegungen mutatis mutandis anzuwenden.

II. Akteure und Interessen

Geht man von einer Ausgangssituation aus, bei der personenbezogene Daten des Fahrers erhoben und verarbeitet werden, so lassen sich ohne Anspruch auf Vollständigkeit folgende Gruppen von Akteuren

5 Speziell zu Daten im Automobilssektor siehe *Kerber/Frank*, Data Governance Regimes in the Digital Economy: The Example of Connected Cars (November 3, 2017), <https://ssrn.com/abstract=3064794>, 8 ff.

6 Das „Extended Vehicle“-Modell wird v.a. von der Automobilindustrie bevorzugt. Auf Initiative des Verbands der Automobilindustrie (VDA) erarbeitet die Internationale Organisation für Normung (ISO) hierzu einen Industriestandard (ISO 20077, 20078, 20080). Hierauf aufbauend hat der VDA das „NEVADA“-Konzept (Neutral Extended Vehicle for Advanced Data Access) entwickelt, welches einen „diskriminierungsfreien“ Zugriff Dritter auf Fahrzeugdaten sicherstellen soll, wobei auch hier der unternehmenseigene Server *immer* zwischen dem Fahrzeug und Dritten steht, siehe die verschiedenen VDA Positionspapiere zum Stichwort „Nevada“ unter <http://www.vda.de>. Siehe auch Kerber, 9 (2018) JIPITEC.

7 Hierzu *Brockmeyer*, ZD 2018, 258.

8 So bietet BMW beispielsweise eine Integration von Microsoft Office 365 an, durch welche E-Mails, Kontakte und Kalendereinträge eines bestehenden Microsoft-Abonnements aus dem Auto heraus bearbeitbar werden. Außerdem will beispielsweise die Allianz Renault-Nissan-Mitsubishi ab 2021 Android als Plattform in das Bordsystem übernehmen, wobei die Datenverarbeitung dann über Googles eigene Infrastruktur erfolgen soll, siehe *Reintjes*, Google dringt ins Auto vor und ist kaum aufzuhalten, WirtschaftsWoche vom 19.10.2018, abrufbar unter: <https://www.wiwo.de/unternehmen/auto/android-auto-google-dringt-ins-auto-vor-und-ist-kaum-aufzuhalten/23187632.html>.

identifizieren, die an einer Nutzung dieser Daten Interesse haben können:⁹

- Fahrzeughersteller und OEM-Aftermarket: Eigene und gebundene Händler, Tochterunternehmen, Partnerunternehmen, Teilezulieferer, gebundene Werkstätten,
- Freier Aftermarket: Freie Händler, Freie Werkstätten, Versicherungen, Apphersteller, Telematic-Service-Provider (TSP), private Straßenbetreiber (Maut), sonstige Dienstleister,
- Sonstiger Markt: Marktforschung- und analyse, Mobilitätsdienstleister (z.B. Carsharing), Werbung,
- Andere private Personen und Akteure: Kfz-Halter, Kfz-Eigentümer, Kfz-Erwerber, Mitinsassen, Verkehrsteilnehmer, Arbeitgeber, sonstige private Dritte,
- Staat und Wissenschaft: Steuerbehörden, Infrastruktur, Strafverfolgungsbehörden, sonstige Behörden, (außer-)universitäre Forschung.

Denkbar ist allerdings auch, dass personenbezogene Daten von Mitinsassen und vom Kfz-Halter beim Betrieb des Fahrzeugs erhoben werden, was zu anderen Konstellationen und Interessen führen kann. Zur Vereinfachung wird im Folgenden – sofern nicht anders vermerkt – davon ausgegangen, dass Fahrzeugeigentümer, -halter und -führer identisch sind.

III. Personenbezogene Daten oder bloße Maschinendaten

Unter welchen Voraussetzungen die von Fahrzeugen gesammelten Daten erhoben und verarbeitet werden dürfen, hängt entscheidend davon ab, ob es sich um personenbezogene Daten handelt. Maßgeblich hierfür ist seit dem 25. Mai 2018 die Definition in Artikel 4 Nr. 1 DS-GVO. Danach sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“ Die Definition ist bewusst weit gefasst. Nach der Rechtsprechung des EuGH handelt es sich um Informationen „über“ eine Person, „wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft ist“.¹⁰ Für viele der Daten, die von Fahrzeugen erhoben und gesammelt werden, ist die Einordnung letztlich unstrittig, so dass die Anwendung von Artikel 4 Nr. 1 DS-GVO auf die verschiedenen Typen von Daten hier

9 Ähnlich von Schönfeld (o. Fn. 2), 618 f.

10 *EuGH*, Urt. v. 20.12.2017 – C-434/16 (Nowak/Data Protection Commissioner), NJW 2018, 767 (768) Rn. 35. Rechtsprechung und Literatur zur Definition personenbezogener Daten nach Art. 2 lit. 1 DSRL sind auf den neuen Art. 4 Nr. 1 DS-GVO weitgehend übertragbar, da die DS-GVO die Begriffsbestimmung größtenteils lediglich präzisiert, die wesentlichen inhaltlichen Bestandteile dabei aber unverändert übernimmt; siehe hierzu *Klabunde in Ehmann/Selmayr*, 2. Aufl. 2018, Art. 4 DS-GVO, Rn. 8. Auch hat die Artikel-29-Datenschutzgruppe bereits zur alten Rechtslage das damalige Tatbestandsmerkmal "Informationen über eine [...] Person" mit dem heutigen "Informationen, die sich auf eine [...] Person [...] beziehen" gleichgestellt: "Allgemein „beziehen“ sich Informationen auf eine Person, wenn es sich um Informationen *über* diese Person handelt"; siehe *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, WP 136, vom 20.06.2007, S. 10, abrufbar unter: https://www.lida.bayern.de/media/wp136_de.pdf.

