baum ▪ reiter & collegen Benrather Schlossallee 101 · D-40597 Düsseldorf

Düsseldorf, den 02.12.2016
MET

Rechtsgutachten zur Kontrolle der Daten bei vernetzten und automatisierten Pkw

Der Verbraucherzentrale Bundesverband e.V. (vzbv) hat die Problemstellung identifiziert, dass Verbraucher im Zuge der fortschreitenden Digitalisierung und Vernetzung des Autos zunehmend die Möglichkeit und das Recht auf Ausübung der Souveränität über ihre Daten verlieren. Verbraucher müssen sich aber darauf verlassen können, dass es für ihre Autos ein angemessenes Datenschutz- und Datensicherheitsniveau gibt, dass dieses Niveau bereits bei der Zulassung von Neufahrzeugen geprüft wird und dass es auch Gegenstand der regelmäßigen Hauptuntersuchungen des Fahrzeugs ist.

Im vorliegenden Rechtsgutachten wird im Auftrag des vzbv untersucht, wie der Anspruch von Verbrauchern auf Datensouveränität und Kontrolle der eingesetzten Software und Programmierungen im Auto durch Rechtsanpassungen und Gesetzesinitiativen durchgesetzt werden kann. Ebenso wird geprüft, durch welche gesetzgeberischen Maßnahmen die Einhaltung von Datenschutz und –sicherheit in den Rechtsgrundlagen für die Zulassungsverfahren und für die technische Prüfung von Pkw sichergestellt werden kann. Darüber hinaus ist Gegenstand des Gutachtens die Frage, wie die während der Fahrt generierten personenbezogenen Daten gegenüber Dritten geschützt werden können und die Vorgaben der Datenschutz-Grundverordnung umzusetzen sind.

Gerhart R. Baum
Bundesminister a. D.*
Rechtsanwalt

Prof. Dr. iur. Julius Reiter
Professor für Wirtschaftsrecht**
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Informationstechnologierecht

Dr. iur. Olaf Methner
Fachanwalt für Bank- und Kapitalmarktrecht
Fachanwalt für Arbeitsrecht
Fachanwalt für Informationstechnologierecht
Lehrbeauftragter FH**

Andrea Burghard, LL.M.
Fachanwältin für Bank- und Kapitalmarktrecht
Fachanwältin für Arbeitsrecht
Zertifizierte Datenschutzbeauftragte

Sylvia Klotzky
Rechtsanwältin

Bénédict Schenkel
Maîtrise en droit, Mag. iur.
Rechtsanwalt
Zertifizierter Datenschutzbeauftragter

Vitalija Mickeviciute
Rechtsanwältin

Sonja Steigerwald
Rechtsanwältin

Christian Leuchter
Rechtsanwalt

Sarah Behrendt
Rechtsanwältin
Zertifizierte Datenschutzbeauftragte

Paiman Manguri
Rechtsanwältin

Marc H. Sundermann
Rechtsanwalt

Benrather Schlossallee 101
40597 Düsseldorf
Fon: +49-(0) 211-836 805.70
Fax: +49-(0) 211-836 805.78
www.baum-reiter.de
kanzlei@baum-reiter.de

* Ubierring 50 · D-50678 Köln
** FOM Hochschule für Oekonomie & Management

Erster Abschnitt: Einführung

I. Einleitung

Ständige Weiterentwicklung und Innovationen in der Fahrzeugtechnik führen dazu, dass auch die rechtlichen Grundlagen für die Produktion sichererer und umweltschonenderer Fahrzeuge angepasst werden müssen. Ab den 1960er-Jahren konnten Fahrzeugkomponenten in Echtzeit Daten austauschen, womit sich z. B. das Antiblockiersystem (ABS) und das Elektronische Stabilisierungsprogramm (ESP) realisieren ließen. Die Einführung von solchen Systemen, die Assistenz für den Fahrer leisten, wurden vorwiegend durch technische Regelungen der Economic Commission for Europe (ECE) rechtlich abgesichert.

Die rechtlichen Rahmenbedingungen für den technischen Fortschritt, wurden allerdings bisher nur unzureichend oder gar nicht angepasst: So ist das Wiener Weltabkommen über den Straßenverkehr seit 1968 nahezu unverändert geblieben.[1] Lediglich im Hinblick auf die Entwicklung autonomer Fahrzeuge wurde im Mai 2014 die Zulässigkeit von Systemen ermöglicht, mit denen ein Kfz autonom fährt. Voraussetzung ist allerdings, dass die Systeme jederzeit vom Fahrer gestoppt werden können.[2]

Dass die rechtlichen Rahmenbedingungen hinter dem Stand der Technik zurückbleiben, ist umso problematischer, als nach dem bisherigen Stand der Technik bereits eine Vielzahl von Datenerhebungen und -verarbeitungen im Fahrzeug stattfindet. Weitere Innovationen in der Fahrzeugtechnik führen vermehrt zur informationstechnischen Interaktion zwischen Fahrzeugen. Dabei können auch Fahrzeugdaten an Dritte wie Autovermietungsunternehmen, Versicherungen, Werkstätten oder Car-Sharing-Anbieter übermittelt werden, was sich als datenschutzrechtlich problematisch erweist.

II. Stufen der Automation nach SAE-Standard

Ein vernetztes Fahrzeug ist im Grundsatz ein mit Kommunikationstechnologie ausgestattetes Auto. Es erlaubt einen direkten Datenaustausch zwischen der Außenwelt und dem Fahrzeug, ohne dass es hierfür eines gesonderten mobilen Gerätes bedarf.

Mit einem automatisierten Fahrzeug kann aufgrund automatisierter Durchführung einzelner Aktivitäten das Fahren komfortabler, effizienter und sicherer werden.

---

[1] Vgl. *Bönninger*, „Wem gehören die Daten im Fahrzeug? Das moderne Fahrzeug – Messgerät, Steuergerät, Datenspeicher“, in: Tagungsband des 52. Deutschen Verkehrsgerichtstags 2014, 229, 230.
[2] Hierzu noch nachfolgend unter II.2.1.

Zur Klassifizierung der Automatisierungsgrade der einzelnen Systeme wurden auf nationaler und internationaler Ebene sechs Stufen von 0 bis 5 definiert:

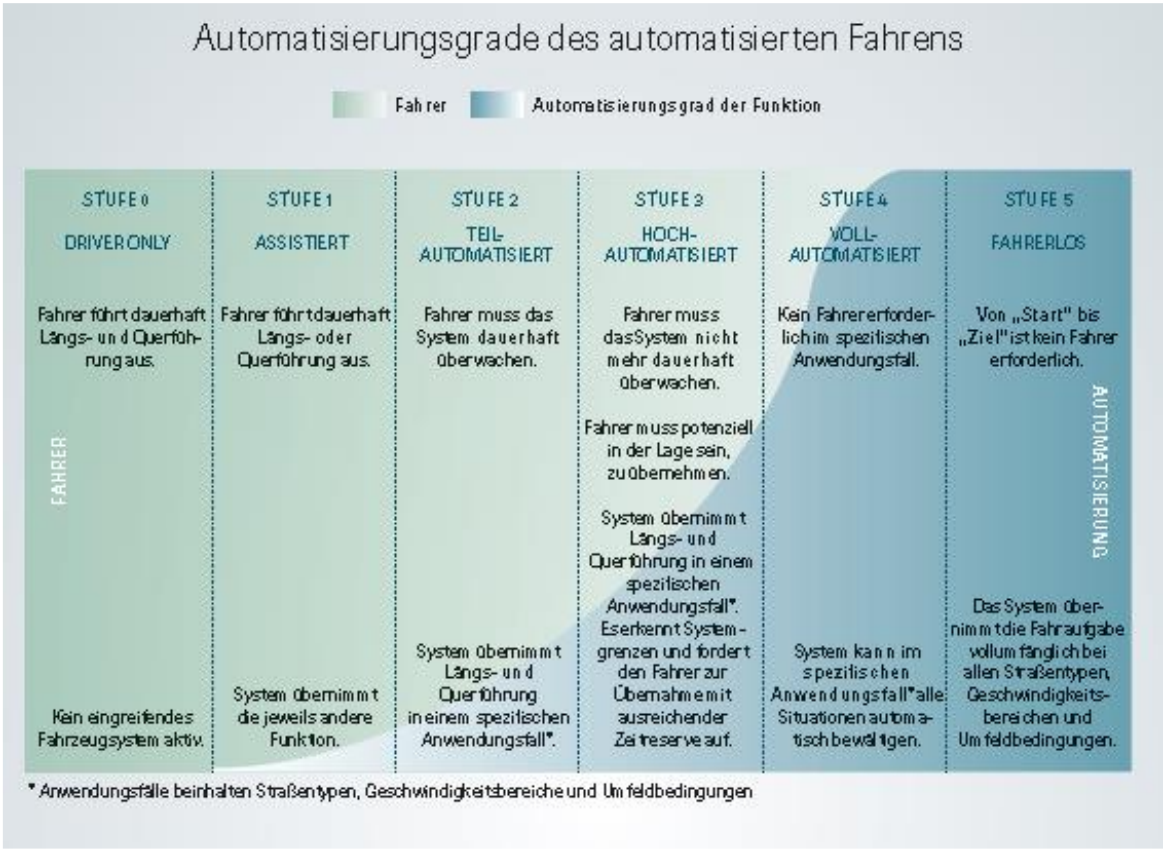


Abb. 1: Automatisierungsgrade des automatisierten Fahrens; Quelle: Verband der Automobilindustrie, „Automatisierung – Von Fahrerassistenzsystemen zum automatisierten Fahren", Berlin 2015, S.15

Die heute weit verbreiteten Fahrerassistenzsysteme, wie wir sie schon seit nahezu 40 Jahren in Form von Systemen wie dem Anti-Blockier System (ABS), Electronic Stability Program (ESP) und dem Adaptive Cruise Control (ACC) kennen, werden ständig weiterentwickelt und sind die Vorstufe zum automatisierten Fahren.

Einige Fahrzeuge verfügen heute schon über Funktionen der Stufe 2 (teilautomatisiert), bei denen die Längs- und Querführung des Fahrzeugs für einen gewissen Zeitraum oder in spezifischen Situationen vom System übernommen wird. Der Fahrer muss die automatischen Funktionen jedoch ständig überwachen und darf keiner fahrfremden Tätigkeit nachgehen.

Hochautomatisierte Fahrfunktionen der Stufe 3 befinden sich derzeit in der Entwicklung und Erprobung. Hierfür hat die Bundesregierung im September 2015 ein „Digitales Testfeld Autobahn“ auf der Autobahn A9 in Bayern geschaffen.[3] Hochautomatisierte Fahrfunktionen unterscheiden sich im Vergleich zu den vorstehend beschriebenen Automatisierungsstufen im Wesentlichen dadurch, dass das System seine Grenzen selbst erkennt und in diesem Fall die Übernahme durch den Fahrer rechtzeitig anfordert. Fahrfremde Tätigkeiten des Fahrers sind begrenzt zulässig.

Beim vollautomatisierten Fahren kann der Fahrer alle Fahraufgaben dem System in spezifischen Anwendungsfällen übergeben. Die Anwendungsfälle beinhalten neben dem Straßentyp und dem Geschwindigkeitsbereich auch die Umweltbedingungen.

Die letzte Entwicklungsstufe 5 bezeichnet das autonome Fahren. Hierbei kann das Fahrzeug alle vorgenannten Situationen autonom bewältigen, sodass eine Überwachung durch den Fahrer nicht mehr erforderlich ist.

III. Einführungsstrategien für automatisiertes Fahren

Bereits heute sind Systeme zur automatisierten Unterstützung bei der Längsführung in modernen Fahrzeugen vorhanden. Erste automatisierte Fahrfunktionen sind beispielsweise der Staupilot auf der Autobahn oder das Einparken in der Stadt. Zunehmend wird auch eine Unterstützung des Fahrers bei der Querführung seines Fahrzeugs durch den Einbau automatisierter Fahrfunktionen zu erwarten sein.

Um diese Funktionen vermehrt einsetzen zu können, liegt der Fokus der Entwicklung bei den Automobilherstellern derzeit auf der Weiterentwicklung bordeigener Sensorik.

Eine langfristige Einführung automatisierter Fahrfunktionen wird von den aktuellen Automobilherstellern bevorzugt, nicht zuletzt aufgrund der langen Investitionszeiträume und den hohen Systemkosten für den Fahrzeugkäufer.[4]

---

[3] Frauenhofer-Institut für Arbeitswirtschaft und Organisation IAO, Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen – Dienstleistungsprojekt 15/14, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie.

[4] *Beiker, S.*: Einführungsszenarien für höhergradig automatisierte Straßenfahrzeuge, in: Autonomes Fahren. Technische, rechtliche und gesellschaftsrechtliche Aspekte, Berlin, 2015: Springer Berlin Heidelberg, S. 197 ff.

IV. Arten der Fahrzeugdaten

Zur Beurteilung, wie man die Erhebung und Verarbeitung von Daten im vernetzten und automatisierten Pkw regeln kann, wird zunächst ein kurzer Überblick über die einzelnen Fahrzeugdaten gegeben.

Bereits heutzutage wird in vernetzten Fahrzeugen eine Reihe von Daten erhoben und verarbeitet.

Zunächst einmal zählen hierzu alle Arten von Standort- und Navigationsdaten. Dies umfasst typischerweise Reiseziele, -zeiten und –gewohnheiten.

Ein aktuelles Beispiel für die Erhebung von Standortdaten aufgrund gesetzlicher Vorgaben ist ferner das europäische eCall-System, das über Sensoren bei einem schweren Unfall automatisch aktiviert wird oder vom Fahrer selbstständig aktiviert werden kann.[5]

Aus verschiedenen Lokationsdaten können über einen gewissen Zeitraum hinweg Daten zum Fahrverhalten abgeleitet werden.

Fahrdynamikdaten erfassen Beschleunigungs- und Verzögerungsvorgänge. Sie liefern Daten zum Verhalten des Fahrzeugs und des Fahrzeugführers, mit denen Aussagen über den Fahrstil getroffen werden können.

Zu den Umgebungsdaten zählen Daten über andere Verkehrsteilnehmer sowie Bildmaterial von Personen.

Mit zunehmender informationstechnischer Ausstattung der Fahrzeuge, Vernetzung der Verkehrsteilnehmer untereinander sowie Anbindung an das Internet ist künftig mit einer Erhebung weiterer Daten abhängig von verschiedenen Einsatzszenarien zu rechnen. Insbesondere werden künftig weitere Daten über die Fähigkeiten und das Fahrverhalten des Fahrers erfasst, beispielsweise unter welchen Umständen der Fahrer die Kontrolle über das Fahrzeug abgibt oder zurückfordert, ob er in der Lage ist, die Kontrolle vom System zurück zu übernehmen und wie lange der Wechsel dauert.

Beim Einsatz eines Parkroboters, dessen Entwicklung künftig zu erwarten ist, werden hingegen mangels Wechselwirkung keine Daten zum Fahrverhalten erfasst.

[5] Vgl. hierzu nähere Ausführungen im dritten Abschnitt, ___.

V. Personenbezug der Kfz-Daten

1. EU-Datenschutzgrundverordnung

Mit der EU-Datenschutzgrundverordnung wird in Europa nach 20 Jahren ein neuer und einheitlicher Rechtsrahmen für den Datenschutz in Form einer EU-Verordnung geschaffen.

Eine wesentliche Änderung in territorialer Hinsicht wird durch die Einführung des sogenannten *Marktortprinzips* bewirkt.

Danach greift die Datenschutzgesetzgebung der Europäischen Union künftig nicht nur dann, wenn die Verarbeitung von personenbezogenen Daten im Kontext einer Niederlassung in der EU stattfindet, Art. 3 Nr. 1 DSGVO, sondern auch wenn sie Personen betrifft, die sich in der Union befinden und die Verarbeitung durch einen nicht in der Union niedergelassenen Verantwortlichen erfolgt, Art. 3 Nr. 2 DSGVO.

Ziele der Datenschutzgrundverordnung sind eine Modernisierung und Verbesserung des Grundrechtsschutzes angesichts der technischen Entwicklungen, die Harmonisierung und Schaffung eines soliden kohärenten und durchsetzbaren Rechtsrahmens im Bereich des Datenschutzes in der Union, sowie die Stärkung des Binnenmarktes durch einheitliche Vorgaben für gleiche wirtschaftliche Bedingungen.

2. Anwendung der DSGVO für Fahrzeugdaten

Zentral für die Entscheidung, ob eine Datenverarbeitung unter den sachlichen Anwendungsbereich der DSGVO fällt, ist naturgemäß die Definition der personenbezogenen Daten. Seit der Einführung des Datenschutzrechts war diese Definition immer wieder Gegenstand von Urteilen und Debatten, weshalb von der Datenschutzreform insbesondere eine Stärkung der Rechtssicherheit bei Betroffenen und Anwendern durch eine einheitliche Definition im Rahmen der Verordnung erwartet wurde.

Die Definition des Begriffs der personenbezogenen Daten bleibt jedoch auch im Rahmen der DSGVO weitestgehend identisch mit § 3 BDSG. Gemäß Art. 4 Nr. 1 DSGVO 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 identifiziert werden kann.[6]

Eine Neuerung ist die expliziert aufgenommene Definition für das sogenannte „Profiling", den Vorgang der Pseudonymisierung personenbezogener Daten und der betroffenen Drittpartei.

Die im Kfz erhobenen Daten betreffen zunächst einmal das jeweilige Fahrzeug und keine natürliche Person. Nach der obigen Darstellung sind sachbezogene Daten dem Grundsatz nicht personenbezogen.

Die meisten der beim Fahren erzeugten Daten enthalten jedoch Informationen und Rückschlüsse über die Gewohnheiten des Fahrzeugführers und weisen demnach einen Personenbezug auf. Damit wird das Kfz auch selbst zu einem informationstechnischen System, wodurch der Schutzbereich des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme betroffen ist.[7]

Ein Personenbezug von Daten ist nur dann zu verneinen, wenn sie technisch sicher anonymisiert werden. Eine Zuordnung der Daten zu dem Fahrer, Eigentümer, Halter sonstigen Insassen oder Personen, muss rechtlich und technisch ausgeschlossen sein. Ansonsten dürfte die Hoheit über die im Fahrzeug anfallenden Daten nach geltendem Recht grundsätzlich beim Halter liegen, soweit es sich um personenbezogene oder zumindest personenbeziehbare Daten handelt.[8]

Der Verband der Automobilindustrie (VDA) und die Datenschutzbehörden des Bundes und der Länder in Deutschland haben in einer gemeinsamen Erklärung vom 26.01.2016 klargestellt, dass Daten, die bei der Kfz-Nutzung anfallen, jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes sind, wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt. Des Weiteren unterscheiden die Behörden und der VDA in ihrer gemeinsamen Erklärung zwischen sog. *„Offline"*- und *„Online"*-Autos.[9]

Diese Erklärung ist im Sinne der Rechtsklarheit zu begrüßen.