kurz gehalten werden kann.¹¹ Es besteht, soweit ersichtlich, darüber Einigkeit, dass grundsätzlich alle Daten, die aus einem vernetzten Kfz gesendet werden, personenbezogen sind, da hier der Fahrer über einen Account, über Zertifikate oder über die Standortdaten identifiziert werden kann. Bei Daten, die gespeichert und später ausgelesen werden, ist die Person des Fahrzeughalters über die Fahrzeugidentifikationsnummer und das Kennzeichen ermittelbar. Ist nicht der Fahrzeughalter selbst, sondern ein Dritter das Fahrzeug gefahren, so kann dessen Identität durch den Halter festgestellt und mitgeteilt werden. Dadurch ist der Kreis der durch digitalisierte und vernetzte Fahrzeuge erhobenen personenbezogenen Daten sehr weit gezogen. Personenbezogen können beispielsweise sein:

- Infotainment- und Komforteinstellungen: Sitzeinstellungen, Lautstärke, Navigationsziele, Adressbuch- und Telefondaten, personalisierter Zugriff auf Dienste Dritter, Kameradaten usw.,
- Betriebswerte, die dem Fahrer angezeigt werden: Füllstände, Verbrauch, Geschwindigkeit usw.,
- Technische Daten: Sensor-Daten, Einspritzverhalten des Motors, Schaltverhalten des Automatikgetriebes, ABS, Airbag, Auslösungen des Gurtstraffers usw.,
- Aggregierte Daten: Durchschnittsverbrauch und -geschwindigkeit, Fehlfunktionen im Fehlerspeicher usw.

Der weite Begriff der personenbezogenen Daten führt zugleich dazu, dass nur wenige der von Fahrzeugen gesammelten Daten aus dem Datenschutzrecht herausfallen und nicht an die strengen Vorgaben der DSGVO gebunden sind. Als „reine“ Maschinendaten sind flüchtige Daten einzuordnen, die weder gespeichert noch gesendet werden, etwa wenn das Fahrzeug die Geschwindigkeit, die Temperatur im Innenraum, Verbrauchswerte usw. nicht aufzeichnet und auch nicht übermittelt.¹² Aus dem Anwendungsbereich der DSGVO heraus fallen auch anonymisierte Daten, bei denen niemand mehr auf die betroffene Person schließen kann.¹³ Vom Hersteller vollständig und endgültig anonymisierte Daten, bei denen weder der Hersteller noch Dritte den Fahrer, den Halter oder sonstige natürliche Personen identifizieren können, verlieren ihren Personenbezug und können isoliert oder in aggregierter Form ohne die Bindungen der DSGVO verarbeitet und an Dritte weitergegeben werden.

IV. Rechtmäßigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist gem. Artikel 6 DSGVO nur zulässig, wenn einer der dort genannten Erlaubnistatbestände eingreift.¹⁴ Verarbeitet ein Kfz-Hersteller alle in Frage kommenden Daten

11 *Balzer/Nugel*, NJW 2016, 193 (195) (zu § 3 BDSG a.F.); *Buchner*, DuD 2015, 372 (373); *Hansen* (o. Fn. 2), 368 f.; *Kunnert*, CR 2016, 509 (510); *Lüdemann*, ZD 2015, 247 (249 ff.); *von Schönfeld* (o. Fn. 2), 619; *Weichert*, SVR 2014, 201 (204). Siehe auch *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder/Verband der Automobilindustrie (VDA)*, Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, 2016, abrufbar unter: <https://www.vda.de>.

12 *Buchner* (o. Fn. 10), 374; vgl. hierzu auch *BVerwG*, DuD 2015, 196 (198) sowie *BVerfG*, DuD 2008, 352 zur verfassungsrechtlichen Einordnung flüchtiger Speicherungen bei automatisierter Kennzeichenerfassung.

13 *Weichert* (o. Fn. 10), 205.

14 Spezialfragen zu Telekommunikationsdaten nach TKG, TMG bzw. den zugrundeliegenden europäischen Richtlinien 2002/58 bzw. der künftigen ePrivacy-VO (*Europäische Kommission*, COM (2017) 10) bleiben im Folgenden ausgeblendet. Hierzu noch vor Inkrafttreten der DSGVO: *Buchner* (o. Fn. 10), 374 f.; *Lüdemann* (o. Fn. 10), 252; *Weichert* (o. Fn. 10), 203.

und möchte diese auch an Dritte weitergeben, so ist die datenschutzrechtliche Rechtfertigung keineswegs trivial.

1. Einwilligung

In Anbetracht der Vielfalt der erhobenen Daten und der möglichen Verarbeitungsszenarien liegt es nahe, die Einwilligung des Betroffenen einzuholen. Eine Datenverarbeitung mit Einwilligung ist grundsätzlich umfassend möglich. Die Einwilligung ist allerdings jederzeit frei widerruflich gem. Artikel 7 Abs. 3 DS-GVO und schon deswegen von begrenztem Interesse für den Fahrzeughersteller. Hinzu treten weitere Bedingungen, denen die Einwilligung genügen muss, um überhaupt wirksam zu sein. Zunächst muss die Einwilligung freiwillig erteilt worden sein. Dies kann man in den Fällen bezweifeln, in denen die Einwilligung erst nach Kauf des Fahrzeugs eingeholt wird und dann zur Nutzung von für den regulären Betrieb des Fahrzeugs notwendigen Diensten erforderlich ist, etwa des Navigationsdienstes. Hier wird man dann kaum noch von einer freien Entscheidung sprechen können, wenn der Fahrer notgedrungen zustimmt, weil er das bereits erworbene und bezahlte Automobil überhaupt nur bei Abgabe der Einwilligungserklärung vertragsgemäß nutzen kann.¹⁵ Weiter sind die allgemeinen Probleme bei datenschutzrechtlichen Einwilligungserklärungen zu berücksichtigen, etwa wenn längliche Datenschutzbestimmungen nur klein auf einem Display angezeigt werden.¹⁶ Ein weiteres Problem ergibt sich im Hinblick auf die Zweckbestimmung der Einwilligung. Die der Einwilligung zugrundeliegende Datenschutzerklärung muss in verständlicher Weise über Art und Umfang der Datenverarbeitung aufklären und darf nicht pauschal verlangt werden; in Anbetracht der verschiedenen denkbaren Szenarien der Verarbeitung von Daten bei der digitalen Mobilität ist eine umfassende Bestimmung der möglichen Zwecke jedoch kaum möglich.¹⁷ Problematisch sind auch Gestaltungen von Datenschutzhinweisen, die nur eine Einwilligung in eine umfassende Datenverarbeitung oder einen vollständigen Verzicht auf den angebotenen Dienst als Alternativen anbieten („Take it or leave it“).¹⁸ Schließlich ist das Kopplungsverbot in Artikel 7 Abs. 4 DS-GVO zu beachten, sofern die Einwilligung im Rahmen eines Vertrages erteilt wird und die Datenverarbeitung über das für die Vertragserfüllung erforderliche Maß hinausgeht. Insoweit ist jedoch zu beachten, dass bei Vertragsverhältnissen eine Koppelung von Einwilligung und Vertragserfüllung nicht pauschal ausgeschlossen ist, sondern eine gesonderte Erforderlichkeitsprüfung vorgesehen ist.¹⁹

2. Zur Erfüllung des Vertrags, berechtigtes Interesse

Grundsätzlich denkbar ist auch, dass die Datenverarbeitung ohne Einwilligung des Betroffenen rechtmäßig sein kann, sofern sie entweder für die Erfüllung des Vertrags gem. Artikel 6 Abs. 1 lit. b) DS-GVO oder zur

15 Kritisch auch *Lüdemann* (o. Fn. 10), 253.

16 Kritisch auch *Weichert*, SVR 2014, 241 (242 f.); insofern auch zweifelhaft die Empfehlung, dass „sämtliche Informationen über die Verarbeitung personenbezogener Daten“ über das „Display des Armaturenbretts“ einsehbar sein sollen, siehe *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Datenschutzrechtliche Empfehlungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum automatisierten und vernetzten Fahren, vom 01.06.2017, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/DatenschutzrechtlicheEmpfehlungenVernetztesAuto.pdf?__blob=publicationFile&v=1, Empfehlung 2.

17 *Lüdemann* (o. Fn. 10), 254.

18 *Buchner* (o. Fn. 10), 376 f. Siehe auch *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (o. Fn. 15), Empfehlung 8.

19 Zum Kopplungsverbot siehe *Heckmann/Paschke* in *Ehmann/Selmayr*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 94 ff. Siehe jetzt auch OGH, 31.8.2018, 6Ob140/18h), 4.4.1. ff.

Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gem. Artikel 6 Abs. 1 lit. f) DS-GVO erforderlich ist. Der erste Fall trifft etwa auf die Verarbeitung von Positionsdaten zu, wenn diese für Navigationsdienste erforderlich sind. Gleiches gilt für weitere Sensorinformationen, die für die Erbringung von Diensten von vernetzten Fahrzeugen erforderlich sind, etwa Notrufsysteme, Assistenzsysteme, Verkehrsinformationen etc. Hierher gehören auch die für die Erbringung von Telematikversicherungen erforderlichen Datenverarbeitungen²⁰ sowie die Obliegenheit des Versicherten bei Kaskoversicherungen, dem Versicherungsunternehmen die Untersuchung des Fahrzeugs zu ermöglichen.²¹ Der zweite Fall umfasst bspw. die Auswertung von Daten im Versicherungsfall²² oder durch den Hersteller zum Beweis der Fehlerfreiheit des Fahrzeugs bei einem Unfall.²³

Eine Rechtfertigung der Datenverarbeitung über die gesetzlichen Tatbestände des Artikel 6 Abs. 1 lit. b) - f) DS-GVO scheidet aber dann aus, wenn es sich bei den erhobenen Daten um sensible Daten gem. Artikel 9 DS-GVO handelt.²⁴ Hier kann allein die Einwilligung des Betroffenen helfen, die zudem noch an verschärfte Anforderungen geknüpft ist. Zu den sensiblen Daten gehören alle Daten, aus denen bestimmte, diskriminierungsanfällige Eigenschaften hervorgehen (z.B. rassische/ethnische Herkunft, politische Meinung) oder die bereits abstrakt ein Diskriminierungsrisiko hervorrufen (z.B. Gesundheitsdaten, biometrische Daten, Daten zum Sexualleben). Wann eine sensible Eigenschaft aus Daten hervorgeht, lässt sich dabei abstrakt kaum definieren. Neben einem Wahrscheinlichkeitskriterium kommt es auch stets auf den Verwendungskontext an. Einzelfallabhängig kann auch die Verwendungsabsicht bedeutsam sein. Pauschale Aussagen über das Vorliegen sensibler Daten sind damit kaum möglich, abgesehen von biometrischen Daten, die eindeutig unter die Vorschrift fallen. Auch Standortdaten können sensibel sein, weil über längere Verweildauer an spezifischen Orten sensible Datenkategorien im Einzelfall mit hinreichender Wahrscheinlichkeit sichtbar werden können, z.B. zur politischen Meinung oder sexuellen Orientierung oder zur Gesundheit wegen des Besuchs entsprechender Orte.

Zusätzliche Beschränkungen ergeben sich gem. Artikel 10 DS-GVO bei der Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten.²⁵ Da Fahrzeuge jedoch nur Daten über Handlungen speichern, etwa das Überfahren roter Ampeln, das Befahren eines Forstweges, eine mögliche Fahrerflucht oder Geschwindigkeitsverstöße, nicht aber über festgestellte Straftaten, dürfte Artikel 10 DS-GVO im hier untersuchten Bereich kaum Bedeutung erlangen.

3. Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung

Denkbar ist schließlich auch eine Rechtfertigung der Datenverarbeitung, wenn diese zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist, Artikel 6 Abs. 1 lit. c) DS-GVO. Momentan ist der Anwendungsbereich noch gering. Beispiele sind die Verpflichtungen im Rahmen der e-Call-

20 *Lüdemann* (o. Fn. 10), 252; *Weichert* (o. Fn. 15), 245 f.