---

[6] Art. 4 Nr. 1 DSGVO, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE, (zuletzt abgerufen am 26.09.2016).
[7] Vgl. BVerfG, Urt. v. 27.02.2008, 1 BvR 370/07, 595/07, BVerfGE 120, 274.
[8] Vgl. Weichert, Datenschutz im Auto, in: Tagungsband des 52. Deutschen Verkehrsgerichtstags 2014, 285, 291; Hilgendorf, Automatisiertes Fahren und Recht, in: Tagungsband des 53. Deutschen Verkehrsgerichtstags 2015, 55, 65.
[9] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26.01.2016, abrufbar unter

Aus Sicht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erscheinen im Hinblick auf die Verknüpfbarkeit mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen alle bei der Nutzung von Fahrzeugen anfallenden Daten als personenbezogen und datenschutzrechtlich relevant.[10]

VI. Betroffene/Verfügungsberechtigte

Mit der zunehmenden Vernetzung des Fahrzeugs wird auch der Kreis der Betroffenen und der an den Daten Interessierten erweitert.

Im Straßenverkehr ist eine klare Abgrenzung der Betroffenheit oftmals schwierig, da regelmäßig Kfz-Daten oder Umgebungsdaten erhoben werden. Neben den eigentlichen Nutzern des Fahrzeugs (Halter, Fahrer, Insassen) ist eine Vielzahl weiterer Personen mit ihren jeweiligen Interessen beteiligt. Diese haben zum Teil unterschiedliche Interessen hinsichtlich des Fahrkomforts, der Fahrsicherheit und an der Nutzung von Internet- und Multimediaanwendungen.

Schon bisher haben neben dem Fahrzeughersteller und deren Zulieferer auch die Werkstätten ein besonderes Interesse an den erhobenen Daten, um ihre Produkte, Reparaturen und Serviceangebote zu verbessern.

Mit dem Einzug des Internet in das Fahrzeug wollen ferner Internet Service Provider, Anbieter von Unterhaltungselektronik u.a. Dienstleister ihre Angebote einbringen.

Für all diese Dienstleister, die Service- und Unterhaltungsangebote für den Fahrer bereitstellen, sind in diesem Zusammenhang insbesondere die Daten, die das Fahrzeug über die Bordelektronik generiert, von eminentem wirtschaftlichem Interesse. Durch die erhobenen Präferenzen besteht die Möglichkeit gezielte Werbeangebote an die Insassen zu richten. Im Bereich des vernetzten Fahrzeugs wird bis 2020 weltweit mit einem Umsatzwachstum von 31 Milliarden Euro im Jahr 2015 auf mehr als 113 Mrd. Euro gerechnet.[11]

Schließlich sind im Fahrzeug generierte Daten in verschiedenen Situationen auch staatliche Stellen von Interesse. Für die Organisation des vernetzten und automatisierten Verkehrs sind in erster Linie Bewegungs- und Umfelddaten erforderlich. Gerade im Bereich der Car-to-Infrastruktur Kommunikation erhofft man sich eine Chance für die Einführung intelligenter Verkehrssysteme und automatisierter Mautverfahren.

---

[10] BfDI, 25. Tätigkeitsbericht zum Datenschutz vom 17.06.2015, S. 208.
[11] *Hornung, Gerrit / Goeble, Thilo*: „Data Ownership“ im vernetzten Automobil, CR 4/2015, 265, 267.

VII. Datenschutzrechtliche Verantwortlichkeit

Nach der Legaldefinition des Art. 4 Nr. 7 DSGVO ist der „Verantwortliche“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Entscheidend für die datenschutzrechtliche Verantwortlichkeit ist demnach die Einflussnahme auf den Zweck und die Mittel der Verarbeitung von personenbezogenen Daten.[12] Diese Definition findet sich bereits in Art. 2 lit. d) EU-DSRL. In diesem Zusammenhang wird vom Verwaltungsgericht Schleswig die Ansicht vertreten, dass eine Verantwortlichkeit nicht besteht, soweit eine Stelle eine vorgegebene Form der Datenverarbeitung nutzt, ohne Verfügungsgewalt über die Daten zu haben.[13] Folgt man der restriktiven Auslegung des VG Schleswig, könnte eine datenerhebende Stelle in Deutschland einen datenschutzwidrigen Dienst zur Verfügung stellen, der die Festlegung der Datenverarbeitung übernimmt, ohne hierfür datenschutzrechtlich zur Verantwortung gezogen zu werden.

Nach dem Wortlaut des Art. 4 Nr. 7 DSGVO ist auch eine gemeinsame Verantwortlichkeit mehrerer Stellen möglich.[14]

Für die Bestimmung, ob eine Erhebung durch eine verantwortliche Stelle stattfindet, ist zunächst danach zu unterscheiden, ob die Daten nur im Fahrzeug oder auf dem Server des Herstellers oder eines Dritten oder in einer Cloud gespeichert werden.

Findet die Datenspeicherung zunächst ausschließlich im Kfz statt, werden Daten erst erhoben, wenn sie verwendet werden, wie beispielsweise beim Auslesen in der Werkstatt. Werden Daten direkt aus dem Fahrzeug heraus übermittelt, ist bereits zu diesem Zeitpunkt von einer Erhebung im Sinne von DSGVO auszugehen.

VIII. Pflichten bei der Verarbeitung personenbezogener Daten

Für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten orientiert sich das Datenschutzrecht auch künftig an dem Grundsatz des sogenannten *Verbots mit Erlaubnisvorbehalt*.

---

[12] Vgl. Art. 4 Abs. 7 DSGVO
[13] VG Schleswig, Urt. v. 09.10.2013 - 8 A 218/11, DuD 2014, 120 = MMR 2014, 51 m. krit. Anmerkung Karg, dagegen auch Weichert, MMR 2014, 1 f.
[14] Vgl. ausdrücklich Art. 4 Abs. 7 DSGVO: abrufbar unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf (zuletzt abgerufen am 29.08.2016).

Danach ist eine Verarbeitung personenbezogener Daten grundsätzlich verboten, sofern diese nicht durch eine ausdrückliche gesetzliche Regelung oder die Einwilligung des Betroffenen erlaubt ist.

Eine Neuerung dürfte hingegen das von der DSGVO verfolgte Rechtmäßigkeitskonzept sein. Nach deutschem Recht war es bisher jedenfalls streitig, ob eine Datenverarbeitung kumulativ auf eine Einwilligung und einen gesetzlichen Erlaubnistatbestand gestützt werden konnte. Nach dem Wortlaut des Art. 6 DSGVO reicht nunmehr die Erfüllung mindestens einer Bedingung aus, sodass eine alternative Rechtfertigung möglich ist.

Von Bedeutung insbesondere im Bereich der Fahrzeugdaten sind die Einhaltung des Grundsatzes der Datensparsamkeit, des Transparenzprinzips sowie der Löschpflichten.[15]

1. Datensparsamkeit

Die Prinzipien der Datenminimierung und Datensparsamkeit sind nunmehr in Art. 5 Abs. 1 lit. c) DSGVO verankert. Danach müssen die personenbezogenen Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Darüber hinaus wird durch die Norm des Art. 25 DSGVO nunmehr ausdrücklich Datenschutz durch Technikgestaltung („Privacy by Design“) und durch datenschutzrechtliche Voreinstellung („Privacy by Default“) vorgeschrieben.

Das vernetzte Fahrzeug eröffnet allerdings auch einen neuen Markt, in dem das Internet Einzug in das traditionelle Produkt „Auto“ erhält. Nicht nur die Wirtschaft, sondern auch die Bundesregierung sieht in der Datennutzung ein enormes Wertschöpfungspotential.[16]

Um einerseits den Grundsatz der Datenminimierung in Art. 5 Abs. 1 lit. c DSGVO zu wahren[17], andererseits die innovativen Dienste am vernetzten Fahrzeug zu fördern, wird angeregt, dass die im Kfz erzeugten anonymen Daten in ihrer Rohform ähnlich den Leitlinien von „open data“ und „open innovation“ allgemein zur Verfügung gestellt werden.[18] Eine gesetzliche Regelung hierzu könnte in das IT-Sicherheitsgesetz aufgenommen werden.

Darüber hinaus sollte eine gesetzliche Grundlage dafür geschaffen werden, solche Daten, die für die Sicherheit und die Funktionalität des Verkehrs notwendig sind, gleichermaßen allen

[15] Siehe hierzu ausführlich Ausführungen im zweiten Abschnitt, Zweites und Drittes Kapitel
[16] Antwort der Bundesregierung auf die kleine Anfrage der Fraktion Bündnis 90/Die Grünen: Datenzugriff und Datenschutz bei digitalisierten und vernetzten Fahrzeugen, BT-Drucks. 18/10192, abrufbar unter dip21.bundestag.de/dip21/btd/18/101/1810192.pdf (zuletzt abgerufen am 10.11.2016).
[17] Vgl. Ausführungen zum Grundsatz der Datensparsamkeit im ersten Abschnitt, S. 8 d.Gutachtens.
[18] Vgl. *Hornung/Goeble*, „Data Ownership im vernetzten Automobil, in: CR 4/2015, S. 265, 272.

Verkehrsteilnehmern zur Verfügung zu stellen. Die Pflicht zur Übermittlung wäre mit der Vorgabe zu verbinden, diese Daten sicher zu anonymisieren, um einen wirksamen Schutz der betroffenen Verkehrsteilnehmer zu gewährleisten.

2. Transparenzprinzip

Der in Art. 5 Abs. 1 lit. c DSGVO verankerte Transparenzgrundsatz zählt zu den wesentlichen Prinzipien der Verordnung. Art. 12 Abs. 1 DSGVO verpflichtet den Verantwortlichen, die betroffene Personen grundsätzlich von der Verarbeitung ihrer personenbezogenen Daten „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer einfachen und klaren Sprache“ zu unterrichten. Dabei sehen vor allem Art. 12 bis Art. 15 DSGVO umfangreiche Unterrichtungsrechte betroffener Personen und Auskunftspflichten Verantwortlicher vor. Verstöße gegen die Transparenzvorschriften werden mit dem erhöhten Bußgeldrahmen von bis zu 4 Prozent des Umsatzes geahndet.

3. Löschpflichten

Die DSGVO sieht umfassende Löschpflichten vor. Art. 17 DSGVO normiert das Recht auf die Löschung personenbezogener Daten. Liegt einer der in Art. 17 Abs. 1 DSGVO genannten Gründe vor, muss der Verantwortliche personenbezogene Daten ohne unangemessene Verzögerung löschen. Einer der dort aufgeführten Gründe ist der Widerspruch der betroffenen Person nach Art. 21 Abs. 1 DSGVO gegen die Verarbeitung ihrer personenbezogenen Daten. Im Falle eines solchen Widerspruchs muss der Verantwortliche diese Daten löschen, sofern keine vorrangigen berechtigten Gründe für die weitere Verarbeitung vorliegen, Art. 17 Abs. 1 lit. c DSGVO.

Nach Art. 17 Abs. 2 DSGVO muss ein Verantwortlicher, der zu löschende personenbezogene Daten öffentlich gemacht hat, andere Verantwortliche, die diese Daten verarbeiten, darüber informieren, dass eine betroffene Person die Löschung aller Links zu oder aller Kopien oder Replikationen von diesen personenbezogenen Daten verlangt hat. Die Ausnahmen von den Löschpflichten in Art. 17 Abs. 3 DSGVO sind insgesamt enger gefasst als im bisherigen Recht.

Zweiter Abschnitt: Datenschutz und Datensicherheit im Auto nach der DSGVO

I. Materielle Voraussetzungen für die Verarbeitung von Standortdaten und anderen personenbezogenen Daten

Liegen personenbezogene Daten vor und hat keine Anonymisierung stattgefunden, bedarf es für eine zulässige Nutzung nach Art. 6 DSGVO grundsätzlich einer Ermächtigungsgrundlage.

Die Datenschutz-Grundverordnung legt in Art. 6 Abs. 1 DSGVO neben der Einwilligung (lit. a) und der Verarbeitung im Kontext eines Vertrages (lit. b) vier weitere Fälle der rechtmäßigen Datenverarbeitung fest:

- ➔ die Erfüllung einer rechtlichen Verpflichtung (lit. c),
- ➔ das lebenswichtige Interesse einer Person (lit. d),
- ➔ die Verarbeitung zur erforderlichen Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (lit. e) oder
- ➔ die Verarbeitung zur Wahrung der berechtigten Interessen eines Datenverarbeiters oder einer Drittpartei, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (lit. f).[19]

II. Erstellung von Profilen; Zweckbindung

Die Erstellung von Datenprofilen ist im Fahrzeugbereich in jüngster Zeit zur gängigen Praxis geworden. Nutzungs-, Bewegungs- und Kommunikationsprofile sind für viele kommerziell Beteiligte von erheblichem Interesse. Im Bereich der Fahrzeugtechnik sind elektronische Auswertungen (sog. Big-Data-Analysen) zwischenzeitlich sowohl in Echtzeit, als auch nachträglich für verschiedene Zwecke möglich. Spekulationen gehen bereits dahin, dass auf der Grundlage von individuellen Risikoprofilen präventive Maßnahmen gegen den Fahrer erlassen werden könnten.

[19] Vgl. Art. 6 Abs. 1 EU-DSGVO, abrufbar unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf (zuletzt aufgerufen am 29.08.2016); Albrecht, CR 2/2016, S. 92.

Der ADAC hat in einer aktuellen Studie die Datensammlung einiger Fahrzeuge untersucht.[20] Danach sammelten die Hersteller in den untersuchten Fahrzeugen eine große Zahl an Informationen, was für die Fahrer und Halter nicht transparent ist. Auch der Zweck der Datenverwendung entzieht sich offenbar den Betroffenen.

Beim Renault Zoe wird beispielsweise bei jeder Fahrt, spätestens jedoch alle 30 Minuten, ein Datenpaket an Renault gesendet, das mindestens VIN, div. Seriennummern, Datum, Uhrzeit, GPS-Position, Temperatur, Ladung und Zellspannung der Hochvolt-Antriebsbatterie enthält. Diese Informationen kann Renault darüber hinaus auch jederzeit anfordern. Beim Mercedes B-Klasse sendet das System etwa alle zwei Minuten die GPS-Position, den Kilometerstand, den Verbrauch und den Reifendruck ebenso wie die Zahl der Gurtstraffungen, z.B. wegen starken Bremsens, an den Hersteller. Bei den untersuchten BMW-Fahrzeugen konnten u.a. die 100 letzten Abstellpositionen des Fahrzeugs ausgelesen werden.

1. Zweckbindungsgrundsatz

Der datenschutzrechtliche Zweckbindungsgrundsatz besagt, dass personenbezogene Daten grundsätzlich nur zu den Zwecken verwendet werden dürfen, zu denen sie erhoben wurden. Nach diesem Grundsatz ist die Datenverwendung aufgrund eines Gesetzes oder einer Einwilligung nur zu einem klar und präzise bestimmten Zweck zulässig.[21] Im Rahmen des EU-Gesetzgebungsprozesses war besonders die Frage nach der Zulässigkeit einer Zweckänderung umstritten.

Die neuen Regelungen in der DSGVO werden künftig verschärfte Anforderungen an „Big Data Anwender“ stellen, weshalb diese bereits bei der Erhebung von Daten prüfen müssen, unter welchen Voraussetzungen eine Zweckänderung möglich ist.

Der im Datenschutzrecht verankerte Zweckbindungsgrundsatz ist mit Big-Data-Anwendungen wie dem vernetzten Fahrzeug vereinbar, wenn eine Einwilligung des Betroffenen zur Verwendung der Daten zu einem konkret benannten Zweck oder eine andere Rechtsgrundlage vorliegt. Problematisch gestalten sich insbesondere Einwilligungserklärungen, bei denen im Zeitpunkt der Einwilligung noch nicht bestimmbar ist, zu welchem Zweck die Daten erhoben werden. Durch die ständige Weiterentwicklung der Technik und staatliche Eingriffe droht eine Aushöhlung des Zweckbindungsgrundsatzes, so dass eine bereits erteilte Einwilligung unwirksam sein könnte. Selbst wenn der Hersteller oder ein sonstiger Dienstleister berechtigt auf Daten zugreifen kann, muss im Übrigen aufgrund des Grundsatzes der Datensparsamkeit

[20] ADAC Untersuchung an vier Fahrzeugen: „Welche Daten erzeugt ein modernes Auto?“, abrufbar unter https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx (zuletzt abgerufen am 03.11.2016).
[21] Art. 5 Abs. 1 lit. b i. V. m. Art. 6 Abs. 4 DSGVO.

durch eine Anonymisierung ein Personenbezug und damit eine Profilbildung weitgehend ausgeschlossen werden.

In diesem Zusammenhang ist ebenfalls der Verkauf eines Fahrzeugs relevant. Der Käufer hat grundsätzlich ein Interesse an der Information, wie das Fahrzeug genutzt und gefahren wurde. Problematisch ist hierbei jedoch, dass ein potentieller Käufer anhand der Daten Bewegungsprofile erstellen könnte. Um einerseits seinem Informationsbedürfnis ausreichend Rechnung zu tragen, andererseits eine Profilbildung unmöglich zu machen, bietet sich als Lösung an, dem Käufer lediglich aggregierte Daten (z.B. über die Kilometerleistung oder einen Airbag-Einsatz) als Information über den Zustand des Fahrzeuges zu überlassen.

Insgesamt wird es entscheidend auf die Entwicklung eines Privacy-by-Design-Konzepts ankommen, nach dem Daten im Hoheitsbereich des Betroffenen liegen und keine Speicherung bestimmter Daten erfolgt. Big-Data-Anwendungen sind dann auch mit dem Zweckbindungsgrundsatz in Einklang zu bringen, wenn kein Personenbezug (mehr) besteht. Darüber hinaus ist eine Änderung des Verarbeitungszwecks möglich, wenn der ursprüngliche Zweck mit dem neuen bzw. veränderten Zweck vereinbar ist oder wenn der Betroffene einwilligt (Art. 6.4. DSGVO). Außerdem gibt es weitreichende Ausnahmen vom strikten Zweckbindungsgebot für die wissenschaftliche Forschung oder statistische Zwecke, worunter Big-Data-Anwendungen im Einzelfall gefasst werden können. Jedoch müssen in diesen Fällen besondere Schutzmaßnahmen getroffen werden, wie die Pseudonymisierung der Daten (Artikel 5.1.b DSGVO i.V.m. Artikel 89.1 DSGVO). Werden die Daten zu statistischen Zwecken verarbeitet, muss es sich bei den Ergebnissen ferner um aggregierte Daten handeln. Außerdem dürfen diese Ergebnisse nicht für Entscheidungen über einzelnen Personen verwendet werden (Erwägungsgrund 162 der DSGVO).