21 Hierzu *Balzer-Nugel* (o. Fn. 10), 198 f. (zu § 28 BDSG a.F.).

22 *Balzer/Nugel* (o. Fn. 10), 196 (zu § 28 BDSG a.F.); kritisch *Lüdemann* (o. Fn. 10), 252 (zu § 28 BDSG a.F.).

23 *Buchner* (o. Fn. 10), 376.

24 Zum Vorliegen sensibler Daten und den Rechtsfolgen siehe *Schiff* in *Ehmann/Selmayr*, DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 13 ff.

25 Hierzu siehe: *Schiff* in *Ehmann/Selmayr*, DS-GVO, 2. Aufl. 2018, Art. 10 Rn. 1 ff.; *Weichert* in: *Kühling/Buchner*, DS-GVO BDSG, 2. Aufl. 2018, Art. 10 Rn. 1 ff.

Verordnung oder § 63a StVG für autonome Fahrzeuge.²⁶ Weitere nachträgliche Verpflichtungen können insbesondere im Rahmen der Strafverfolgung bestehen; die mögliche spätere Verpflichtung im Rahmen der Strafverfolgung bietet aber keinen Rechtsgrund für die ansonsten anlasslose Datenerhebung im früheren Betrieb des Fahrzeugs. Künftig könnte die Vorschrift größere Relevanz erhalten. Für die C-ITS-Plattform schlägt die Artikel-29-Datenschutzgruppe vor, die Datenverarbeitung auf eine neu zu schaffende Verpflichtung i.V.m. Artikel 6 Abs. 1 c) DS-GVO zu stützen – dieser Vorschlag wurde auch von der Kommission übernommen.

V. Modelle der Datennutzung bei vernetzten Fahrzeugen – zwei Fallstudien

Vor dem Hintergrund der genannten rechtlichen Rahmenbedingungen sind mittlerweile verschiedene Modelle der Datenverarbeitung bei vernetzten Fahrzeugen am Markt erkennbar. Die folgende Darstellung basiert allein auf den öffentlich verfügbaren Informationen von BMW und Tesla.

1. BMW ConnectedDrive

BMW eignet sich in besonderem Maße für eine Fallstudie an dieser Stelle, weil BMW das NEVADA-Konzept des VDA umzusetzen versucht.²⁷

BMW ConnectedDrive ist eine von BMW aufgebaute IT-Plattform mit entsprechenden Vertragsbedingungen. Bei BMW ConnectedDrive werden über eine fest verbaute SIM-Karte Online-Dienste im Auto angeboten, teilweise in Verbindung mit einer Smartphone-App. Dazu werden u.a. folgende Daten übermittelt: GPS-Standort, Geschwindigkeit, Laufleistung, Sensorinformationen (Radar, Kamera, Mikrofon, Regen) etc. Hierauf aufbauend können beispielsweise folgende Dienste in Anspruch genommen werden: Navigation, Spracherkennung, intelligenter Notruf, Parkplatzsuche, „Remote 3D-View“ (ermöglicht am Smartphone über die Außenkameras eine 3D-Rundumsicht des PKW in seiner tatsächlichen Umgebung), Remotefunktionen wie die Temperatursteuerung, Entsperrern etc. Teilweise sind hier auch Drittanbieterapps integriert (z.B. Microsoft Office).

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 genaue Anwendungsbereich von BMW CarData ist im Moment noch unklar. Insbesondere für unabhängige Werkstätten, Händler und weitere „Aftermarket“-Anbieter existieren öffentlich einsehbare AGB, die den Datenzugang regeln.²⁸ Für andere mögliche Interessenten, bspw.

26 Hierzu *Berndt*, NZV 2018, 249; *Putzki/Sesing*, MMR-Aktuell 2017, 388288; *Wagner/Goebel*, ZD 2017, 263 (267 f.); so auch *Klink-Straub/Straub*, NJW 2018, 3201 (3203) für § 63a StVG, wohingegen Art. 6 eCall-Verordnung vorzugsweise der öffentlichen Aufgabenwahrnehmung gem. Artikel 6 Abs. 1 lit. e) DS-GVO zuzuordnen sei.

27 Zum NEVADA-Konzept s.o. Fn. 5; zur Anwendung bei BMW CarData siehe *Zimmermann/Zoller*, A Neutral and Secure Approach for Accessing In-Vehicle Data for 3rd Party Services, Präsentation vom 18.04.2018, abrufbar unter: https://at.projects.genivi.org/wiki/download/attachments/16027368/180418_GENIVI-AMM_Access-to-in-vehicle-data_pub.pdf; *BMW*, BMW Group startet BMW CarData: neue und innovative Services für den Kunden – sicher und transparent, Pressemitteilung vom 30.05.2017, abrufbar unter: <https://www.press.bmwgroup.com/deutschland/article/detail/T0271366DE/>.

28 *BMW*, Aftersales Online System, Nutzungsbedingungen, abrufbar unter: <https://aos.bmwgroup.com/de/terms-of-use>.

Versicherungen oder Anbieter weiterer Dienste, liegt im Moment nur eine Pressemitteilung vor.²⁹ Legt man das dort beschriebene Modell zugrunde, so sollen sich Dritte diskriminierungsfrei bei BMW CarData anmelden können. Dort können die erwünschten Daten (z.B. Kilometerstand, GPS) festgelegt werden und dann über die Plattform die Einwilligung des Kunden (identifiziert nach Fahrzeug-ID-Nummer) eingeholt werden. Eine Weitergabe von personenbezogenen Daten über BMW CarData findet also nur nach Einholung einer auf die konkrete Anfrage des Interessenten bezogenen Einwilligung statt. Nach Angaben von BMW haben sich in den ersten sechs Monaten seit dem Start von BMW CarData im Jahr 2017 bereits über 60 Drittanbieter mit über 40 in Entwicklung befindlichen Anwendungen registriert; insgesamt seien zu diesem Zeitpunkt bereits mehr als eine Million Datensätze über das System verteilt worden.³⁰ Bezahlt wird die Nutzung der Daten durch den Dritten, wobei die Gebühr von Häufigkeit und Umfang der Datenabfrage abhängt (max. fünf € pro Auto pro Monat).³¹ Aufbauend auf der Plattform BMW CarData können weitere unabhängige Marktplätze wie Otonomo und Caruso ihren Kunden Zugang zu BMW-Daten eröffnen.³²

Die rechtliche Basis von BMW ConnectedDrive ist weitgehend offen im Internet abrufbar, bei BMW CarData gilt dies nur teilweise. Relevant sind zunächst die AGB zu BMW ConnectedDrive.³³ Danach trägt der Kunde durch Abschluss eines Kaufvertrags über einen BMW-Neuwagen BMW den Abschluss eines Rahmenvertrags an (1.4 AGB) und verzichtet auf den Zugang der Annahmeerklärung (1.7 AGB). Bei einem Opt-Out des Kunden wird die SIM-Karte ausgebaut und die Dienste werden „deaktiviert“ (1.5 und 6.1 AGB). Interessant ist die vertragliche Konstruktion beim Weiterverkauf des Fahrzeugs durch den Kunden an einen Dritten (7.1-7.3 AGB). Danach kann der BMW-ConnectedDrive-Vertrag nur mit Zustimmung von BMW übertragen werden. Der Kunde muss in diesem Fall alle seine Daten löschen lassen und die Verknüpfung im Webportal beenden. Zudem muss der Kunde den Käufer über (de)aktivierte Dienste informieren. Die Übermittlung der Daten erfolgt im Übrigen mit SSL-Verschlüsselung (11 AGB). Grundsätzlich werden diese zum Zweck der Vertragserfüllung (insbesondere Punkt B der Datenschutzhinweise - DSH) sowie aufgrund berechtigter Interessen (insbesondere Punkte C, D, E DSH) verarbeitet. Vor einer Datenverarbeitung zum Zweck der Werbung und Marktforschung sowie bei Weitergabe an Dritte wird dagegen eine Einwilligung eingeholt (Punkte F, H DSH). BMW ConnectDrive kombiniert damit eine Datenverarbeitung auf Grundlage gesetzlicher Erlaubnistatbestände der Artikel 6 Abs. 1 lit. b), c) und f) DS-GVO, über die in den Datenschutzhinweisen nur informiert wird, mit Formen der Datenverarbeitung, für die die Einwilligung des Betroffenen erforderlich ist. Hierzu zählt insbesondere die Weitergabe von Daten an Dritte über die BMW-CarData-Plattform.

2. Tesla „Kundendatenschutzrichtlinie“

Tesla bietet sich für eine zweite Fallstudie an, weil der US-amerikanische Hersteller zu den Technologieführern im Bereich der vernetzten Mobilität gehört und zugleich außerhalb der Oligopol-Struktur der deutschen Automobilindustrie steht. Tesla differenziert in seiner

29 *BMW* (o. Fn. 26).

30 *Clauss*, BMW CarData Presentation, Präsentation vom 07.11.2017, abrufbar unter: <https://youtu.be/pcLsGapVkrY?t=632> (ab 10 Min. 32 Sek.).

31 Ebd. ab 14 Min. 25 Sek.

32 *Zimmermann/Zoller* (o. Fn. 26), S. 17.

33 *BMW*, Allgemeine Geschäfts- und Nutzungsbedingungen BMW ConnectedDrive, Stand: 31.10.2018, abrufbar unter: https://www.bmw-connecteddrive.de/gcdm/public/cdfupo/DE-de/policies/AGB_REGISTER/versions/majorVersion/7/minorVersion/0/documents/PDF/languages/DE.

„Kundendatenschutzrichtlinie“³⁴ (KDSRL) zunächst zwischen verschiedenen Datenarten: „Informationen von Ihnen, über Sie oder Ihre Geräte“, „Von Ihrem oder über Ihr Tesla-Fahrzeug“ und „Von oder über Ihre Tesla-Energieprodukte“. Differenziert wird zudem zwischen verschiedenen Arten der Datenverarbeitung: „Zur Kommunikation mit Ihnen“, „Um unsere Produkte und Dienstleistungen anzubieten und zu verbessern“ und „Für andere Zwecke“. Bei der Weitergabe unterscheidet die KDSRL zwischen „An unsere Dienstleister und Geschäftspartner“, „An von Ihnen genehmigte Dritte“, „In rechtlich vorgeschriebenen Fällen“ und „Unter anderen Umständen“, worunter sich beispielsweise auch die Weitergabe an den Arbeitgeber findet, wenn das Fahrzeug von einem Arbeitnehmer gefahren wird, „sofern dies nach geltendem Recht zulässig ist.“

Die rechtliche Konstruktion der Datenverarbeitung durch Tesla basiert auf einem Vertrag zwischen Tesla und dem Nutzer der Dienste (Einleitung KDSRL am Ende): „Indem Sie uns Informationen zur Verfügung stellen oder unsere Produkte oder Dienstleistungen in Anspruch nehmen, stimmen Sie den Bestimmungen und Bedingungen dieser Datenschutzrichtlinie zu.“ Im Weiteren wird nicht zwischen gesetzlichen Erlaubnistatbeständen und der Einwilligung in die Datenverarbeitung durch Tesla differenziert. Dies entspricht der auch im Internet verbreiteten Praxis, den Abgrenzungsschwierigkeiten bei den gesetzlichen Erlaubnistatbeständen des Datenschutzrechts durch eine weit gefasste Einwilligung des Kunden aus dem Weg zu gehen. Entsprechend umfassende Einwilligungserklärungen sind datenschutzrechtlich problematisch.³⁵ Von besonderem Interesse ist, dass auch Tesla die Weitergabe an Dritte – sofern es sich nicht um Dienstleister und Geschäftspartner von Tesla handelt – an eine gesonderte „Genehmigung“ des Kunden knüpft. Die Verträge zwischen Tesla und solchen Dritten, an die die Weitergabe mit Zustimmung des Kunden erfolgt, sind nicht öffentlich zugänglich.