2. Transparenz und Information für den Betroffenen

Die Transparenz der Fahrzeugdaten muss gewährleistet sein. Das ist Voraussetzung dafür, dass der Fahrer wie auch der Halter sein Recht auf informationelle Selbstbestimmung ausüben und wahren kann. Die DSGVO normiert in Art. 12 bis 15 Informations- und Auskunftspflichten des Verantwortlichen gegenüber dem Betroffenen. Die zentralen Informationspflichten, durch die die Herstellung von Transparenz bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten sichergestellt werden soll, finden sich in Art. 13 und 14 DSGVO. Hieraus folgt, dass der Kunde bereits in der Betriebsanleitung detailliert über die im Fahrzeug erhobenen und verarbeiteten Daten informiert werden muss. Andererseits muss aufgrund der Art. 12 bis 15 DSGVO außerhalb der gesetzlich vorgegebenen Datenverwendung (beispielsweise eCall, digitaler Tachograph) weiterhin eine Wahlfreiheit zwischen Diensten mit unterschiedlicher Datenintensität gewährleistet sein.

Dennoch sehen die Vorschriften keine explizite Regelung für eine situationsgerechte Bereitstellung der Informationen vor. Eine Transparenz über die erhobenen und verarbeiteten Daten während des Betriebs des Fahrzeugs ist daher in der DSGVO nicht ausdrücklich geregelt. Gerade diese Informationen sind aber bei vernetzten Fahrzeugen von immenser Bedeutung. Dem Fahrzeugnutzer muss während der Fahrt verständlich mitgeteilt werden, welche Daten zu welchem Zweck erhoben werden. Das gilt insbesondere dann, wenn beispielsweise ein Datenzugriff oder eine Zweckänderung stattfindet, da in letzterem Fall der betroffenen Person vor dieser Weiterverarbeitung Informationen über den geänderten Zweck und alle anderen maßgeblichen Informationen zur Verfügung gestellt werden muss (Art. 13.3 DSGVO).

3. Lösung durch Verbesserung der Fahrzeug-Infrastruktur (Privacy by Design und Privacy by Default, Risikoanalysen)

Empfehlenswert sind Verbesserungen der Fahrzeug-Infrastruktur für den Datenschutz. Durch eine effektive Umsetzung der Datenschutzprinzipien sowie Risikoanalysen, Standardisierungen und Zertifizierungen kann das Datenschutzniveau speziell bei der Kfz-Datenverarbeitung massiv verbessert werden.

Die Datensouveränität sollte über die Prinzipien „Privacy by Design“ und „Privacy by Default“ erzielt werden. Hierzu bedarf es allerdings weiterhin risikoadäquater Vorgaben für diese Prinzipien. Hierbei ist zunächst kritisch anzumerken, dass sich die nunmehr in der DSGVO verankerten Prinzipien allein an die für die Verarbeitung Verantwortlichen, nicht hingegen an den Hersteller der Datenverarbeitungstechnik richten. Insoweit sind die Prinzipien entsprechend ihrer Ausgestaltung in Art. 25 Abs. 1 und 2 DSGVO für das spezifische Anwendungsfeld des Smart Car kaum relevant. Einerseits richten sie sich bereits an den falschen Adressaten, nämlich nicht unmittelbar an den Hersteller. Darüber hinaus überlässt die DSGVO die Einschätzung allein dem für die Datenverarbeitung Verantwortlichen und enthält weitreichende Ausnahmetatbestände. Die Anforderungen an den Datenschutz sollten aber ausdrücklich für den Hersteller geregelt werden und wie bereits beim „eCall“ bei der Zulassung der Fahrzeuge geprüft werden.

Zur Gewährleistung von Transparenz sollten Hersteller die Grundsätze der „Privacy by design“ und „Privacy by default“ bereits in der Entwicklungsphase beachten und künftig verpflichtet werden, dem Halter eine Auflistung der im Fahrzeug erhobenen, verarbeiteten und genutzten Daten öffentlich zur Verfügung zu stellen. Neben dem Halter sollte die Auflistung auch einer neutralen Stelle zur Verfügung stehen, die die Einhaltung der Datenschutzbestimmungen überprüfen kann.[22] Darüber hinaus sollte jedes Fahrzeug hinsichtlich der Stärke und des

[22] Vorschlag des ADAC, zur Sache: Daten im Fahrzeug, abrufbar unter https://www.adac.de/_mmm/pdf/28684_263046.pdf (zuletzt abgerufen am 27.09.2016).

Umfang der Datensicherheits- und Datenschutzmaßnahmen durch eine standardisierte Grafik gekennzeichnet werden, um hierdurch den Nutzer auf leicht verständliche Weise zu informieren.

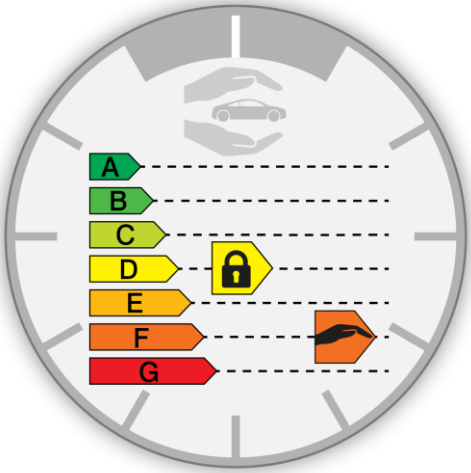


Abb. 2: Beispiel für eine standardisierte Grafik, Quelle: FSD – Zentrale Stelle nach StVG

Dieses System hat sich auf dem Markt bereits bei Elektrogeräten bewährt. Gleichwohl sind die Anforderungen, eine Grafik im Bereich des Datenschutzes und der Datensicherheit verständlich darzustellen, wesentlich höher.

Insbesondere bei Dienst- oder Car-Sharing Fahrzeugen kann zudem einer unkontrollierten Erhebung, Einsicht, Löschung und Weitergabe von Daten durch die Vornahme individueller Einstellungen nach dem Motorstart vorgebeugt werden. Die vom Fahrer einmal vorgenommenen Einstellungen können hierbei verschlüsselt gespeichert werden und bei der Anmeldung (z.B. mit einer PIN) aktiviert werden.

Abb. 3: Beispiel für eine individuelle Anmeldung, Quelle: FSD – Zentrale Stelle nach StVG

Darüber hinaus sollte der Fahrer in der Lage sein, bei Inbetriebnahme seines Fahrzeug die aufzuzeichnenden Daten individuell auszuwählen und sich über die einzelnen Daten, die bei

der aktivierten Aufzeichnung gespeichert werden, kurz und verständlich zu informieren. Der aktuelle Vernetzungsstatus ist im Cockpit durch standardisierte Symbole anzuzeigen und sollte vom Fahrer jederzeit aktiviert und deaktiviert werden können.

Abb. 4: Beispiel für Auswahl und Informationen des Vernetzungsstatus, Quelle: FSD – Zentrale Stelle nach StVG

III. Einzelne datenschutzrechtliche Fragen

1. Anforderungen an eine wirksame Betroffeneneinwilligung bzw. Widerspruch

Art. 4 Nr. 11 DSGVO definiert die Einwilligung als jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Die Erklärung muss qualifiziert erfolgen, was voraussetzt, dass sie Angaben über die verantwortliche Stelle, den erlaubten Zweck und über Art und Umfang der Daten enthalten muss.

Die DSGVO sieht darüber hinaus weitergehende Anforderungen an eine wirksame Einwilligung vor.

Insbesondere stellt Erwägungsgrund 32 der DSGVO nunmehr unmissverständlich klar, dass jede Einwilligung nur durch eine eindeutig bejahende Handlung in einer schriftlichen Erklärung oder durch eine sonstige aktive, eindeutig bestätigende Handlung, wie beispielsweise durch das Anklicken eines Buttons oder durch die Auswahl entsprechender Einstellungen erfolgen kann.

Nach dem Erwägungsgrund 43 der DSGVO gilt eine Einwilligung nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten keine gesonderte Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist.

Darüber hinaus kann nach Art. 7 Nr. 4 DSGVO eine Einwilligung in der Regel nicht frei erfolgen, wenn sie zur Bedingung für die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung gemacht wird, obwohl sie hierfür nicht erforderlich ist (sog. Kopplungsverbot).[23]

Ferner geht aus Art. 12 DSGVO hervor, dass eine Information über die Reichweite der Einwilligung präzise, transparent und verständlich ausgestaltet werden muss.

Hieran gemessen reicht eine pauschale datenschutzrechtliche Einwilligungserklärung beim Kauf auf keinen Fall aus.

Es ist zu überlegen, dem Nutzer situationsbezogene Informationen per visuellem oder akustischem Signal sowohl vorab als auch bei Erforderlichkeit während des Betriebs zukommen zu lassen, sog. „Layered Policy Design“. Durch die auf dem Display erscheinenden Hinweise soll der Nutzer zur Entscheidung befähigt werden, ob und insbesondere auch in welcher Detailfülle er weitergehende Erläuterungen wünscht.

Da ein Schutz nicht nur für Nutzer bestehen soll, die ihr System umkonfigurieren wollen, beruht eine weitere praktikable Sicherung des Erklärungswillens des Einwilligenden auf dem Prinzip des „Privacy by Default“.

Problematisch ist die Einholung einer Einwilligung hingegen bei anderen Verkehrsteilnehmern. Vor allem bei Passanten wird die Einholung faktisch nahezu unmöglich sein. In diesen Fällen muss eine Personenerkennung ausgeschlossen werden, indem die erfassten Personen anonymisiert werden. Hierzu können beispielsweise Kameras eingesetzt werden, deren Sensor nur Bewegungsinformationen des betroffenen Verkehrsteilnehmers erfasst (z.B. Objekt: Mensch/Tier, Größe, Bewegungsgeschwindigkeit und –richtung) und eine Speicherung der Aufnahme des Gesichts technisch unausführbar ist.

Insgesamt stellt die Umsetzung von wirksamen Einwilligungserklärungen im „Connected Car“ eine Herausforderung dar. Bei einer ernsthaften Umsetzung der Konzepte „Privacy by Design“ und „Privacy by Default“ haben die Automobilhersteller aber auch die Chance, das Vertrauen der Fahrzeugnutzer zu gewinnen und sich einen Wettbewerbsvorteil zu verschaffen. Es sind nämlich nach wie vor die Unternehmen, die für Datenvorfälle verantwortlich gemacht werden – egal, ob sie durch Kriminelle oder staatliche Stellen außerhalb ihrer Kompetenzen begangen

[23] *Albrecht, Jan Philipp*: Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung in CR 2/2016, S. 91.

wurden. Dies führt zu einem Verlust von Kundenvertrauen in die Unternehmen und die virtuelle vernetzte Welt, dem Automobilhersteller auch im eigenen Interesse entgegenwirken sollten.

In Art. 7 Abs. 3 DSGVO ist im Übrigen nun erstmals eine ausdrückliche Regelung zur Widerrufsmöglichkeit einer erteilten Einwilligung vorgesehen. Danach wird die Rechtmäßigkeit der aufgrund der Einwilligung erfolgten Datenverarbeitung bis zum Widerruf nicht berührt.

2. Löschungsfristen

Von wesentlicher Bedeutung für den Datenschutz im vernetzten Fahrzeug ist auch die Entwicklung differenzierter Speicher- und Löschkonzepte, die gleichzeitig für die Akzeptanz vernetzter Fahrzeuge relevant sind. Art. 17 DSGVO normiert das in der Öffentlichkeit bekannt gewordene „Recht auf Vergessen-Werden“, indem das Recht auf Löschung von Daten ausdrücklich festgeschrieben wird.[24] Wie schon im BDSG finden sich auch in der DSGVO keine starren Zeitangaben, innerhalb derer Daten gelöscht werden müssen. In Erwägungsgrund 39 ist aber davon die Rede, dass die Speicherfrist auf das unbedingt erforderliche Maß beschränkt sein soll. Daten dürfen nicht länger als nötig gespeichert werden.

Daher sind bereits bei der Entwicklung von Fahrzeugen und ihren IT-Systemen systematische Löschkonzepte zu erarbeiten. Hierbei ist zu prüfen, welche Daten wie lange und zu welchem Zweck bereitgehalten werden müssen.

Um einen datenschutzgerechten Umgang zu gewährleisten, sollten insbesondere bei einem Teil der Daten kurzzeitig definierte Löschungsereignisse vorgesehen sein, wie beispielsweise beim Öffnen der Fahrertür oder dem Abstellen des Motors.

Will der Fahrzeugnutzer selbst eine Datenlöschung beispielsweise im persönlichen Profil vornehmen, muss sichergestellt sein, dass diese Daten real gelöscht werden. Ausnahmen hiervon dürfen nur dann gelten, wenn diese Daten für einen zulässigen Zweck weiterhin gespeichert werden dürfen.

Ferner empfiehlt es sich, bei bestimmten Ereignissen, wie der Deinstallation einer mit dem Fahrzeug vernetzten Anwendung (App) oder der Kündigung des Nutzungsvertrages des Fahrzeugs eine turnusmäßige Löschung der Nutzerdaten einzurichten.[25]

[24] *Schumacher* in Smart World – Smart Law? Tagungsband Herbstakademie 2016, S. 309, 320.
[25] *Weichert, Thilo*: Datenschutz im Auto, in: 52. Deutscher Verkehrsgerichtstag, S. 285, 304.

Unabhängig davon sollte für spezifische Standort- und Nutzungsdaten, eine Löschung beim Verkauf des Fahrzeugs vorgesehen sein, um die Gefahr einer nachträglichen Profilbildung zu vermeiden.

Hierzu hat haben das Deutsche Institut für Normierung (DIN) bereits Projekte entwickelt. Des Weiteren wurde im September 2015 eine Leitlinie zum Löschkonzept vom zuständigem Arbeitskreis im DIN verabschiedet.[26] Diese Initiativen bauen größtenteils auch das Konzept der Datenlöschung im Mautsystem „Toll Collect“ für LKW auf.

3. Exkurs: Versicherungstarif „Pay as you drive“

Ein Beispiel für die „freiwillige“ Erfassung von personenbezogenen Fahrzeugdaten sind die Telematik-Tarife bei der Kfz-Versicherung.

Während in den USA bereits jedes siebte Fahrzeug telematisch versichert ist, befindet sich das Versicherungssystem in Deutschland erst in seinen Anfängen.

Die Daten des Fahrverhaltens werden dabei in der Weise erfasst, verarbeitet und ausgewertet, dass dem Versicherer abstrakte Scoring-Punkte übermittelt werden, aus denen sich die Kfz-Versicherungsprämie berechnet.

Es wird vermutet, dass mit der Einführung des eCalls und der damit verbundenen verpflichtenden Ausstattung der Fahrzeuge mit einer SIM-Karte derartige Versicherungstarife auch hier zum Standard werden.[27] In seiner aktuellen Ausgestaltung bestehen bei dem Versicherungstarif darüber hinaus massive Bedenken.

Die Daten werden mit Einwilligung des Versicherungsnehmers erlangt. Zugriff hierauf haben jedoch allein der Versicherer und sein Partnerunternehmen, das für die Durchführung des Telematik-Scores zuständig ist. Dem Versicherungsnehmer selbst werden die Daten nur auf einer App oder einem Web-Portal zur Überprüfung bereitgestellt.[28] Insoweit ist es zumindest zweifelhaft, ob der Versicherungsnehmer seine Daten aus der Telematik-Box löschen kann, um sie beispielsweise vor dem Zugriff der Strafverfolgungsbehörden zu schützen und den „Nemo-tenetur“-Grundsatz wahrzunehmen.

---

[26] DIN, „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“, Oktober 2015.
[27] *Kinast/ Kühnl*, NJW 2014, 3057, 3058.
[28] *Mielchen*, „Verrat durch den eigenen PKW – wie kann man sich schützen?“, in Tagungsband des 52. Deutschen Verkehrsgerichtstags 2014, 241 ff., 248.

Zu Problemen können die Tarife insbesondere dann führen, wenn nicht der Versicherungsnehmer selbst, sondern eine andere Person das Fahrzeug führt.

Im Rahmen dieser und weiterer Geschäftsmodelle bietet sich eine Regelung der rechtlichen Rahmenbedingungen durch entsprechende Vertragsgestaltung an.

Hier sollte die Wirtschaft gemeinsam mit der Rechtswissenschaft entsprechende Musterverträge mit Regelungen zu Nutzungs-, Verwertungs- und Verfügungsrechten, sowie der Inhaberschaft an Daten entwickeln.