VI. Vertragsverhältnisse und vertragsrechtliche Probleme bei der vernetzten Mobilität

Mangels staatlicher Regulierung organisieren sich die verschiedenen Märkte für Daten im Bereich der vernetzten Mobilität bislang auf Basis privatautonom ausgehandelter Verträge. Folgt man der ökonomischen Grundannahme, dass Verträge zu einer effizienten Allokation von Gütern und damit zu einer Steigerung der gesellschaftlichen Wohlfahrt führen, so sind die staatlichen Akteure auch gut beraten, zunächst einmal auf die Kräfte des Marktes zu vertrauen. Diese befinden sich gegenwärtig noch in einer Experimentierphase. Gleichwohl zeichnen sich erste Konturen ab, die auch bereits Hinweise auf mögliche Problemfelder eines Marktversagens enthalten. Überlegungen zu einem künftigen Vertragsrecht für die verschiedenen Datenmärkte müssen zum momentanen Zeitpunkt aber notgedrungen skizzenhaft bleiben.

1. Primärmarkt für Fahrzeugdaten

Auf dem Primärmarkt für Daten, die beim Betrieb vernetzter Fahrzeuge anfallen, ist zwischen verschiedenen Vertragsverhältnissen zu differenzieren:

a) Vertrag mit dem Kfz-Hersteller

Im Mittelpunkt des Interesses steht – jedenfalls im Moment – das Vertragsverhältnis zwischen dem Fahrzeugkäufer bzw. -nutzer und dem Fahrzeughersteller. Schon bei der Bestimmung der Vertragsparteien taucht jedoch das erste Problem auf: Knüpft man, so wie das oben beschriebene Vertragsmodell von BMW,

34 *Tesla*, Kundendatenschutzrichtlinie, Stand: 31.10.2018, abrufbar unter: https://www.tesla.com/de_DE/about/legal.

35 *Buchner/Kühling* in *Kühling/Buchner*, DS-GVO BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 61 ff.

an den Kaufvertrag über das Neufahrzeug an, so sind andere Nutzer des Fahrzeugs, insbesondere andere Fahrer, zunächst nicht erfasst. Knüpft man wie im Fall von Tesla an die Nutzung der Dienste und die Überlassung von Daten an, so dürfte dem Hersteller oft gar nicht bekannt sein, mit wem der Vertrag zustande kommt und wessen Daten verarbeitet werden. Auf der Seite des Fahrers wird es oft an einem Erklärungs-bewusstsein fehlen, welches für die Wirksamkeit bzw. Unanfechtbarkeit der Willenserklärung aber vorausgesetzt wird.³⁶ Zusätzliche Probleme ergeben sich, wenn das Fahrzeug veräußert wird. In den oben geschilderten Vertragsmodellen wird für die infolge der Vernetzung möglichen Dienste oft kein Zusatzentgelt erhoben, vielmehr sind die Dienste in den Kaufpreis des Fahrzeugs eingepreist.³⁷ Dies kann allerdings nicht darüber hinwegtäuschen, dass der Käufer heute neben dem Kaufpreis und einem etwaigen zusätzlichen Entgelt auch mit seinen Daten bezahlt, wenn er die Dienste seines vernetzten Fahrzeugs in Anspruch nimmt.³⁸ Hierbei darf jedoch die Rechtsgrundlage der Datenverarbeitung nicht aus dem Blick geraten. Diese kann, wie oben gezeigt, auch ohne Einwilligung des Betroffenen zulässig sein, etwa wenn sie zur Vertragserfüllung erforderlich ist. Sobald es sich aber um sensible Daten gem. Artikel 9 DS-GVO handelt, hilft indes nur noch die Einwilligung. Gleiches gilt für die Weitergabe an Dritte. Für den letztgenannten Fall scheint sich am Markt durchzusetzen, dass insoweit eine zusätzliche Einwilligung des Fahrers eingeholt wird.³⁹

In der schönen neuen Welt der Mobilitätsdaten lassen sich allerdings auch schon erste vertragsrechtliche Probleme erkennen. Die offenkundige Informationsasymmetrie zwischen Kfz-Herstellern und Fahrern kann durch die umfangreichen, zum Teil auch intransparenten Datenschutzhinweise der Hersteller kaum ausgeglichen werden. Selbst wenn dem Käufer die Datenschutzhinweise beim Abschluss des Kaufvertrags in ausgedruckter Form überreicht werden, wird dieser den „information overload“ kaum verarbeiten können. Werden die Datenschutzhinweise nur auf einem Display des Fahrzeugs – am besten noch während des Fahrens – angezeigt, wird die Vorstellung einer echten Informationsvermittlung an den Verbraucher vollkommen unrealistisch.⁴⁰ Hinzu treten die bekannten Probleme des „Privacy Paradox“⁴¹: Auch informierte Verbraucher neigen dazu, den Wert ihrer Daten zu verkennen und sie zu günstig preiszugeben. Weitere vertragsrechtliche Probleme können sich aus den Einschränkungen des Wettbewerbs ergeben, sobald man sich für ein Fahrzeug entschieden hat. Die oben näher untersuchten Hersteller gewähren insoweit zwar die Möglichkeit eines „Opt out“. In diesem Fall muss der Nutzer dann aber ganz auf die Vernetzungsfunktion des Fahrzeugs verzichten. Die genannten Probleme zeigen sich in verschärfter Form bei der datenschutzrechtlichen Bewertung der Einwilligung des Betroffenen, sofern diese für die konkrete Art der

36 Allgemein zum Erklärungsbewusstsein siehe *Rüthers/Stadler*, Allgemeiner Teil des BGB, 19. Aufl. 2017, S. 136 ff.; zu den weitergehenden Anforderungen des Art. 4 Nr. 11 DS-GVO siehe *Buchner/Kühling* (o. Fn. 34) Art. 7 DS-GVO Rn. 56, die hier vom „Einwilligungsbewusstsein“ sprechen.