4. Videokontrolle im Fahrzeug

a) Rechtsprechung deutscher Gerichte

Die bisherige Rechtsprechung zur beweisrechtlichen Verwertbarkeit der sog. Dashcams zeigt ein uneinheitliches Bild. Die Gerichte entscheiden jeweils aufgrund einer Abwägung der beteiligten Interessen im Einzelfall. In die Abwägung fließt in der Regel auf der Seite des Betroffenen das Datenschutzrecht, namentlich § 6b BDSG, ein. Dem stehen auf der Seite des Geschädigten das Interesse an einer Aufklärung des Sachverhalts und das Interesse an einem Ersatz des entstandenen Schadens sowie die ansonsten bestehende Beweislosigkeit des Geschädigten gegenüber. Es müssen allerdings zugunsten des Verwenders der Kamera Gesichtspunkte hinzutreten, die das Interesse an der Beweiserhebung trotz Rechtsverletzung als schutzwürdig erscheinen lassen. Im strafrechtlichen Bereich sei dies zumeist unter Annahme einer Notwehrsituation oder notwehrähnlichen Lage anzunehmen. Auch die Erforderlichkeit der „Überwachung“ spielt eine entscheidende Rolle. In dem Standardfall der Dashcam wird davon ausgegangen, dass durch die heimlichen Aufnahmen eine permanente Aufzeichnung einer Vielzahl von Personen in ihrem allgemeinen Persönlichkeitsrecht betroffen wird. Es erfolgt auch keine „anlassbezogene“ Aufzeichnung sowie keine nur örtlich beschränkte, wie bei einer fest installierten Anlage an einem bestimmten Ort. Eine ähnliche Abwägung wird auch im Rahmen des § 6 b Abs. 1 Nr. 3 BDSG und § 22 S. 1, 23 Abs. 1 Nr. 2 KUG vorgenommen.[29]

Das Amtsgericht Nürnberg urteilte in einem Fall, dass eine private Videoaufzeichnung als Beweismittel verwertet werden können. Es sei im Rahmen einer Interessenabwägung zu klären, ob schutzwürdige Interessen des Betroffenen überwiegen. Das Aufklärungsinteresse des Ge-

[29] Vgl. LG Traunstein, Urteil vom 01.07.2016, 3 O 1200/15.

schädigten könne bei einem Unfall mit Personenschaden aber auch bei einem reinen Sachschaden grundsätzlich das Persönlichkeitsrecht gefilmter Personen überwiegen.[30] Das Oberlandesgericht Stuttgart hat in einer jüngsten Entscheidung in einem Bußgeldverfahren ebenfalls eine Verwertbarkeit derartiger Aufnahmen bejaht. Zur Begründung hat es ausgeführt, dass aus einem eventuellen datenschutzrechtlichen Verbot kein Beweisverwertungsverbot folge. Aber auch hier stellte das Oberlandesgericht fest, dass für die datenschutzrechtlichen Grundlagen von Dashcams § 6b Abs. 1 Nr. 3 BDSG heranzuziehen ist.[31] Anders sah es das LG Memmingen, das ein Verstoß gegen das Recht auf informationelle Selbstbestimmung annimmt, wenn der Einsatz der Dashcam nicht nach § 6b BDSG gerechtfertigt ist. Die bloß theoretische Möglichkeit der Notwendigkeit einer Beweisführung aufgrund der generellen Gefährlichkeit des Straßenverkehrs oder der Möglichkeit von Vandalismus genüge nicht für ein überwiegendes Interesse, zu diesem Zwecke zu beliebigen Zeitpunkten den Zugang zu einem privaten Anwesen zu überwachen. Ein rechtswidriger Überwachungsdruck gehe auch von einer aufnahmebereiten Kamera aus, weshalb deren Bereithalten zum Zwecke eines effektiven Rechtsschutzes zu untersagen sei.[32]

b) Rechtsprechung des EuGH

Der europäische Gerichtshof hatte in einem Fall die private Videoüberwachung im öffentlichen Raum zu beurteilen.[33] Hier erfasste eine in einem Eingangsbereich eines Privathauses angebrachte Kamera auch Teile des Straßenraums. Der EGMR zog als Prüfungsmaßstab für die Zulässigkeit der Kamera insbesondere Art. 7 lit. f der EG-Datenschutz-RL heran. Danach falle diese Art der Aufzeichnung nicht mehr unter eine ausschließlich private Tätigkeit.

c) Regelung in der DSGVO

Mit Inkrafttreten der DSGVO wird sich die datenschutzrechtliche Beurteilung von Dashcams ändern, da sie keine dem § 6b BDSG entsprechende Norm zur Videoüberwachung enthält.

Es ist zu erwarten, dass künftig Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage für den Einsatz von Dashcams herangezogen wird. Diese Norm ähnelt sprachlich dem bisherigen Art. 7 lit. f EG-Datenschutz-RL, den der Europäische Gerichtshof als Prüfungsmaßstab herangezogen hat.

---

[30] AG Nürnberg, Urteil vom 08.05.2015, Az. 18 C 8938/14, DAR 2015, 472; ebenso LG Traunstein a.a.O.; LG Nürnberg-Fürth, Urteil vom 08.02.2016, 2 O 4549/15.
[31] OLG Stuttgart, Beschluss vom 04.05.2016, 4 Ss 543/15, BeckRS 2016, 09359.
[32] LG Memmingen, Urteil vom 14.01.2016, 22 O 1983/13.
[33] EuGH, NJW 2015,463.

d) Lösungsansätze

Im Rahmen des automatisierten Fahrens werden künftig voraussichtlich vermehrt Systeme wie jetzt schon bei der Einparkhilfe eingesetzt werden, die die Umwelt des Fahrzeugs scannen und filmen. Aktuell wird auf EU-Ebene die Einführung eines Unfalldatenspeichers (UDS) diskutiert. In einem solchen werden die Daten zumindest vorübergehend gespeichert, sodass die rechtliche Situation vergleichbar mit dem Einsatz von Dashcams ist. Die datenschutzrechtlichen Probleme des Betriebs von Dashcams haben einige Hersteller bereits zum Anlass genommen, die Funktionsweise der Kameras zu optimieren. Es wurden beispielsweise Kameras entwickelt, die nur die letzten 15 Sekunden aufzeichnen und zurückliegende Bildsequenzen automatisch löschen. Nur im Falle einer starken Erschütterung, durch die ein Unfall indiziert wird, wird die automatische Löschfunktion ausgeschaltet.

In diesem Zusammenhang dürfte eine Einschränkung des Datenschutzrisikos insbesondere bei Unfalldatenspeichern in Betracht kommen. In den USA werden beispielsweise vom Hersteller UDS mit einem sogenannten „Crash Data Retrieval Kit“ eingebaut. Die Daten werden langfristig nur bei der Auslösung des Airbags gespeichert. Darüber hinaus kann die verschlüsselte Speicherung im System rechtlich und technisch nur bei einem Unfall aufgehoben werden.[34]

In Anbetracht der erheblichen rechtlichen Unsicherheiten diesbezüglich wurde vom Deutschen Verkehrsgerichtstag empfohlen, den Umfang der Verwendung von Dashcams und Verwertung entsprechender Aufnahmen gesetzlich zu regeln.[35]

5. Exkurs: Beschäftigtendatenschutz

Datenschutzrechtliche Anknüpfungspunkte ergeben sich aufgrund der Verarbeitung von Fahrzeugdaten zudem beim Beschäftigtendatenschutz. Automatisierte Fahrzeuge können auch den Beschäftigten und dessen privates Umfeld, mit dem das Fahrzeug naturgemäß in Berührung kommt, und den Arbeitgeber in Verbindung bringen, sofern es sich zumindest teilweise um eine dienstliche Nutzung des Fahrzeugs handelt.

Die DSGVO sieht hierzu in Art. 82 eine Rechtssetzungsbefugnis der Mitgliedsstaaten vor. Zentrale Norm für die Zulässigkeit der Datenerhebung bei Beschäftigten stellt daher weiterhin § 32 BDSG dar. Danach dürfen personenbezogene Daten zum Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies (…) für die Zwecke des

[34] *Haustein, B.*, Datenschutzrechtskonforme Ausgestaltung von Dashcams, S. 43 ff.
[35] Empfehlung des 54. Deutschen Verkehrsgerichtstages, Arbeitskreis VI: Dashcam, abrufbar unter www.gdv.de/wp-content/uploads/2016/01/Verkehrsgerichtstag_2016_Empfehlungen_Arbeitskreis_6.pdf (zuletzt abgerufen am 13.10.2016).

Beschäftigungsverhältnisses erforderlich ist. Für nicht unmittelbar auf das Beschäftigungsverhältnis bezogene Zwecke bleibt der Anwendungsbereich des Art. 6 DSGVO eröffnet.

Bei der Nutzung vernetzter Fahrzeuge im Rahmen von Beschäftigungsverhältnissen kommt ferner dem § 87 Abs. 1 Nr. 6 BetrVG eine besondere Bedeutung zu. Danach steht dem Betriebsrat bei Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, ein Mitbestimmungsrecht zu. Erforderlich ist hierfür lediglich die Geeignetheit der Einrichtung zur Überwachung der Arbeitnehmer. Hierbei ist zu beachten, dass grundsätzlich eine Vielzahl im Fahrzeug anfallenden Daten zur Verhaltens- und Leistungskontrolle der Arbeitnehmer geeignet sein können.[36]

IV. Datensicherheit: Schutz vor Manipulation, Datenverlust

Die Komplexität der im vernetzten und automatisierten Fahrzeug erhobenen Daten erfordert die Gewährleistung einer umfassenden IT-Sicherheit. Mit den bereits Ende 2014 vom VDA formulierten Datenschutz-Prinzipien wurde die Automobilwirtschaft zu einem verantwortungsbewussten Umgang mit im vernetzten Fahrzeug erhobenen Daten und einer Verankerung des *privacy by design* im Wege der Selbstregulierung angehalten.[37]

Die europäischen Herstellerverbände haben sich nach dem Vorbild der amerikanischen Herstellerverbände selbstregulierende Prinzipien des Datenschutzes auferlegt. Darunter fallen neben der Transparenz, Rechtmäßigkeit der Verarbeitung, Accountability, die Datensicherheit sowie die Verhältnismäßigkeit. Anders als in den USA werden etwaige Verstöße bei Zuwiderhandlungen gegen die Prinzipien jedoch nicht sanktioniert werden können, da eine Aufsichtsbehörde zur Überwachung und Vollstreckung nicht vorgesehen ist.

In diesem Zusammenhang regelte der bislang geltende § 9 BDSG nebst Anlage, welche technisch-organisatorischen Maßnahmen die verantwortliche Stelle zur Gewährleistung der Datensicherheit treffen musste. Die Regelung wird künftig durch Art. 32 DSGVO ersetzt. Im Interesse der Datensicherheit wurden technisch-organisatorische Anforderungen gesetzlich nach Maßnahmen benannt. In Anbetracht der rasanten Weiterentwicklung der Technik, stellen die künftigen Regelungen nunmehr auf Schutzziele ab. Ausdrücklich als Schutzziele benannt werden die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit.

---

[36] *Jaspers/Franck,* RDV 2015, 69, 72.

[37] Datenschutzprinzipien für vernetzte Fahrzeuge vom 03.11.2014 mit einer Landkarte der Daten-Kategorien beim vernetzten Fahrzeug, https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.pdf; dazu auch Hornung, DuD 2015, S. 359, 366.

Die Umsetzung der Schutzziele stellt an die Gestaltung der Kfz-IT hohe Anforderungen. Übernimmt beispielsweise ein Hacker die Souveränität über die Kfz-IT, ist nicht nur die Integrität der Daten, sondern auch die körperliche Integrität der Insassen und weiterer Verkehrsteilnehmer gefährdet. Das gilt ebenfalls, wenn Behörden der Zugriff auf die Kfz-IT gewährt wird und sie gestohlene Fahrzeuge während des Betriebs stoppen können. Die Integrität von Unfalldatenspeichern muss zudem gewährleistet sein, um Verkehrsunfälle zuverlässig rekonstruieren zu können. Diese Beispiele zeigen, dass die technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit gerade hinsichtlich des Straßenverkehrs eine geradezu lebenswichtige Bedeutung haben. Ansonsten droht nicht nur der Autofahrer, Manipulationen ausgeliefert zu sein, sondern Fahrzeuginsassen und andere Verkehrsteilnehmer können an Leib und Leben gefährdet werden. Der Nachweis der Einhaltung der technisch-organisatorischen Maßnahmen kann ausweislich Art. 32 Nr. 3 DSGVO durch die Einhaltung von genehmigten Verhaltensregeln oder Zertifizierungsverfahren erfolgen.

Verstöße werden nunmehr nach Art. 83 Abs. 4 lit. a DSGVO mit Bußgeldern von bis zu 2 % des Vorjahresumsatzes geahndet.

Mit dem am 25.07.2015 in Kraft getretenen IT-Sicherheitsgesetz[38] müssen Betreiber kritischer Infrastrukturen vorgegebene IT-Sicherheitsstandards einhalten und Vorfälle dem Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. In § 5 Abs. 4 der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (*BSI-Kritisverordnung - BSI-KritisV*)[39] wird der Anwendungsbereich für den Sektor Informationstechnik und Telekommunikation bereits definiert. Ein weiterer wichtiger Sektor für den Bereich des automatisierten Fahrens, Transport und Verkehr, soll bis Ende 2016 durch Änderungsverordnung ebenfalls geregelt werden.[40]

Es stellt sich insoweit die Frage, ob mit dem IT-Sicherheitsgesetz und der BSI-KritisVO eine rechtliche und praxistaugliche Rechtsgrundlage für das automatisierte und vernetzte Fahren geschaffen wurde. Nach der Gesetzesbegründung besteht der Gesetzeszweck in der Verbesserung des Schutzes der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können.[41]

---

[38] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) v. 17.07.2015, BGBl. I, S. 1324.
[39] BSI-Kritisverordnung vom 22.04.2016, BGBl. I, S. 958.
[40] Vgl. Kurzmeldung des Bundesministerium des Inneren vom 07.03.2016, abrufbar unter http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2016/03/kritis-vo-verbaendeanhoerung.html (zuletzt abgerufen am 13.09.2016).
[41] Vgl. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), BT-Drs. 18/4096, S. 1.

Nach § 1 Abs. 1 KritisVO fallen unter den Anlagenbegriff sowohl Betriebsstätten und ortsfeste Einrichtungen als auch Maschinen, Geräte und ortsveränderliche Einrichtungen, die zur Erbringung einer kritischen Dienstleistung notwendig sind. Nach dieser Definition dürfte grundsätzlich auch das einzelne vernetzte Fahrzeug eine Anlage im Sinne der Verordnung darstellen, jedenfalls aber die Vielzahl geschäftsmäßig angebotener Telemedien und Steuerungsdienste des automatisierten Fahrens.

Zur Bestimmung des Stands der Technik können einschlägige internationale, europäische und nationale Standards herangezogen werden, sofern sie in der Praxis erfolgreich erprobt wurden.

Vom Bundesverband IT-Sicherheit e.V. wurde hierzu eine Handreichung herausgegeben.[42]

Auf den Bereich des automatisierten Fahrens übertragen, bietet sich grundsätzlich eine Regelung der Anforderungen an den Stand der Technik in den internationalen Abkommen an, worauf im folgenden Abschnitt konkreter eingegangen wird.

[42] TeleTrust – Bundesverband IT-Sicherheit e.V., Handreichung zum Stand der Technik im Sinne des IT-Sicherheitsgesetztes (ITSiG), Stand 2016, abrufbar unter https://www.teletrust.de/arbeitsgruppen/recht/stand-der-technik/ (zuletzt abgerufen am 10.10.2016).

Dritter Abschnitt: Bestehende Rahmenbedingungen und Gesetzgebungsbedarf im Verkehrs- und Zulassungsrecht

Erstes Kapitel: Nationales Verkehrsrecht

I. Bestehende Rahmenbedingungen im Straßenverkehrsrecht und Zulassungsrecht (StVZO/ FZV)

Für die Umsetzung des automatisierten und vernetzten Fahrens stellen sich zunächst Fragen aus dem Straßenverkehrsrecht. Rechtsgrundlage ist vornehmlich das Straßenverkehrsgesetz (StVG)[43], das unter anderem die Zulassung von Kraftfahrzeugen und Personen zum öffentlichen Straßenverkehr und die Haftung des Halters und Fahrers für Rechtsgutsverletzungen im Straßenverkehr regelt.

Auf Grundlage des § 6 StVG, nach der das Bundesministerium für Verkehr und digitale Infrastruktur ermächtigt ist, Rechtsverordnungen mit Zustimmung des Bundesrates zu erlassen, wurde unter anderem die Straßenverkehrsordnung (StVO)[44], die Straßenverkehrszulassungsordnung (StVZO)[45] und die Fahrzeugzulassungsverordnung (FZV)[46] erlassen.

Hoch automatisierte Fahrzeuge dürfen aufgrund der bestehenden gesetzlichen und rechtlichen Rahmenbedingungen nur als Testfahrzeuge zugelassen werden, §§ 70 StVZO, 46 StVO.

1. Vereinbarkeit automatisierter Fahrzeuge mit der StVO

Unter Zugrundelegung der Definition eines Fahrzeugführers muss der Fahrer eines teilautomatisierten Fahrzeugs dieses ständig überwachen und sich für eine ggf. erforderlich werdende Übernahme oder Übersteuerung bereithalten.

In diesem Zusammenhang ist zunächst zu hinterfragen, ob hochautomatisierte Fahrerassistenzsysteme mit der geltenden StVO (oder StVZO) vereinbar sein können.

---

[43] Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Artikel 15 des Gesetzes vom 24. Mai 2016 (BGBl. I S. 1217).
[44] Straßenverkehrsordnung vom 6. März 2013 (BGBl. I S. 367), zuletzt geändert durch Artikel 2 der Verordnung vom 17. Juni 2016 (BGBl. I S. 1463).
[45] Straßenverkehrs-Zulassungs-Ordnung vom 26. April 2012 (BGBl. I S. 679), zuletzt geändert durch Artikel 1 der Verordnung vom 17. Juni 2016 (BGBl. I S. 1463).
[46] Verordnung über die Zulassung von Fahrzeugen zum Straßenverkehr vom 3. Februar 2011 (BGBl. I S. 139), zuletzt geändert durch Artikel 16 der Verordnung vom 2. Juni 2016 (BGBl. I S. 1257).

Dies ist aus den nachfolgenden Gründen zu verneinen.

Fahrzeugführer ist, wer eigenständig unter Allein- oder Mitverantwortung ein Fahrzeug in Bewegung setzt, um es unter Handhabung essentieller technischer Vorrichtungen während der Fahrbewegung ganz oder wenigstens teilweise durch den Verkehrsraum zu leiten.

Der Fahrzeugführer muss nach dem Leitbild der StVO ein menschliches Wesen sein.[47]

Die Wortlautformulierungen der StVO richten sich teilweise direkt an den Fahrzeugführer. Dieser hat beispielsweise nach § 3 Abs.1. S. 1 StVO die Pflicht zur Fahrzeugbeherrschung in Bezug auf die Geschwindigkeit.

Unter Zugrundelegung dieser Definition muss der Fahrer eines automatisierten Fahrzeugs dieses ständig überwachen und sich für eine ggf. erforderlich werdende Übernahme oder Übersteuerung bereithalten.

Zwar richten sich nicht alle Normen der StVO ihrem Wortlaut nach an den Fahrzeugführer als Menschen. Aus der Begründung des Straßenverkehrsgesetzes wird jedoch geschlussfolgert, dass die Regeln der StVO als Gesamtes den Verkehrsteilnehmer ansprechen. Hierin heißt es: „[…] Erst wenn man dem Verkehrsteilnehmer im Einzelnen sagt, wie er sich in solchen Verkehrslagen und bei solchen Fahrmanövern zu verhalten hat und worauf er dabei zu achten hat, entbindet man ihn von gefährlichen „Problemfahren"[…]".[48]

Um der Pflicht der Fahrzeugbeherrschung nachzukommen, muss der Fahrzeugführer das Verkehrsgeschehen ständig überwachen. Hochautomatisierte Fahrzeuge, bei denen die Fahraufgaben zeitweise auf das System übertragen werden und der Fahrer in dieser Zeit von der ständigen Überwachungspflicht befreit ist, sind demnach nicht mit den geltenden Regelungen der StVO zu vereinbaren.

Daraus folgt, dass für hochautomatisiertes, vollautomatisiertes oder gar fahrerloses Fahren eine Änderung des StVG und der StVO erforderlich ist. Dabei müssen die Fahrerpflichten konkretisiert und eine Abwendung des Fahrers von der Fahrzeugführung, z.B. durch die Nutzung bordeigener Infotainmentsysteme, erlaubt werden. Außerdem muss klargestellt werden, wann welche Fahraufgaben durch Systeme übernommen werden dürfen und wie die Verantwortlichkeit zwischen dem Menschen als Fahrzeugführer und dem steuernden System verteilt

[47] *Lennart S. Lutz, M. Sc. Tito Tang, Markus Lienkamp*: Analyse der rechtlichen Situation von teleoperierten (und autonomen) Fahrzeugen
[48] Frauenhofer-Institut für Arbeitswirtschaft und Organisation IAO, Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen – Dienstleistungsprojekt 15/14, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie.

wird. Zudem muss das Zulassungsrecht erlauben, z.B. automatische Lenksysteme oberhalb der Geschwindigkeit von 10 km/h einzusetzen.

2. Änderungen in der StVO

Durch eine Klarstellung in der StVO, dass dem Fahrzeugführer eine voll- und hochautomatisierte Fahrfunktion gleichgestellt wird, kann die erörterte Problematik der Auslegung des Fahrzeugführers beseitigt werden.

Hierfür würde sich die folgende Ergänzung des § 3 StVO anbieten:

§ 3 StVO

(1) Wer ein Fahrzeug führt – das kann auch eine hochautomatisierte Fahrfunktion sein –, darf nur so schnell fahren, dass das Fahrzeug ständig beherrscht wird. Die Geschwindigkeit ist insbesondere den Straßen-, Verkehrs-, Sicht- und Wetterverhältnissen sowie den persönlichen Fähigkeiten und den Eigenschaften von Fahrzeug und Ladung anzupassen. Beträgt die Sichtweite durch Nebel, Schneefall oder Regen weniger als 50 m, darf nicht schneller als 50 km/h gefahren werden, wenn nicht eine geringere Geschwindigkeit geboten ist. Es darf nur so schnell gefahren werden, dass innerhalb der übersehbaren Strecke gehalten werden kann. Auf Fahrbahnen, die so schmal sind, dass dort entgegenkommende Fahrzeuge gefährdet werden könnten, muss jedoch so langsam gefahren werden, dass mindestens innerhalb der Hälfte der übersehbaren Strecke gehalten werden kann.

(2) Ohne triftigen Grund dürfen Kraftfahrzeuge nicht so langsam fahren, dass sie den Verkehrsfluss behindern.

(2a) Wer ein Fahrzeug führt, muss sich gegenüber Kindern, hilfsbedürftigen und älteren Menschen, insbesondere durch Verminderung der Fahrgeschwindigkeit und durch Bremsbereitschaft, so verhalten, dass eine Gefährdung dieser Verkehrsteilnehmer ausgeschlossen ist.

(3) Die zulässige Höchstgeschwindigkeit beträgt auch unter günstigsten Umständen…

Die entsprechenden Pflichten der StVO, die allgemein in § 60 beschrieben werden, wären durch eine Änderung ebenso auf hochautomatisierte Fahrzeuge anwendbar und könnten bei einer Verletzung entsprechend sanktioniert werden.

§ 60 StVO Zustand und Beleuchtung der Fahrzeuge

(1) Ein Fahrzeug darf auf Straßen nur verwendet werden, wenn es so gebaut und ausgerüstet ist, daß durch seinen sachgemäßen Betrieb Personen nicht gefährdet oder durch Geruch, Geräusch, Staub, Schmutz u. dgl. nicht über das gewöhnliche Maß hinaus belästigt oder Sachen, insbesondere die Fahrbahn, nicht beschädigt werden. *Dies gilt auch für ihren Betrieb mit Assistenzfunktionen und automatisierten sowie hochautomatisierten Fahrfunktionen.*

Durch den Verweis auf europarechtliche Verordnungen ist das nationale Straßenverkehrszulassungsrecht stark von der Ausgestaltung des internationalen Rechtsrahmens abhängig, weshalb bei einer Änderung der nationalen Vorschriften immer auch auf eine internationale Harmonisierung zu achten ist, worauf im Folgenenden eingegangen wird.

II. Konkretisierungen im Zulassungsrecht

Für die Gewährleistung eines effektiven Daten- und Verbraucherschutzes muss die Einhaltung der festgelegten Mindeststandards von Datenschutz und Datensicherheit bereits Voraussetzung für die Verkehrstauglichkeit und damit die Zulassung von Fahrzeugen sein. Hierzu sind die technischen, rechtlichen und organisatorischen Maßnahmen in die nationalen, europäischen und internationalen Zulassungsvorschriften aufzunehmen.

Mit Blick auf die DSGVO, die eine Vollharmonisierung des Datenschutzrechts vorsieht, stellt sich zudem die Frage, ob der deutsche Gesetzgeber eine eigene Gesetzgebungskompetenz zur Regelung datenschutzrechtlicher Fragen hat und ob der Themenkomplex unter die bestehende DSGVO zu fassen ist. Die Gesetzgebungskompetenz des nationalen Gesetzgebers ist im Ergebnis zu bejahen, denn die unmittelbare Geltung der DSGVO steht einer Normierung der Einhaltung von datensicherheits- und datenschutzrechtlichen Vorschriften für die Zulassung von Kraftfahrzeugen in den nationalen Zulassungsvorschriften nicht entgegen. Durch die gesetzgeberischen Maßnahmen im Zulassungsrecht wird lediglich die Einhaltung der DSGVO (u.a. die Einhaltung der Grundsätze des „Privacy by Design“ und „Privacy by Default“) zur Voraussetzung für die Zulassung eines Fahrzeugs für den Straßenverkehr gemacht. Damit werden u.E. erst die europarechtlichen Vorschriften der DSGVO im Kfz-Zulassungsrecht umgesetzt. Das von der DSGVO voll harmonisierte Datenschutzrecht wird hierbei inhaltlich nicht berührt.

1. StVG

Datenschutz und Datensicherheit sind für den Straßenverkehr von zunehmender Relevanz, sodass eine Ermächtigungsgrundlage für das Verkehrsministerium geschaffen werden muss, um entsprechende Maßnahmen zu erlassen. Hierzu könnte in der Ermächtigungsnorm des § 6 Abs. 1 Nr. 2 StVG ergänzt werden, dass in der StVZO bei der Zulassung neben der Gewährleistung der Verkehrssicherheit auch auf die Gewährleistung der Datensicherheit und des Datenschutzes zu beachten sind. Das Gleiche gilt für die Verordnungsermächtigung über die regelmäßigen Hauptuntersuchungen der Fahrzeuge, die ebenso jedenfalls die Datensicherheit zum Gegenstand haben müssen:

§ 6 StVG Abs. 1 Nr. 2

a) Voraussetzungen für die Zulassung von Kraftfahrzeugen und deren Anhänger, vor allem über Bau, Beschaffenheit, Abnahme, Ausrüstung und Betrieb, Begutachtung und Prüfung, Betriebserlaubnis und Genehmigung sowie Kennzeichnung der Fahrzeuge und Fahrzeugteile, um deren Verkehrssicherheit *und Datensicherheit* zu gewährleisten und
um die Insassen und andere Verkehrsteilnehmer *vor dem Missbrauch von Daten, die beim Verkehr des Fahrzeugs anfallen, zu schützen und* bei einem Verkehrsunfall vor Verletzungen zu schützen oder deren Ausmaß oder Folgen zu mildern [...]

l) Art, Umfang, Inhalt, Ort und Zeitabstände der regelmäßigen Untersuchungen und Prüfungen, um die Verkehrssicherheit *und die Datensicherheit* der Fahrzeuge und
den Schutz der Verkehrsteilnehmer zu gewährleisten sowie Anforderungen an Untersuchungsstellen und Fachpersonal zur Durchführung von Untersuchungen und Prüfungen, einschließlich der Anforderungen an *die Zentrale Stelle*, zur Überprüfung der Praxistauglichkeit von Prüfvorgaben oder deren Erarbeitung, sowie Abnahmen von Fahrzeugen und Fahrzeugteilen einschließlich der hierfür notwendigen Räume und Geräte, Schulungen, Schulungsstätten und –institutionen, [...]

2. StVZO

Darüber hinaus sind die Datensicherheit und der Datenschutz in der Straßenverkehrszulassungsverordnung (§ 30) vorzuschreiben.

§30 Beschaffenheit der Fahrzeuge

(1) Fahrzeuge müssen so gebaut und ausgerüstet sein,

1. dass ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar gefährdet, behindert oder belästigt; *dies gilt auch für ihren Betrieb mit Assistenzfunktionen und automatisierten sowie hochautomatisierten Fahrfunktionen.*
2. dass die Insassen *und andere Verkehrsteilnehmer* insbesondere bei Unfällen vor Verletzungen möglichst geschützt sind und das Ausmaß und die Folgen von Verletzungen möglichst gering bleiben.

(2) Fahrzeuge müssen in straßen- und umweltschonender *sowie datensicherer und datengeschützter* Weise gebaut sein und in dieser erhalten werden.

(3) Für die Verkehrs- oder Betriebssicherheit wichtige Bauteile und Komponenten müssen einfach zu überprüfen und leicht auswechselbar sein;
für die für die Sicherheit wichtigen elektronischen Bauteile, Komponenten und Funktionen ist zu gewährleisten, dass

1. *deren Störungen dem Fahrer über Warneinrichtungen angezeigt und*
2. *deren Überprüfung über die elektronische Fahrzeugschnittstelle unterstützt werden.*

Zweites Kapitel: Europäisches Verkehrsrecht

I. Bestehende völkerrechtliche Verträge über den Straßenverkehr

1. Wiener Übereinkommen über den Straßenverkehr

Die meisten Verkehrsregeln basieren derzeit noch auf der Wiener Straßenverkehrskonvention von 1968. Bei dem Abkommen handelt es sich um einen völkerrechtlichen Vertrag, der die Vertragspartner verpflichtet, einheitliche Verkehrs- und Zulassungsregeln zu erlassen. Die Zulassung zum internationalen Verkehr erhält ein Fahrzeug nur, wenn die dortigen Bestimmungen eingehalten sind, Art. 3 Abs. 3 WÜ.

Ein Fahrzeug im Sinne des Wiener Übereinkommens muss nach Art. 8 Abs. 1 WÜ einen Fahrer haben, welcher gemäß Art. 1 lit. (v) WÜ eine Person sein muss. Ferner wird der Fahrzeugführer mit der Pflicht belegt, sein Fahrzeug ständig zu beherrschen, Art. 8 Abs. 5, 13 Abs. 1 WÜ.

Darüber hinaus stellen zahlreiche weitere Vorschriften des WÜ Anforderungen an den Fahrzeugführer; so muss dieser etwa gem. Art. 8 Abs. 6 WÜ Nebentätigkeiten minimieren bzw. vermeiden und nach Art. 7 Abs. 3 WU gegenüber den schwächsten Verkehrsteilnehmern erhöhte Vorsicht walten lassen.

Danach waren alle Fahrzeugsysteme, die Einfluss auf das Führen eines Fahrzeugs nehmen konnten, unzulässig. Die aufgrund des technischen Fortschritts im Jahr 2014 eingeleitete Änderung des Übereinkommens ist mit Ablauf der in Art. 49 Abs. 2 lit. a. S. 3 WÜ festgelegten 18monatigen Wartefrist am 23.03.2016 in Kraft getreten. Inhaltlich wurde Art. 8 WÜ um einen neuen Abs. „5bis“ erweitert. Danach gelten Fahrzeugsysteme als mit Art. 8 Abs. 5 und Art. 13 WÜ vereinbar, wenn sie entweder die Anforderungen der ECE-Regelungen erfüllen (Satz 1) oder durch den Fahrer übersteuerbar und abschaltbar sind (Satz 2). Die nach dem oben dargelegten Vorgaben in Art. 8 Abs. 5 und Art. 13 Abs. 1 S. 1 WÜ stehen einer Zulassung automatisierter Fahrzeugen bei Erfüllung der Voraussetzungen des neuen Art. 8 Abs. 5bis WÜ nicht mehr entgegen.

Problematisch ist jedoch, dass nach dem oben Gesagten weitere Vorschriften des Wiener Übereinkommens Anforderungen an den Fahrzeugführer stellen. Wird der Fahrer jedoch auch nach der Änderung des WÜ weiterhin durch die genannten Vorschriften verpflichtet, sein Fahrzeug entsprechend den Vorgaben zu beherrschen, dürfte eine Nutzung eines hoch- oder vollautomatisierten Fahrzeugs wenig reizvoll sein.

Es wäre widersinnig, die mit der Novelle bezweckte Lockerung der Beherrschbarkeitsregel unter Berufung auf andere Bestimmungen zu verhindern. Daher wird bislang unbestritten da-

von ausgegangen, dass Art. 8 Abs. 5 und Art. 13 Abs. 1 WÜ und damit auch der neue Art. 8 Abs. 5bis Spezialregeln enthalten, die jenen Bestimmungen vorgehen.[49]

Übersteuerbare Fahrzeugsysteme werden danach ausdrücklich von Satz 2 des Art. 8 Abs. 5bis WÜ erfasst. Daraus lässt sich bereits schließen, dass Satz 1 auch solche Systeme erfassen muss, die nicht übersteuerbar sind, da er andernfalls keinen eigenen Anwendungsbereich hätte.

Die Änderung des Übereinkommens wird sich durch die UN/ECE-Regelungen (R 79) und EU-Richtlinien, insbesondere 2007/46/EG, nicht nur auf das deutsche Verkehrszulassungs- und Verhaltensvorschriften (StVZO, FZV, StVO etc.) auswirken, sondern auch auf das hiesige Haftungs-, Versicherungs- und Strafrecht.[50]

2. Fahrzeugteileübereinkommen von 1958 (FTÜ)

Neben dem Wiener Übereinkommen ist das Fahrzeugteileübereinkommen von 1958 (FTÜ)[51] ein weiterer völkerrechtlicher Vertrag, der Zulassungsvoraussetzungen regelt und die gegenseitige Anerkennung von Fahrzeuggenehmigungen erleichtern soll.

3. ECE-Regelungen

Auf Grundlage des Fahrzeugteileübereinkommens wurden von den Vertragsparteien ECE-Regelungen für Radfahrzeuge, Ausrüstungsgegenstände und Teile, die in Radfahrzeuge eingebaut werden können erlassen. Diese technischen Bauvorschriften sind aufgrund der zwingenden unionsrechtlichen Vorgaben in Anhang IV Teil 1 der RL 2007/46/EG bei der Fahrzeugzulassung zu beachten.

Mit fortschreitender Automatisierung werden Fahrzeuge künftig vermehrt Überholvorgänge oder Spurwechsel selbstständig einleiten und ausführen können. Autonome Lenkanlagen sind mit der ECE-Regelung 79 zu Lenkanlagen ausgenommen und daher bislang nicht zulas-

---

[49] *Lohmann*: Erste Barriere für selbstfahrende Fahrzeuge überwunden – Entwicklungen im Zulassungsrecht, www. http://sui-generis.ch/17, Abschnitt III; *dies*, Automatisierte Fahrzeuge im Lichte des Schweizer Zulassungs- und Haftungsrechts, 2016, im Erscheinen; *Cacilo et al.*, Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen, 2015, S. 120 ff.

[50] *Neidhart*, ZAP 2016, 503 f..

[51] „Übereinkommen über die Annahme einheitlicher technischer Vorschriften für Radfahrzeuge, Ausrüstungsgegenstände und Teile, die in Radfahrzeuge(n) eingebaut und/oder verwendet werden können, und die Bedingungen für die gegenseitige Anerkennung von Genehmigungen, die nach diesen Vorschriften erteilt wurden“(UNECE 1995).

sungsfähig. Fahrerassistenz-Lenkanlagen, die den Fahrer beim Lenken unterstützen, sind zulässig, solange der Fahrzeugführer die Hauptverantwortung beim Führen behält. Durch Abs. 5.1.6.1. der allgemeinen Bauvorschriften für Lenkanlagen werden automatisierte Lenkfunktionen allerdings dahingehend eingeschränkt, dass sich die Steuerung bei einer Überschreitung der Fahrzeuggeschwindigkeit von 10 km/h um 20 % automatisch abschalten muss. Daher können auf Grundlage dieser Vorschrift derzeit nur Einparkassistenten genehmigt werden

Ferner ist nach § 5 Abs. 4a StVO das Ausscheren zum Überholen und das Wiedereinordnen rechtzeitig und deutlich durch Benutzung des Fahrtrichtungsanzeigers anzuzeigen. Wird der Überholvorgang oder Spurwechsel durch das System übernommen, bedarf es ebenfalls einer automatischen Aktivierung des Fahrtrichtungsanzeigers, die bislang von der einschlägigen ECE-Regelung 6 nicht umfasst ist.

Vollautomatisierte Fahrzeuge sind momentan daher nicht zulassungsfähig und können folglich nicht über den Verweis in Art. 8 Abs. 5bis S. 1 WÜ als mit dem WÜ vereinbar gelten. Das für die Änderungen der ECE-Regeln zuständige Gremium, die WP 29 der UNECE, hat jedoch bereits Anfang des Jahres 2015 eine sog. „Informal Group“ eingerichtet, die kurzfristig Änderungsvorschläge erarbeiten soll. Im günstigsten Fall könnte insbesondere die ECE-Regel 79 daher noch im Jahr 2016 modifiziert werden.

4. „eCall“-VO 2015/758/EU

Ab dem 31.03.2018 ist für neue Fahrzeugmodelle eine Ausrüstung mit dem Notrufsystem „eCall“ verpflichtend. Durch dieses System soll ein Unfall über die im Fahrzeug vorhandenen Sensoren automatisch erkannt und einen Notruf über das Mobilfunknetz absetzen.

In einem Minimaldatensatz nach DIN EN 15722 erhalten die Rettungsdienste Angaben zum Standort, zur Fahrtrichtung, zum Unfallzeitpunkt, zur Anzahl der Insassen und zum Fahrzeugtyp, um so schnell und effizient Hilfe leisten zu können.[52] Der Autofahrer kann den eCall-Notruf ebenfalls manuell auslösen.

Die Datenverarbeitung ist auf die Rettungsleitstelle und ihre Hilfsmaßnahmen beschränkt. Auch eine Ortung findet nur im Notfall statt.