37 Siehe aber die für die Bereitstellung einzelner Dienste bei BMW Connected Car geforderten Entgelte <https://www.bmw-connecteddrive.de/app/index.html#/portal/store>.

38 Zu Verträgen über Dienste gegen Daten siehe *Metzger/Efroni/Mischau/Metzger*, 9 (2018) JIPITEC 90 (92 ff.); *Metzger*, AcP 2016, 817; *Specht* in: DGRI Jahrbuch 2017; *Langhanke*, Daten als Leistung, Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz, 2018.

39 So sieht das NEVADA-Konzept des *VDA* (o. Fn. 5), S. 4, explizit die Einholung einer Einwilligung vor und verweist insofern ausdrücklich auf die Empfehlungen der Europäischen Kommission in *C-ITS Platform*, Final Report Phase I, January 2016, S. 11 f., abrufbar unter: <https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf>.

40 So aber *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (o. Fn. 15).

41 Siehe o. Fn. 1.

Datenverarbeitung eingeholt werden muss. Für die Kfz-Hersteller ist es keine triviale Aufgabe, Vertragsmodelle zu entwerfen, die alle Anforderungen des BGB-Vertragsrechts, insbesondere der §§ 305 ff. BGB, und der DS-GVO einhalten. Abschließende Aussagen sind dabei jeweils nur im Hinblick auf konkrete Vertragsklauseln und Datenschutzhinweise möglich.

b) Vertrag mit weiteren Anbietern (Aftermarket)

Zusätzlich zum Vertrag zwischen dem Hersteller und dem Käufer (oder Nutzer der Dienste) werden in Zukunft die Verträge zwischen dem Nutzer des Fahrzeugs und den Anbietern auf den benachbarten Märkten in den Mittelpunkt des Interesses rücken, beispielsweise der Versicherungsvertrag, für dessen Abschluss oder Leistungserbringung der Versicherer die Einwilligung des Versicherungsnehmers einholt, um die Fahrzeugdaten vom Kfz-Hersteller abrufen zu können. Hier kommen, wie oben gezeigt, ganz verschiedene Akteure in den Blick, insbesondere freie Händler und Werkstätten, Versicherungen, Apphersteller, Telematic-Service-Provider (TSP), private Straßenbetreiber (Maut), Mobilitätsdienstleister (z.B. Carsharing), die Werbewirtschaft etc. Für jeden dieser Akteure wird sich die Frage stellen, ob die Datenverarbeitung auf einen gesetzlichen Erlaubnistatbestand gestützt werden kann oder ob zusätzlich zum Vertrag über die erbrachte Dienstleistung (oder als Bestandteil eines solchen Vertrags) eine datenschutzrechtliche Einwilligung erforderlich ist. Willigt der Kunde in einem solchen Vertrag in die Verarbeitung seiner Daten ein, so kann es sich hierbei um eine versteckte Gegenleistung neben dem eigentlichen Entgelt handeln. Die vertrags- und datenschutzrechtlichen Probleme ähneln denjenigen, die sich bei den Verträgen mit den Kfz-Herstellern zeigen.

2. Sekundärmarkt für Fahrzeugdaten

Auf dem Sekundärmarkt für Daten, auf dem der Kfz-Hersteller Dritten Zugang zu den Daten seiner Kunden gewährt, ist zwischen der Weitergabe personenbezogener und anonymisierter Daten zu unterscheiden:

a) Verträge über personenbezogene Daten

Eine Weitergabe personenbezogener Daten durch den Kfz-Hersteller an Anbieter auf nachgelagerten Märkten kommt, wie oben gesehen, nur auf Grundlage einer konkret auf diesen Zweck bezogenen Einwilligung des Betroffenen in Frage. Die oben näher beleuchteten Vertragsmodelle von BMW bzw. Tesla sehen dies vor, auch wenn der Kreis der anderen Unternehmen, an die eine Weitergabe auch ohne ausdrücklich hierauf bezogene Einwilligung zulässig sein soll, sehr weit gezogen wird. Die vertraglichen Absprachen zwischen den Kfz-Herstellern und den Anbietern auf den nachgelagerten Märkten sind, mit einer Ausnahme, nicht öffentlich zugänglich. Im Fall BMW sind zwar die „Nutzungsbedingungen“ eines „Aftersales Online Systems“ online abrufbar, auf welchem die Datenweitergabe an unabhängige Werkstätten und Händler erfolgt. Die Verträge über die Datenweitergabe an sonstige Dritte, bspw. Versicherungen, können von der Öffentlichkeit dagegen nicht eingesehen werden. Gleiches gilt für die Datenweitergabe durch Tesla. Es wäre wünschenswert, dass die anwendbaren Vertragsbedingungen veröffentlicht würden, um die Transparenz der Modelle zu erhöhen und das Vertrauen der Nutzer zu stärken.

Rechtliche Probleme können sich für entsprechende Vereinbarungen zunächst aus dem Datenschutzrecht ergeben, wenn die Anforderungen an eine datenschutzkonforme Einwilligung nicht eingehalten werden. Die durch die DS-GVO entstandene Rechtsunsicherheit behindert die Entwicklung datenbasierter Dienste auf den nachgelagerten Märkten und sorgt für erhebliche Transaktionskosten. Weitere Rechtsfragen können sich ergeben, wenn Kfz-Hersteller, anstatt einen diskriminierungsfreien Zugang für Drittanbieter zu ermöglichen, ausschließlich selektiv mit einzelnen Partnerunternehmen zusammenarbeiten. Dies gilt umso mehr, wenn sich Kfz-Hersteller, wie dies in der Vergangenheit schon öfter der Fall war, koordinieren. Insoweit ist das Wettbewerbsrecht berufen, wettbewerbswidrige Absprachen bzw. den Missbrauch marktbeherrschender