Durch die europäische Regelung soll sowohl eine Transparenz für den Betroffen wie auch die Grundsätze der Datensparsamkeit, Zweckbindung und Erforderlichkeit gewahrt bleiben. Konkretisierungen hinsichtlich der einzelnen Vorschläge sollen jedoch auf untergesetzlicher Ebene erfolgen.

[52] Vgl. Bönninger, zfs 2014, 184, 186.

Eine Regulierung des Datenschutzes hatte die Verordnung 2015/758/EU über Anforderungen für die Typengenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen zum Ziel. In Art. 6 der Verordnung 2015/758/EU wurden nunmehr in 13 Absätzen konkrete technische und rechtliche Anforderungen an das System gestellt.

In dieser Vorschrift ist unter anderem festgelegt, dass kein Austausch zwischen dem öffentlichen eCall System und den optionalen privat betriebenen Systemen in einem Fahrzeug möglich sein darf.

Zur Umsetzung dieser Anforderung hatte beispielsweise die nordrheinwestfälische Polizei mit BMW vertraglich vereinbart, dass „die fest in die Streifenfahrzeuge eingebauten SIM-Karten (embedded SIM) von der BMW AG beim Netzbetreiber abgemeldet werden. Somit ist nur der reine eCall (Notruf 112), der ab 2018 für die Erlangung der Betriebserlaubnis von Neufahrzeugen vorgeschrieben ist, ohne weitere Datenübermittlung gewährleistet. Eine darüberhinausgehende Datenübertragung, z.B. an BMW, wurde durch diese Maßnahme ausgeschlossen.“[53]

Die nunmehr in der Verordnung 2015/758/EU über Anforderungen für die Typengenehmigung zur Einführung des eCall-Systems konkretisierten technischen und rechtlichen Anforderungen an eine Datenschutzregulierung zeigen deutlich, dass der Gesetzgeber auch für neuartige Technologien detaillierte Datenschutzanforderungen festlegen kann.

5. EU-RiLi 2007/46/EG

Die Typengenehmigungsanforderungen sind derzeit in der Richtlinie 2007/46/EG geregelt. Nach Art. 4 Abs. 2 der RiLi 2007/46/EG darf eine Genehmigung für Fahrzeuge, Systeme, Bauteile oder selbstständige technische Einheiten von den Mitgliedstaaten nur erteilt werden, wenn sie den Anforderungen der Richtlinie entsprechen. Regelungen zum Datenschutz und zur Datensicherheit sind in den Vorschriften bislang nicht enthalten.

II. Änderungsvorschläge für die EU-Typgenehmigung – EU-RiLi 2007/46 (COM 2016/31 final)

Bereits in den Erwägungsgründen sollten der Datenschutz und die Datensicherheit hinreichend berücksichtigt und erwähnt werden.

[53] https://netzpolitik.org/2016/neue-streifenwagen-in-nrw-uebermitteln-keine-daten-an-bmw/.

Bei der Verarbeitung personenbezogener Daten durch automatisierte oder vernetzte Fahrzeugfunktionen sind die Vorschriften zum Datenschutz gemäß Art. 5-11 DSGVO in vollem Umfang einzuhalten, insbesondere damit gewährleistet werden kann, dass Fahrzeuge mit automatisierten oder vernetzten Funktionen nur nach informierter Einwilligung verfolgbar sind.

Nach Art. 5 Nr. 1 des Vorschlags für eine Typgenehmigungsverordnung (COM 2016/31) müssen Fahrzeuge, Systeme, Bauteile und selbstständige technische Einheiten die Anforderungen der in Anhang IV aufgeführten Durchführungsrechtsakte erfüllen. Art. 5 Nr. 2 ermächtigt die Kommission, gemäß Art. 88 delegierte Rechtsakte zu erlassen, um die Anforderungen in Anhang IV unter anderem zu ergänzen.

Von dieser Ermächtigungsgrundlage sollte die Kommission Gebrauch machen. Außerdem sollten die Anforderungen an den Datenschutz und die Datensicherheit in den für alle Fahrzeugklassen geltenden Anhang IV aufgenommen werden, um die Einhaltung des Datenschutzes und der Datensicherheit bereits bei der Zulassung der Fahrzeuge zu gewährleisten.

1. Konkretisierungen zur Datensicherheit (Manipulationssicherheit)

Weltweit im Fokus steht derzeit die Manipulation von Fahrzeugsoftware. Ursächlich für diese Entwicklung sind nicht zuletzt die unzureichenden Formulierungen der rechtlichen Regelungen, die die Sicherheit (Integrität) der Fahrzeugdaten betreffen. Zur Vermeidung solcher Entwicklungen in der Zukunft müssen rechtliche Grundlagen auch zur Konkretisierung der Fahrzeugdatensicherheit geschaffen werden, die automatisierte und vernetzte Fahrzeuge hinreichend berücksichtigen.[54] Sollte es doch zu einer sicherheitsrelevanten Fahrzeugdaten-Panne kommen, muss sichergestellt sein, dass das Fahrzeug eigenständig mit einem Notsystem an den Fahrbahnrand fährt und anhält. Im Folgenden werden einige Anregungen zur Anpassung des Vorschlages für eine Verordnung des Europäischen Parlaments und des Rates über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für dieses Fahrzeug (COM 2016/31 final) und der Richtlinie 2014/45/EU erläutert.

a) Offenlegung von Quellcodes zur Prüfung der Fahrzeugsoftware

Art. 23 enthält eine Regelung, welche zusätzlichen Angaben bei Anträgen auf bestimmte EU-Typgenehmigungen bereitzustellen sind. Nach Ziffer 4 erhalten die Typengenehmigungsbehörde und der technische Dienst Zugang zur Software und den Algorithmen des Fahrzeugs.

[54] S. bereits oben: Zweiter Abschnitt unter Ziff. IV.

Diese Vorschrift sollte dahingehend ergänzt werden, dass die genannten Stellen ebenso Zugang zu den Quellcodes des Fahrzeugs erhalten.

Hintergrund ist, dass Verstöße gegen die Verordnung ohne eine Offenlegung der Quellcodes nicht oder nur schwer erkannt werden können.

Die in Absatz 2 der Vorschrift enthaltene Möglichkeit, nach der die Genehmigungsbehörde vom Hersteller unter Angabe von Gründen zusätzliche Informationen anfordern kann, die für die Entscheidung über die erforderlichen Prüfungen notwendig sind oder die die Durchführung der Prüfung erleichtern, reicht für die Erkennung nicht aus.

b) PTI – Periodische Fahrzeugüberwachung

Das Sicherheitsniveau der Fahrzeugdaten ist zudem über den gesamten Fahrzeuglebenszyklus auf einem einheitlich hohen Niveau zu halten. Die Vorschriften zur regelmäßigen technischen Fahrzeugüberwachung (PTI = Periodical Technical Inspection) basieren auf der Richtlinie 2014/45/EU.

Die Untersuchungskriterien Ausführung, Zustand, Funktion und Wirkung sind für sicherheitsrelevante elektronische Funktionen möglichst eindeutig in den internationalen Vorschriften festzulegen.

Um Auffälligkeiten des Zustandes von sicherheitsrelevanten Funktionen künftig bewerten zu können, bedarf es darüber hinaus differenzierter Prüffeststellungen nach Softwareversion, Länderkennung und Konfiguration.

Nach Art. 6 Abs. 2 der Richtlinie ist eine Demontage von Bauteilen, Abdeckungen o.ä. bei der regelmäßigen technischen Untersuchung der Fahrzeuge nicht zulässig. Dies führt bei der Untersuchung von Kraftfahrzeugen im Rahmen der Untersuchung dazu, dass eine Sichtprüfung von sicherheits- und emissionsrelevanten Bauteilen nicht mehr möglich ist, was eine Funktionsprüfung mit Nutzung der elektronischen Fahrzeugschnittstelle unerlässlich macht. Aus diesem Grund ist die Einbeziehung der elektronischen Fahrzeugschnittstelle bereits in der PTI-Richtlinie 2014/45/EU enthalten. Es sollte auch ein Verweis in die Typengenehmigungsrichtlinie 2007/46 (COM2016/31 final) auf die Richtlinie 2014/45/EU aufgenommen werden, die einen Nachweis der Durchführbarkeit der in der Richtlinie 2014/45/EU vorgeschriebenen Prüfungen fordert.

c) Exkurs: Datenbereitstellung für PTI

Es sollte eine Klarstellung mit dem Inhalt aufgenommen werden, dass vollständige OBD-, Reparatur- und Wartungsinformationen auch Organisationen zur Erarbeitung und Bereitstellung von PTI-Vorgaben zur Verfügung gestellt werden.

Der Rechtsanspruch von Organisationen zur Erarbeitung und Bereitstellung von PTI-Vorgaben auf den diskriminierungsfreien Zugang zu dem OBD-, Reparatur- und Wartungsinformationen ist derzeit nicht ganz eindeutig formuliert. Aufgrund dessen wird die Herausgabe der nach der EU-Verordnung 715/2007 zu liefernden Diagnosedaten von den Fahrzeugherstellern derzeit teilweise verweigert.

Ohne Zugang zu den vollständigen Daten ist die Entwicklung moderner elektronischer Prüfungen für die regelmäßige technische Überwachung und deren Umsetzung auf EU-Ebene jedoch mit einem unverhältnismäßigen Aufwand verbunden, da die erforderlichen Daten alternativ nur durch Re-Engineering beschafft werden können.

Es bedarf daher einer Klarstellung in den nachfolgenden Vorschriften der EU-Typengenehmigungsrichtlinie 2007/46 (COM 2016/31 final), dass die vollständigen OBD-, Reparatur- und Wartungsinformationen auch Organisationen zur Erarbeitung und Bereitstellung von PTI-Vorgaben zur Verfügung gestellt werden.

Artikel 3 Begriffsbestimmungen

(47) „unabhängiger Wirtschaftsteilnehmer“

eine natürliche oder juristische Person, die kein Vertragshändler oder keine Vertragswerkstatt und direkt oder indirekt an der Wartung und Reparatur von Fahrzeugen beteiligt ist, einschließlich Reparaturbetriebe, Hersteller oder Händler von Werkstattausrüstung, Werkzeugen oder Ersatzteilen, Herausgeber von technischen Informationen, Automobilclubs,

Pannenhilfsdienste, Anbieter von Inspektions- und Prüfdienstleistungen entspr. 2014/45/EU, Organisationen zur Erarbeitung und Bereitstellung von PTI-Vorgaben sowie Einrichtungen der Aus- und Weiterbildung von Mechanikern, Herstellern und Reparaturkräften für Ausrüstungen von Fahrzeugen, die mit alternativen Kraftstoffen betrieben werden;
hierzu gehören auch Vertragswerkstätten und Händler, die zum Vertriebsnetz eines Fahrzeugherstellers gehören, sofern sie Reparatur- und Wartungsarbeiten an Fahrzeugen ausführen, die nicht von dem Hersteller stammen, zu dessen Vertriebsnetz sie gehören;

Artikel 65

Pflichten des Herstellers zur Bereitstellung von Reparatur- und Wartungsinformationen

1. Die **Hersteller gewähren** unabhängigen Marktteilnehmern **uneingeschränkten und standardisierten Zugang zu Fahrzeug-OBD-Informationen**, Diagnose- und anderen Geräten und Instrumenten einschließlich einschlägiger Software sowie zu Fahrzeugreparatur- und -wartungsinformationen.

Die Hersteller stellen eine standardisierte, zuverlässige und ortsungebundene Struktur zur Verfügung, die es unabhängigen Reparaturbetrieben ermöglicht, Arbeiten durchzuführen, bei denen auf das Sicherheitssystem des Fahrzeugs zugegriffen werden muss.

Anlage 2 OBD-Informationen

1. Der Fahrzeughersteller muss die folgenden, in dieser Anlage geforderten Informationen bereitstellen, damit die Herstellung von OBD-kompatiblen Ersatzteilen und Diagnose und Prüfgeräten ermöglicht wird.

2. Die folgenden Informationen sind allen interessierten Herstellern von Bauteilen oder Diagnose- und Prüfgeräten sowie Organisationen zur Erarbeitung und Bereitstellung von PTI-Vorgaben auf Anfrage zu gleichen Bedingungen zur Verfügung zu stellen:

Anlage 2 OBD-Informationen

3. Für die Herstellung von Diagnosegeräten erforderliche Informationen

Um die Bereitstellung universeller Diagnosegeräte für Mehrmarken-Reparaturbetriebe sowie Organisationen zur Erarbeitung und Bereitstellung von PTI-Vorgaben zu vereinfachen, müssen Fahrzeughersteller die Informationen gemäß den Nummern 3.1, 3.2 und 3.3 auf ihren Reparaturinformations-Websites zugänglich machen. Diese Informationen müssen alle Diagnosefunktionen sowie alle Links zu Reparaturinformationen und Anweisungen zur Störungsbehebung umfassen. Für den Zugang zu diesen Informationen kann eine angemessene Gebühr erhoben werden.

Für die PTI-relevanten Daten (z.B. FIN-spezifische Vorgaben, Prüfverfahren) ist ein offenes, konvertierbares und effizientes Austauschformat für eine vorgegebene Datenbankstruktur eindeutig zu definieren, um die durch die steigende Komplexität der sicherheitsrelevanten Fahrzeugtechnik verursachte Kostensteigerung zu reduzieren.

d) Anwendbarkeit der Prüfverfahren in PTI

Die verifizierten Prüfverfahren, Daten und Informationen sollten daher auch bei der Hauptuntersuchung Anwendung finden, um die Sicherheit, Umweltverträglichkeit und zukünftig auch Datensicherheit und Datenschutz eines Fahrzeugs kontinuierlich sicherzustellen.

Darüber hinaus sollte die EU-PTI-Richtlinie um bislang fehlende sicherheitsrelevante Funktionen erweitert und deren Prüfverfahren festgelegt werden.

2. Sanktionen

Die VW-Abgasaffäre hat darüber hinaus gezeigt, dass in den meisten EU-Mitgliedsstaaten derzeit keine ausreichenden Sanktionsmöglichkeiten bei Verstößen gegen die Typenzulassungsverordnung bestehen.

Die Einhaltung eines verlässlichen Zulassungsverfahrens gemäß der Verordnung kann aber nur sichergestellt werden, wenn diese zugleich wirkungsvolle, verhältnismäßige und abschreckende Sanktionsinstrumente vorsieht.

Art. 89 und 90 der Verordnung greifen diesen Aspekt bereits auf, überlassen die Regelung der Sanktionen bei Verstößen aber nach Art. 89 Abs. 1 der Verordnung den einzelnen Mitgliedsstaaten.

Zur Schaffung gleicher Wettbewerbsregelungen im europäischen Wirtschaftsraum, ist es jedoch unerlässlich, einheitliche Sanktionsmöglichkeit für die Typengenehmigungsbehörden in allen Mitgliedsstaaten aufzustellen.

Daher wird angeregt, eine allgemeingültige und klar definierte Sanktion in Erwägungsgrund 40 und Artikel 89 bei Verstößen gegen die Verordnung aufzunehmen.

Die Sanktionen sollten bei einmaligen und leichten Verstößen zunächst eine abgestufte Strafzahlung festlegen, die anhand festgelegter Kriterien bestimmbar sein sollte. Hierdurch soll eine unterschiedliche Festlegung durch einzelne Mitgliedsstaaten vermieden werden.

Die Strafzahlungen könnten sich je nach Gewicht des Verstoßes im Rahmen von 5.000,00 € bis 50.000 € bewegen. Dabei sollte ferner festgelegt werden, dass die Zahlungen pro Verstoß und Fahrzeug festgesetzt werden, um eine wirkungsvolle Abschreckung Massenverstößen des Herstellers zu erzielen.

Darüber hinaus sollten die Hersteller verpflichtet werden, bei festgestellten Verstößen, die Daten in den Typengenehmigungsunterlagen zu korrigieren.

Bei schwereren oder wiederholten Verstößen sollte ebenfalls ein Entzug der Typengenehmigung festgeschrieben werden.

Explizit aufgenommen werden sollte ferner ein Verstoß gegen Artikel 69, der den Zugang zu Reparatur und Wartungsinformationen regelt. Darüber hinaus sollte der Einsatz von Abschaltautomatiken (sog. Defeat device) sanktioniert werden.

Vierter Abschnitt: Weitere rechtliche Maßnahmen

Erstes Kapitel: Möglichkeiten externer Datenschutzzertifizierungen

Mit der Normierung eines Europäischen Datenschutzsiegels wird der Datenschutz durch die Aktivierung selbstregulierender Kräfte gestärkt. Die Nutzung von Datenschutzzertifizierungen bietet sich insbesondere bei der Kfz-IT an. Die Kundenakzeptanz spielt in diesem Markt eine herausragende Rolle.

Bislang sind in Art. 42 Abs.1 und Abs. 3 DSGVO Datenschutzzertifizierungen vorgesehen, wie sie durch das Unabhängige Landeszentrum für Datenschutz (ULD) gemäß nationalem als auch europäischem Recht, - dem Gütesiegel Schleswig Holstein und dem European Privacy Seal entwickelt wurden.

Die Möglichkeit der Zertifizierungen von Verarbeitungsvorgängen stellt ein wichtiges Instrument der Selbstregulierung dar. Hierdurch kann nachgewiesen werden, dass die Datenschutz-Grundverordnung bei Verarbeitungsvorgängen eingehalten wird. Gemäß Art. 42 Abs. 5 DSGVO werden die Zertifizierungskriterien von den Aufsichtsbehörden gegebenenfalls in einem Kohärenzverfahren festgelegt. Die Zertifizierung ist nicht allein den Aufsichtsbehörden vorbehalten, sondern kann auch durch eine private, akkreditierte Zertifizierungsstelle wahrgenommen werden, sofern diese unabhängig ist und über eine hinreichende Sachkunde verfügt.[55] Hierdurch ist die Möglichkeit eröffnet, dass die Sachkunde Dritter in den Prozess mit einbezogen werden kann.

Art. 43 Abs. 8f. DSGVO eröffnet ferner die Möglichkeit, dass in delegierten Rechtsakten Anforderungen sowie in Durchführungsrechtsakten technische Standards von der Europäischen

[55] Art. 43 Abs. 1 und Abs. 2 DSGVO.

Kommission festgelegt werden. Problematisch hieran ist, dass die Erlasse technikneutral formuliert sind und konkrete Zertifizierungsinhalte zunächst spezifiziert werden müssen. International anerkannte Standards zur Ausgestaltung datenschutzrechtlicher Vorgaben bestehen bislang nicht.

Um verlässliche Aussagen für Verbraucher treffen zu können, muss gewährleistet sein, dass Zertifizierungsdienste geeignete inhaltliche und organisatorische Vorkehrungen für Datenschutzzertifizierungen entsprechend der DSGVO im automatisierten Fahrzeug treffen, um eine sachgerechte und unabhängige Bewertung vorzunehmen. Hierbei sollten insbesondere Bedingungen für die Erteilung, die Geltungsdauer und den Entzug von Zertifikaten bestimmt werden. Zudem sollten die geprüften und zertifizierten Sachbereiche für die Kunden so umschrieben werden, dass sie die Reichweite der Prüfaussage ohne Fachkenntnisse dem Zertifikat entnehmen können.

Für die Bestätigung käme zunächst eine Common-Criteria-Zertifizierung nach ISO/IEG 15408 des Bundesamtes für Sicherheit in der Informationstechnik in Betracht.

Beim Entwicklungsprozess der Sicherheitssiegel sollten Automobilhersteller und Zulieferer für Produkte aus dem Bereich des automatisierten und vernetzten Fahrens maßgeblich beteiligt werden, um das gebotene Maß an Verfügbarkeit, Vertraulichkeit und Integrität der Daten zu gewährleisten.

Zertifizierungen haben eine Höchstgültigkeit von drei Jahren und können verlängert werden, solange die Voraussetzungen erfüllt sind.[56] In diesem Zusammenhang ist es bei der Ausgestaltung erforderlich, dass beim Einsatz von Zertifikaten oder vergleichbaren Sicherheitseinrichtungen die Handlungsfähigkeit des Systems auch beim Gültigkeitsablauf oder Entzug des Zertifikates in Notfallsituationen sichergestellt bleibt.

Zweites Kapitel: Aktuelle Gesetzesinitiativen

I. Exkurs: „Security and Privacy in your car Act (SPY car Act) of 2015“ des US-Senates

Als Anhaltspunkte für Gesetzesinitiativen in Deutschland und Europa kann der Blick zunächst auf die aktuelle Rechtsentwicklung in den USA gerichtet werden.

Dem US-amerikanischen Datenschutzrecht ist das dem europäischen Datenschutzrecht innewohnende Prinzip des Verbots mit Erlaubnisvorbehalt fremd. Anders als in der EU können

[56] Art. 43 Abs. 7 DSGVO.

sich die Betroffenen in den USA nicht auf allgemeine Normen des Datenschutzrechtes berufen. Ein Schutz besteht nur, soweit eine entsprechende Norm existiert. Vor diesem Hintergrund wurde in den USA eine Gesetzesinitiative als staatliche Regulierung gestartet. Durch den „SPY car Act" sollen Automobil-Hersteller, die auf dem US-Markt tätig sind, verpflichtet werden, „angemessene Maßnahmen gegen Hacker-Angriffe" zu treffen. Hierbei sollen alle möglichen Angriffspunkte abgesichert werden.

Die Anforderungen an die technische Datensicherheit sind im Gesetzesentwurf allgemein gehalten. Es wird beispielsweise gefordert, „angemessene Maßnahmen zum Schutz gegen Hacking-Angriffe" zu implementieren und kritische von nicht kritischen Systemen zu trennen.[57]

In Hinblick auf die Datenschutzanforderungen bezweckt das Gesetz in erster Linie eine Transparenz für den Verbraucher. Hierfür wird eine „Cyber-Anzeige" der Datensicherheit im Auto vorgeschlagen, durch die Insassen anhand standardisierter und leicht verständlicher Grafiken über die IT-Sicherheit und den Schutz der Privatsphäre im Fahrzeug informiert werden.

Angesichts der Gesetzesinitiative wird nun auch in Deutschland die Frage nach einer entsprechenden rechtlichen Regelung[58] laut.

Anhand der obigen Ausführungen wird ersichtlich, dass auch in Deutschland eine Vielzahl von Kfz-spezifischen Sachverhalten gesetzlich entweder gar nicht oder nur unzureichend geregelt sind. Der Schaffung eines eigenen umfassenden Gesetzes zur IT-Sicherheit und zum Datenschutz in Autos entsprechend dem Vorbild der USA bedarf es allerdings nach der hiesigen Auffassung dennoch nicht. Vielmehr hat der europäische Gesetzgeber mit der Regulierung des eCalls bewiesen, dass auch bei neuen Diensten konkrete Datenschutzanforderungen normiert werden können. Es sollten daher die erforderlichen technischen, rechtlichen und organisatorischen Maßnahmen im Kfz-Bereich durch einheitliche Datenschutz- und Datensicherheitsstandards in den europäischen und nationalen Zulassungsverordnungen festgeschrieben werden.

Hierdurch kann der Gefahr widersprüchlicher Regelungen in unterschiedlichen Gesetzen begegnet werden.

---

[57] *Reibach*: „Smart Cars – Smart Privacy Law? Regionale Datenschutzregulierung des KFZ", in: Smart World – Smart Law? Tagungsband Herbstakademie 2016, S. 13 ff., 21.
[58] Vgl. *Schulzki-Haddouti, Christiane*: IT-Sicherheitsgesetz für Autos in den USA vorgestellt, abrufbar unter http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-fuer-Autos-in-den-USA-vorgestellt-2761772.html (zuletzt abgerufen am 02.11.2016).

II. Geplante Änderung des Straßenverkehrsgesetzes

Nach der Änderung des Wiener Übereinkommens steht mit der Reform des Straßenverkehrsrechts nun der nächste Schritt in Richtung des hochautomatisierten Fahrens bevor. Im Bundesverkehrsministerium liegt derzeit ein Änderungsentwurf des Straßenverkehrsgesetzes vor, um dem hochautomatisierten Fahren in Deutschland die erforderliche Rechtsgrundlage zu geben.

Beim G7-Verkehrsministertreffen in Karuizawa/Japan hat Bundesverkehrsminister Dobrindt am 24.09.2016 seinen Gesetzentwurf zum automatisierten und vernetzten Fahren vorgestellt. Kern der Änderung des Straßenverkehrsgesetzes ist die rechtliche Gleichstellung von menschlichem Fahrer und automatisiertem System.[59]

Parallel hierzu ist auf internationaler Ebene allerdings noch eine entsprechende weitere Änderung des Wiener Übereinkommens erforderlich, da bislang dessen Art. 8 Abs. 1, 5 und 6 die permanente Beherrschung durch seinen Fahrer verlangt. Dies steht bislang einer internationalen Einführung höherer Entwicklungsstufen des automatisierten Fahrens entgegen.

1. Haftung für Verkehrsunfälle

Schon heute wird die Sicherheit im Straßenverkehr durch die Nutzung von Fahrassistenzsystemen erhöht. Da statistisch gesehen 90 % aller Verkehrsunfälle auf menschliches Versagen zurückzuführen sein sollen[60], wird prognostiziert, dass sich zukünftig durch zunehmend automatisiert gesteuerte Fahrzeuge die Verkehrsunfallzahlen erheblich reduzieren sollen. Der Mensch, der äußeren Einflüssen wie der Mündigkeit oder Ablenkung unterliege, falle als Unfallverursacher weg.[61]

Gleichwohl wird auch zukünftig mit Verkehrsunfällen zu rechnen sein, sodass die Haftung eine entscheidende Frage des autonomen Fahrens ist.

Nach dem derzeitigen Gesetzesentwurf darf sich der Fahrzeugführer von der Fahrzeugsteuerung und dem Verkehrsgeschehen abwenden. Er muss jedoch derart „wahrnehmungsbereit bleiben“, dass er „nach Aufforderung durch das automatisierte System die Fahrzeugsteuerung

---

[59] http://www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2016/152-dobrindt-g7-verkehrsministertreffen.html
[60] 2015 wurden in Deutschland rund 366.000 Unfälle durch menschliches Fehlverhalten verursacht, https://www.destatis.de/DE/ZahlenFakten/Wirtschaftsbereiche/TransportVerkehr/Verkehrsunfaelle/Tabellen/FehlverhaltenFahrzeugfuehrer.html
[61] *Brisch, Klaus / Müller-ter Jung, Marco*: Autonomous Driving – Von Data Ownership über Blackbox bis zum Beweisrecht, in CR 6/2016, S. 411, 412.

wieder übernehmen“ und auf „erkennbare technische Störungen angemessen reagieren“ kann.[62]

Welche Anforderungen an die Wahrnehmungsbereitschaft gestellt werden, geht aus dem Gesetzentwurf nicht hervor. Da es sich um die zentrale Norm für die Verteilung der Verantwortlichkeit zwischen Fahrer und System handelt, sind aber Konkretisierungen erforderlich. Dies betrifft u.a. die Fragen, wie der jeweilige Fahrer über die bestimmungsgemäße Nutzung informiert wird, welche Tätigkeiten für die Wahrnehmungsbereitschaft zulässig sind, welche Reaktionszeit für die Übernahme durch den Fahrer angemessen ist und wie das System technische Störungen anzeigen muss.

Darüber hinaus wird auch das bisherige Haftungsmodell (Fahrer – Halter – Hersteller) voraussichtlich beibehalten. Das bedeutet, dass es im Falle des fehlenden Verschuldens des Fahrers bei der Gefährdungshaftung des Halters nach § 7 StVG bleibt. Dies soll dazu führen, dass letztendlich die Haftpflichtversicherung des Halters und die Versicherung des Herstellers klären müssen, wer die Kosten des Unfalls zu tragen habe. Die Haftungshöchstbeträge, wie sie heute in § 12 StVG vorgesehen sind, sollen nicht greifen, wenn ein Systemfehler unfallursächlich war.[63]

Die Haftung des Herstellers richtet sich auch bei Fahrzeugen mit automatisierten Fahrfunktionen nach den allgemeinen Vorschriften des Produkthaftungsgesetzes, des Produktsicherheitsrechts und der deliktischen Produzentenhaftung.

Gemäß § 1 ProdHaftG haftet der Hersteller für Personen und Sachschäden, die durch einen Fehler des Produktes verursacht werden.

Die Haftung des Herstellers ist allerdings nach § 1 Abs. 2 ProdHaftG ausgeschlossen, wenn einer der dort genannten Fälle vorliegt. Eine weitgehende Haftungseinschränkung folgt darüber hinaus aus der Legaldefinition des Produktfehlers in § 3 Abs. 1 ProdHaftG. Danach liegt ein Produktfehler vor, wenn das Produkt nicht die Sicherheit bietet, die zum Zeitpunkt des Inverkehrbringens berechtigterweise erwartet werden konnte.

Anders als im geplanten Gesetzentwurf zur Änderung des StVG ist der Anspruch auf Ersatz von Personenschäden, der durch ein Produkt verursacht wurde, nach § 10 Abs. 1 ProdHaftG auf 85 Mio. € beschränkt.

---

[62] *Grünvogel, Thomas*: Rechtslage für autonomes Fahren, abrufbar unter http://www.cmshs-bloggt.de/emobilitaet/rechtslage-fuer-autonomes-fahren-in-deutschland/ (zuletzt abgerufen am 05.10.2016).
[63] *Delhaes, D., Fasse, M., Menzel, S.*: Berlin will neue Standards setzen, in Handelsblatt vom 18.07.2016, S. 4 f.

Darüber hinaus kommt eine Haftung des Herstellers aus § 823 Abs. 2 BGB in Verbindung mit den Vorschriften des Produktsicherheitsgesetzes in Betracht, soweit diese als Schutzgesetze einzuordnen sind. Für Fahrzeuge sind hier insbesondere die spezialgesetzlichen Vorschriften, insbesondere die StVZO, die Verordnung über die EU-Genehmigung für Kraftfahrzeuge und ihre Anhänger, die Verordnung über die Prüfung der Genehmigung der Bauart von Fahrzeugteilen sowie deren Fahrzeugkennzeichnen sowie weitere europäische Vorschriften heranzuziehen. Die Schutzgesetzeigenschaft der Vorschriften des Produktsicherheitsgesetzes ist teilweise nicht abschließend geklärt. Gerade die Schutzgesetzeigenschaft der spezifischen Normen für Kraftfahrzeuge ist bislang nur unzureichend diskutiert worden. Grundsätzlich wird jedoch die Schutzgesetzeigenschaft für Vorschriften der StVZO, die Anforderungen an die Beschaffenheit von Fahrzeugen aufstellen, bejaht.[64] Zwar war die Haftung bislang ohne praktische Relevanz. Dies könnte sich jedoch mit der Festschreibung der konkreten technischen Anforderungen an automatisierte Systeme für den Hersteller ändern.

2. Datenschutz/Datenerhebung

Zur Klärung der Haftungsfrage sieht der Gesetzesentwurf künftig den verpflichtenden Einbau einer Blackbox vor. Diese soll aufzeichnen, wann das System aktiv war, wann der Fahrer fuhr und zu welchem Zeitpunkt das System den Fahrer zur Übernahme der Fahrzeugführung aufgefordert hat.[65]

Die Datenerhebung und –verarbeitung soll künftig in der Weise normiert werden, dass die vorgenannten aufgezeichneten Daten „...auf Verlangen zuständigen Kontrollorganen zugänglich zu machen“ sein sollen. Bei dieser Regelung ist schon unklar, wer die Daten zugänglich machen soll. Dies dürfte mit der rechtlich umstrittenen Frage, wer über die Daten verfügen darf, sowie den technischen Zugängen zu den Daten im Zusammenhang stehen und bedarf der Klärung.

Bedenklich ist ebenfalls die Regelung des Entwurfs über den Zugang zu den aufgezeichneten Daten. Der Gesetzentwurf sieht vor, dass „Dritten … Zugang zu diesen Daten zu gewähren (ist), wenn sie glaubhaft machen, dass die Daten zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen (…) benötigt werden“.[66] Auch hier ist nicht geregelt, wer die Daten zugänglich machen soll und auf welche Weise dies technisch und inhaltlich geschehen

[64] OLG Naumburg, Urteil vom 29.12.2011, Az. 4 U 65/11 (zu § 67 StVZO), *Borges*: Haftung für selbstfahrende Autos in CR 4/2016, S. 272 ff.
[65] *Delhaes, D., Fasse, M., Menzel, S.* (Fn. 36).
[66] *Noerr*, Zeitunglesen unerwünscht – Dobrindt-Entwurf setzt vollautonomem Fahren rechtliche Grenzen, abrufbar unter https://www.noerr.com/de/newsroom/News/zeitunglesen-unerw%C3%BCnscht-%E2%80%93-dobrindt-entwurf-setzt-vollautonomem-fahren-rechtliche-grenzen.aspx (zuletzt abgerufen am 05.10.2016).

soll. Diese Vorgehensweise sowie die Regelung einer strengen Zweckbindung der Daten müsste gesondert (ggf. durch Rechtsverordnung) ausgestaltet werden.

3. Exkurs: Parallelwertung Haftung und Unfalluntersuchung in der Luftfahrt

Bei der Bewertung der vorgesehenen Regelung zur Haftung anhand der Blackbox kann zunächst auf die Situation im Luftverkehr abgestellt werden. Die Steuerung eines hoch– oder vollautomatisierten Fahrzeugs ist zwar technisch nur eingeschränkt mit dem Fliegen eines Luftfahrzeuges mittels Autopilot vergleichbar.

Im Hinblick auf die nun vorgesehene technische Auswertung der sogenannten Blackbox können jedoch Parallelen aus der Luftfahrt gezogen werden. Gerade wenn es sich um Unfälle und Störungen von besonderer Bedeutung für die Sicherheit im Straßenverkehr handelt, kann eine vollständige Sachverhaltsaufklärung zur Vermeidung künftiger Schadensereignisse erforderlich sein.

Zwar dient die in § 3 Abs. 1 des Gesetzes über die Untersuchungen von Unfällen und Störungen bei dem Betrieb ziviler Luftfahrtflugzeuge (FiUUG) vorgesehene Unfallaufklärung ausschließlich dem Zweck der Ursachenaufklärung und schließt eine Feststellung des Verschuldens der Haftung oder von Ansprüchen nach § 3 Abs. 2 FiUUG aus.

Allerdings ist in § 21 FiUUG ein mit einer Anzahl von Ausnahmen gesetzlich normiertes Auskunftsrecht der Betroffenen vorgesehen. Danach hat die Bundesstelle für Fluguntersuchung den von dem Ereignis Betroffenen oder deren Rechtsbeiständen Auskunft aus den Akten des Untersuchungsverfahrens zu erteilen oder Akteneinsicht zu gewähren, soweit dies zur Feststellung, Durchsetzung oder zur Abwehr von Rechtsansprüchen im Zusammenhang mit dem Unfall oder der Störung erforderlich ist. Der Änderungsentwurf des StVG sieht nunmehr ebenfalls einen Auskunftsanspruch vor, der nach dem oben Gesagten gegen einen unbestimmten Dritten zu richten ist.

In diesem Zusammenhang liegt es nahe, im Rahmen der Unfallaufklärung für Verkehrsunfälle ein Treuhänder für die erhobenen Daten einzurichten. Der Vorteil eines solchen Treuhänders ist darin zu sehen, dass das nunmehr gesetzlich vorgesehene Auskunftsrecht bei einer zentralen und unabhängigen Stelle geltend gemacht werden können. Dadurch wird einerseits die Gefahr einer Manipulation der Schnittstellen und der erhobenen Daten vermieden, andererseits aber auch verhindert, dass der Betroffene seine Auskunftsansprüche erst zivilprozessual durchsetzen muss.

Drittes Kapitel: Aufbau und Betrieb einer intelligenten Verkehrssysteminfrastruktur und eines Trust Centers

Bereits im Jahr 2013 wurde die Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern durch das Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (ISVG) vom 11.06.2013[67] in nationales Recht umgesetzt.

§ 5 ISVG enthält eine Verordnungsermächtigung für das damalige Bundesministerium für Verkehr, Bau und Stadtentwicklung, durch Rechtsverordnung mit Zustimmung des Bundesrats die Anforderungen an intelligente Verkehrssysteme in vorrangigen Bereichen, § 4 ISVG zu regeln. Das nunmehr zuständige Bundesministerium für Verkehr und digitale Infrastruktur hat von dieser Ermächtigung bislang keinen Gebrauch gemacht. Mit intelligenten Verkehrssystemen können eine Vielzahl personenbezogener Daten erhoben und verarbeitet werden, sodass bei unzureichender Klärung der rechtlichen Rahmenbedingungen die Gefahr besteht, dass der Datenschutz ins Hintertreffen gerät.

Darüber hinaus ist die bislang mangelhafte Zusammenführung und Bereitstellung relevanter Verkehrsdaten ein zentrales Hemmnis für die vollumfängliche Nutzung der digitalen Möglichkeiten. Es fehlt an einer verbindlichen Koordination, die als neutrale Instanz mit den zuständigen Akteuren für die Bereitstellung, Pflege und Aktualität der Verkehrsdaten sorgt.