Stellungen abzustellen. Ob und unter welchen Voraussetzungen der Gesetzgeber über das heutige Wettbewerbsrecht hinausgehen sollte, um weitere Zugangsrechte zu Daten zu schaffen, gehört zu den meist diskutierten Fragen in der aktuellen Debatte.⁴² Schließlich stellt sich für Kfz-Hersteller die nach wie vor ungeklärte Frage, was eigentlich der Gegenstand von Verträgen mit Anbietern auf den nachgelagerten Märkten ist. Rein faktisch wird der Zugang zu Kundendaten gewährt. Ein die Position der Kfz-Hersteller schützendes Immaterialgüterrecht an Daten, welches Gegenstand eines Lizenzvertrags sein könnte, gibt es bislang nicht und dürfte es auch in naher Zukunft nicht geben. Sofern nicht ausnahmsweise die Voraussetzungen für ein Datenbankherstellerrecht gem. § 87a UrhG oder für ein Geschäftsgeheimnis im Sinne der Richtlinie 2016/943/EU vorliegen, muss der Kfz-Hersteller schuldrechtliche Absprachen treffen, die die Verwendung der Daten durch den Vertragspartner beschreiben und einschränken. Verstöße gegen die vertraglichen Absprachen können dabei mit Vertragsstrafen bewehrt werden, um eine effektive Durchsetzung von Ansprüchen sicherzustellen.

b) Verträge über anonymisierte Daten

Gewährt der Kfz-Hersteller Zugang zu anonymisierten Daten, so entfallen die datenschutzrechtlichen Vorgaben und Rechtsprobleme. Dies setzt allerdings voraus, dass niemand – auch nicht der Kfz-Hersteller selbst – mehr auf die betroffenen Personen schließen kann.⁴³ Entsprechende Daten können gleichwohl für Dienstleister auf nachgelagerten Märkten von großem wirtschaftlichem Wert sein, etwa für die Marktforschung. Abgesehen vom Datenschutzrecht stellen sich insoweit aber die gleichen rechtlichen Fragen wie bei der Weitergabe personenbezogener Daten, insbesondere im Hinblick auf das Wettbewerbsrecht und die schuldrechtliche Absicherung unter Verzicht auf Immaterialgüterrechte.

VII. Schlussfolgerungen

Die Verarbeitung und Weitergabe von Daten beim vernetzten Fahren erfolgt – Stand heute – vornehmlich auf Basis von Vertragsverhältnissen zwischen dem Kfz-Hersteller, dem Fahrzeugkäufer bzw. -nutzer und weiteren Akteuren auf den nachgelagerten Märkten. Die Akteure nutzen miteinander verwobene Verträge, um ihre zum Teil gleich-, zum Teil gegenläufigen Interessen auszutarieren, abzusichern, und um mit verschiedenen Geschäftsmodellen zu experimentieren. Nach dem vorläufigen Scheitern der Pläne für die Einführung eines Immaterialgüterrechts für Daten sind die Absprachen der Beteiligten dabei allein schuldrechtlicher Natur. Dass die privatautonom ausgehandelten Verträge der verschiedenen Akteure und das Vertragsrecht die wesentlichen rechtlichen Strukturen für die entstehenden Dienste der digitalen Mobilität liefern, sollte in einer Marktwirtschaft nicht überraschen. In Anbetracht des internationalen Wettbewerbs um die Technologie- und Marktführerschaft bei der digitalen Mobilität ist der Freiraum, den das Vertragsrecht den Akteuren lässt, von zentraler Bedeutung. Jede staatliche Regulierung muss deshalb mit Augenmaß vorgehen. Dies betrifft zunächst das Datenschutzrecht. Die Rechtmäßigkeit der Datenverarbeitung durch Kfz-Hersteller und andere Anbieter ist heute in vielen Konstellationen an den gesetzlichen Erlaubnistatbeständen von Artikel 6 Abs. 1 lit. b) - f) DS-GVO zu messen. Bei der weiteren Entwicklung vernetzter Mobilitätsdienste sollte sorgsam erwogen werden, ob nicht zusätzliche gesetzliche Erlaubnistatbestände im Rahmen von Artikel 6 Abs. 1 lit. c) DS-GVO (rechtliche Verpflichtungen des

42 Hierzu Heike Schweitzer in diesem Heft der GRUR.

43 *Weichert* (o. Fn. 10), 205. Die AGB von BMW Connected Drive gehen zutreffend davon aus, dass bei einer bloßen „De-Personalisierung“, bei der „die Daten nicht mehr unmittelbar auf Sie oder Ihr Fahrzeug zurückzuführen sind“, weiter von personenbezogenen Daten auszugehen ist, für deren Verarbeitung eine Rechtsgrundlage erforderlich ist, siehe *BMW* (o. Fn. 30), Datenschutzhinweise – Punkt C.

Verantwortlichen) für ein Mehr an Rechtssicherheit für alle Beteiligten sorgen können. Daneben wird die Einwilligung weiter von Bedeutung bleiben, insbesondere bei der Weitergabe von personenbezogenen Daten an Dritte und bei sensiblen Daten gem. Artikel 9 DS-GVO. Kfz-Hersteller und Datenschutzbehörden sollten gemeinsam vorgehen, um die Entwicklung und Etablierung von Mobilitätsdiensten zu erleichtern, die das europäische Datenschutzniveau einhalten. Auf dem Sekundärmarkt für die von Fahrzeugen gesammelten Daten sind in der Praxis erste Geschäftsmodelle zu erkennen, deren vertragliche Grundlagen aber nicht öffentlich zugänglich sind. Kfz-Hersteller sollten hier der Forderung der EU-Kommission nach mehr Transparenz nachkommen. Ob es neben dem Datenschutzrecht weiterer regulatorischer Eingriffe bedarf, um Wettbewerb auf den nachgelagerten Märkten zu ermöglichen, muss die Entwicklung der nächsten Jahre zeigen. Die Diskussion über (sektorspezifische) Zugangsrechte zu Daten jenseits der bereits vorhandenen Regelungen hat gerade erst begonnen.