Um dies zu vermeiden, sollte von der Ermächtigungsgrundlage des ISVG und der StVZO Gebrauch gemacht werden und eine gesetzliche Grundlage für eine Digital-Verkehrsinfrastruktur-Gesellschaft im hoheitlichen Auftrag zur Planung, Errichtung und Unterhaltung der digitalen Infrastruktur für Intelligente Verkehrssysteme (IVS) geschaffen werden.

Darüber hinaus bedarf es des Aufbaus eines Trust Centers, das Verkehrsdaten für das reibungslose Funktionieren der intelligenten Verkehrsinfrastruktur verarbeitet und bereitstellt und dabei die geltenden aktuellen Datensicherheits- und Datenschutzstandards einhält. Das Trust Center "iMobile" hat heute u.a. die Maut- und Mobilfunkabrechnung übernommen und fungiert als Clearingstelle zwischen den verschiedenen Anbietern. Im Bereich der IVS bietet sich die Datenverarbeitung über ein Trust Center ebenfalls an. Über eine Public-Key-Infrastruktur könnte ein Trust Center Fahrzeugen Signaturen vergeben. Hierdurch werden dem Fahrzeug Signaturen zugewiesen, die einerseits eine eindeutige Identifizierbarkeit der Quelle einer übertragenen Information gewährleisten, anderseits ausschließen, dass personenbezogene Details über den Fahrer oder das Fahrzeug veröffentlicht werden.

[67] Intelligente Verkehrssysteme Gesetz vom 11. Juni 2013 (BGBl. I S. 1553), das durch Artikel 479 der Verordnung vom 31. August 2015 (BGBl. I S. 1474) geändert worden ist.

Über das Trust Center als neutrale Instanz könnten ebenfalls entsprechende Auskunftsersuchen für die Bereitstellung von Daten, wie sie nunmehr durch den Änderungsentwurf des Straßenverkehrsgesetzes vorgesehen sind, abgewickelt werden.

Diese sollte sich am Beispiel der Verkehrsinfrastrukturfinanzierungsgesellschaft (VIFG), der FSD – Zentralen Stelle nach StVG und der österreichischen Autobahnen- und Schnellstraßen-Finanzierungs-Aktiengesellschaft (ASFINAG) orientieren.

Diese Einrichtungen haben bereits gezeigt, dass ein Kompetenzzentrum für Infrastrukturinvestitionen enorme Vorteile bieten kann. Es ist unter anderem in der Lage, einheitliche Strukturen zu entwickeln und Standards zu setzen, Bewertungen zu professionalisieren und zu vereinheitlichen und einen einheitlichen, kompetenten Ansprechpartner bereitzustellen.

Die österreichische Autobahnbetreibergesellschaft ASFINAG beispielsweise wurde mit Kapital vom Bund ausgestattet. Sie sammelt und stellt bereits heute sämtliche Verkehrsdaten über seine zentrale Datendrehscheibe bereit. Darüber hinaus beteiligt sie sich an verschiedenen Projekten zur Planung und Erforschung von IVS und hat hierzu u.a. bereits auf dem Testfeld Telematik eine Vielzahl von Sensoren eingerichtet, um eine effiziente Erfassung von Verkehrsdaten zu ermöglichen.

Der Realisierung von Finanzierungsgesellschaften sind jedoch durch das Demokratieprinzip nach Art. 20 Abs. 2 GG rechtliche Grenzen gesetzt, da jede Ausübung von Staatsgewalt zumindest mittelbar demokratisch legitimiert sein muss. Dies bedeutet, dass bei der Einrichtung ein Verbleib der Aufgabe in öffentlicher Hand oder eine vertragliche Sicherung entsprechender Kontroll- und Einwirkungsmöglichkeiten beachtet werden muss.

In Deutschland könnte daher eine Finanzierungsgesellschaft gegründet werden, der im Interesse des Bundes konkrete Aufgaben zur effektiven Planung und Einrichtung intelligenter Verkehrssysteme übertragen werden.

Entsprechend dem österreichischen Modell sollte darüber hinaus frühzeitig eine sogenannte „IVS-Schlichtungsstelle“ zur außergerichtlichen Streitbeilegung eingerichtet werden. Durch die ständige Entwicklung neuer Dienste und Anwendungen im Bereich intelligenter Verkehrssysteme muss die Einhaltung entsprechender Datenschutz- und Datensicherheitsstandards gewährleistet sein. Mithin ist ein reibungsloser Geschäftsablauf zwischen den Bereitstellern von entsprechenden Diensten und deren Kunden im B2B-Bereich (Business to Business) und im B2C-Bereich (Business to Consumer) von immenser Bedeutung. Ziel des Schlichtungsverfahrens sollte es sein, bei Streitigkeiten in diesen Bereichen innerhalb eines angemessenen Zeitraumes ein für alle Beteiligen akzeptables Ergebnis herbeizuführen, um so kostspielige und langwierige Prozesse zu vermeiden.

Die Finanzierung ist für die Einrichtung intelligenter Verkehrssysteme ebenfalls ein wichtiger Aspekt. Da die Einführung intelligenter Verkehrssysteme voraussichtlich nicht kostendeckend errichtet werden kann, sind vom Bund Zuschüsse für die Finanzierung zu leisten.

Die zu gründende Gesellschaft sollte sich darüber hinaus an einer verstärkten Zusammenarbeit mit europäischen Ländern und deren Autobahnbetreibern orientieren.

In diesem Zusammenhang bedarf es der Festlegung eines einheitlichen Vernetzungsstandards (Machine-to-Machine), um später europaweit einen direkten und standardisierten Datenaustausch zu gewährleisten.

Fünfter Abschnitt: Zusammenfassung

Mit der Einführung der Datenschutzgrundverordnung wird zwar ein einheitlicher Datenschutzstandard in Europa geschaffen, der die datenschutzrechtlichen Leitlinien für vernetzte Fahrzeuge aufstellt. Dennoch werden die allgemein gehaltenen Bestimmungen der DSGVO den spezifischen Besonderheiten des Datenschutzes im Auto nicht gerecht. Es werden daher spezielle gesetzliche Regelungen benötigt, um dem Datenschutz und der Datensicherheit im vernetzten und automatisierten Fahrzeug einen hinreichend konkreten Rahmen zu geben.

Dies ist auch erforderlich, um einen Missbrauch und eine zweckfremde Verwendung von Daten zu verhindern, Manipulationen wirksam zu begegnen und Rechts- und Planungssicherheit für alle Akteure zu schaffen.

Hierzu sind bereichsspezifische Regelungen im nationalen und internationalen Zulassungs- und Verkehrsrecht sowie im europäischen Datenschutzrecht, ggf. auch im Rahmen von Rechtsverordnungen, erforderlich, um einheitliche Standards in Bezug auf Datenschutz und Datensicherheit im Fahrzeug vorzuschreiben. Der aktuell vorgesehene Regelungsansatz für automatisierte Systeme reicht dafür bei weitem nicht aus.

Im Einzelnen:

1. Rechtsanpassungen zur Einhaltung von Mindeststandards von Datenschutz und Datensicherheit in Fahrzeugen

a) Nationale Gestaltungsspielräume

Für die Gewährleistung eines effektiven Daten- und Verbraucherschutzes muss die Einhaltung der festgelegten Mindeststandards von Datenschutz und Datensicherheit bereits Voraussetzung für die Verkehrstauglichkeit und damit die Zulassung von Fahrzeugen sein. Datenschutz und Datensicherheit sind für den Straßenverkehr von zunehmender Relevanz, sodass eine Ermächtigungsgrundlage für das Verkehrsministerium geschaffen werden muss, um entsprechende Maßnahmen zu erlassen. Hierzu könnte in der Ermächtigungsnorm des § 6 Abs. 1 Nr. 2 StVG ergänzt werden, dass in der StVZO bei der Zulassung neben der Gewährleistung der Verkehrssicherheit auch auf die Gewährleistung der Datensicherheit und des Datenschutzes zu beachten sind. Das Gleiche gilt für die Verordnungsermächtigung über die regelmäßigen Hauptuntersuchungen der Fahrzeuge, die ebenso jedenfalls die Datensicherheit zum Gegenstand haben müssen.

Auch nach Inkrafttreten der DSGVO besteht neben der Zuständigkeit des Europäischen Gesetzgebers eine diesbezügliche Gesetzgebungskompetenz des nationalen Gesetzgebers, denn durch gesetzgeberische Maßnahmen im Zulassungsrecht wird lediglich die Einhaltung der DSGVO (u.a. die Einhaltung der Grundsätze des „Privacy by Design“ und „Privacy by Default“) zur Voraussetzung für die Zulassung eines Fahrzeugs für den Straßenverkehr gemacht. Damit werden erst die europarechtlichen Vorschriften der DSGVO im Kfz-Zulassungsrecht umgesetzt. Das von der DSGVO voll harmonisierte Datenschutzrecht wird hierbei inhaltlich nicht berührt.

b) Regelung in einer EU-Verordnung über die Betriebserlaubnisse von Kfz

Derzeit befindet sich ein neues Regelwerk auf europäischer Ebene für die Typgenehmigung von Kraftfahrzeugen in Bearbeitung. Hierin ist der Themenkomplex „Datensicherheit und Datenschutz“ zusätzlich zu den Umwelt- und Sicherheitszielen bzw. –anforderungen aufzunehmen. Dabei sind folgende Aspekte zu regeln:

- Zum *Schutz der Verkehrsteilnehmer vor Missbrauch ihrer Daten* sollten die Fahrzeughersteller den Grundsatz der Datenschutzgrundverordnung „eingebauter Daten-

schutz“ („privacy by design“) umsetzen und bei der Entwicklung entsprechende technische Vorrichtungen zur Sicherheit des Datenschutzes in die bordeigenen Systeme einbauen.

- Zur *Vermeidung von Fälschung, Manipulation und unbefugter Verwendung der Daten*, die von im und am Fahrzeug verbauten Systemen erfasst werden, müssen diese Systeme nachprüfbar geschützt sein. Sollte es doch zu einer sicherheitsrelevanten Fahrzeugdaten-Panne kommen, muss sichergestellt sein, dass das Fahrzeug eigenständig mit einem Notsystem an den Fahrbahnrand fährt und anhält.
- Zur *Vermeidung des Abfangens von Daten und der unbefugten Übernahme der Kontrolle über das Fahrzeug* muss jedes Fahrzeug, das Zugangspunkte zu elektronischen Systemen bietet, mit Fahrfunktionen ausgestattet sein, die derartige Angriffe sofort entdecken, melden und stoppen können. Diese Funktionen müssen regelmäßig gemäß geltender IT-Security-Standards auf Sicherheitslücken überprüft werden.

Um verlässliche Aussagen für Verbraucher treffen zu können, muss zudem gewährleistet sein, dass Zertifizierungsdienste geeignete inhaltliche und organisatorische Vorkehrungen für Datenschutzzertifizierungen entsprechend der DSGVO im Fahrzeug treffen, um eine sachgerechte und unabhängige Bewertung vorzunehmen.

c) Transparenz

Jedes Fahrzeug ist hinsichtlich des Inhalts und Umfangs der vorhandenen Datensicherheits- und Datenschutzsysteme durch eine standardisierte Grafik zu kennzeichnen, um den Nutzer auf eine leicht verständliche Weise hierüber zu informieren. Die EU-Kommission sollte in diesem Zusammenhang von der ihr eingeräumten Befugnis nach Art. 12 Nr. 8 DSGVO Gebrauch machen und delegierte Rechtsakte zur Bestimmung der Informationen, die durch Bildsymbole im Bereich des Fahrzeugdatenschutzes und der Fahrzeugdatensicherheit darzustellen sind, und der Verfahren für die Bereitstellung der standardisierten Bildsymbole erlassen.

d) Verknüpfung von Typengenehmigung und PTI : Regelmäßige technische Überwachung

Die Vorschriften zur regelmäßigen technischen Fahrzeugüberwachung (PTI = Periodical Technical Inspection) basieren auf der Richtlinie 2014/45/EU. In eine Neufassung dieser Richtlinie ist aufzunehmen, dass die Fahrzeuge so konstruiert werden, dass moderne elektronische Fahrzeugsysteme im Rahmen der regelmäßigen technischen Überwachung auch über die elektronische Fahrzeugschnittstelle untersucht werden können.

Die Typengenehmigungsbehörde und der technische Dienst müssen Zugang zur Software und den Algorithmen des Fahrzeugs haben. Entsprechende Vorschriften sollten dahingehend ergänzt werden, dass die genannten Stellen ebenso Zugang zu den Quellcodes des Fahrzeugs erhalten.

Zudem ist die Erfüllung der Anforderungen für die Prüfung der sicherheits- und umweltrelevanten Systeme, Bauteile und Funktionen über die Fahrzeugschnittstelle bereits bei der Fahrzeuggenehmigung nachzuweisen, um die Effizienz der Fahrzeuguntersuchungen und so die (Daten-)Sicherheit und den Datenschutz der zukünftig im Verkehr befindlichen Fahrzeuge sicherzustellen. Zudem sollten die geprüften und zertifizierten Sachbereiche für die Kunden so umschrieben werden, dass sie die Reichweite der Prüfaussage ohne Fachkenntnisse dem Zertifikat entnehmen können.

2. Best Practice für EU-Mitgliedsstaaten: Aufbau und der Betrieb einer Connected-Car-Infrastruktur

Mit intelligenten Verkehrssystemen können eine Vielzahl personenbezogener Daten erhoben und verarbeitet werden, sodass bei unzureichender Klärung der rechtlichen Rahmenbedingungen die Gefahr besteht, dass der Datenschutz ins Hintertreffen gerät. Andererseits ist die bislang mangelhafte Zusammenführung und Bereitstellung relevanter Verkehrsdaten ein zentrales Hemmnis für die vollumfängliche Nutzung der digitalen Möglichkeiten. Es bedarf daher des Aufbaus eines Kompetenzzentrums, das als neutrale Instanz mit den zuständigen Akteuren für die Bereitstellung, Pflege und Aktualität der Verkehrsdaten sorgt.

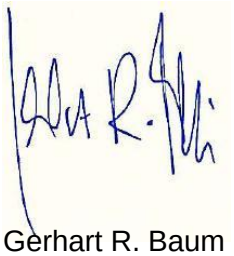
Der österreichische Autobahnbetreibergesellschaft ASFINAG beispielsweise sammelt bereits heute sämtliche Verkehrsdaten und stellt sie über seine zentrale Datendrehscheibe bereit. Darüber hinaus beteiligt sie sich an verschiedenen Projekten zur Planung und Erforschung von Verkehrsmanagementsystemen und hat hierzu u.a. bereits auf dem Testfeld Telematik eine Vielzahl von Sensoren eingerichtet, um eine effiziente Erfassung von Verkehrsdaten zu ermöglichen.

In Deutschland könnte ebenfalls eine Finanzierungsgesellschaft gegründet werden, die sich an dem Beispiel der ASFINAG orientiert und der im Interesse des Bundes konkrete Aufgaben zur effektiven Planung und Einrichtung intelligenter Verkehrssysteme übertragen werden.

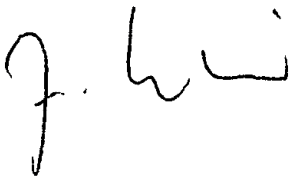
Entsprechend dem österreichischen Modell sollte darüber hinaus frühzeitig eine Stelle zur außergerichtlichen Streitbeilegung eingerichtet werden.

3. Vertrauen schaffen – Kernaufgabe eines unabhängigen „Trust Centers“

Zur Schaffung einer transparenten und gleichzeitig geschützten Verwaltung der Fahrzeugdaten sollte ein unabhängiges „Trust Center“ eingerichtet werden, das Fahrzeug- und Verkehrsdaten für das reibungslose Funktionieren der intelligenten Verkehrsinfrastruktur verwaltet, verarbeitet und bereitstellt und dabei die Datensicherheits- und Datenschutzstandards einhält. Als vertrauenswürdiger und neutraler Datentreuhänder für Fahrzeug- und Verkehrsdaten kann ein Trust Center daneben eine Vermittlerposition zwischen den Dateninhabern/-betroffenen und berechtigten Dritten einnehmen, um berechtigte Datenanforderungen zu prüfen und ggf. zu erfüllen.



Gerhart R. Baum
Rechtsanwalt
Bundesminister a.D.



Prof. Dr. Julius F. Reiter
Rechtsanwalt
FA für IT-Recht

Dr. Olaf Methner
Rechtsanwalt
FA für IT-Recht

Rechtsgutachten zur Kontrolle der Daten bei vernetzten und automatisierten Pkw

Gliederung **Seite**

Literaturverzeichnis

ADAC e.V.: Untersuchung an vier Fahrzeugen: „Welche Daten erzeugt ein modernes Auto?“, unter https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx (abgerufen am 03.11.2016).

Albrecht, Jan Philipp: Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, Heft 2, S. 88-98.

Beiker, Sven A.: Einführungsszenarien für höhergradig automatisierte Straßenfahrzeuge, in: Maurer, M. / Gerdes, J.C. / Lenz, B. / Winner, H. (Hg.): Autonomes Fahren. Technische, rechtliche und gesellschaftsrechtliche Aspekte, Berlin, 2015, S. 197-217.

Bönninger, Jürgen: Wem gehören die Daten im Fahrzeug? Das moderne Fahrzeug – Messgerät, Steuergerät, Datenspeicher“, in: Deutscher Verkehrsgerichtstag (Hg.): Tagungsband des 52. Deutschen Verkehrsgerichtstags 2014, Köln, 2014, 229-239.

Bönninger, Jürgen: Wem gehören die Daten im Fahrzeug?, zfs 2014, Heft 4, S. 184-189.

Borges, Georg: Haftung für selbstfahrende Autos, CR 2016, Heft 4, S. 272-280.

Brisch, Klaus / Müller-ter Jung, Marco: Autonomous Driving – Von Data Ownership über Blackbox bis zum Beweisrecht, CR 2016, Heft 6, S. 411-416.

Delhaes, D., Fasse, M., Menzel, S.: Berlin will neue Standards setzen, in: Handelsblatt vom 18.07.2016, S. 4-5.

Deutscher Bundestag: Antwort der Bundesregierung auf die kleine Anfrage der Fraktion Bündnis 90/Die Grünen - Datenzugriff und Datenschutz bei digitalisierten und vernetzten Fahrzeugen, BT-Drucks. 18/10192, unter dip21.bundestag.de/dip21/btd/18/101/1810192.pdf (abgerufen am 10.11.2016).

Frauenhofer-Institut für Arbeitswirtschaft und Organisation (IAO), Hochautomatisiertes Fahren auf Autobahnen – Industriepolitische Schlussfolgerungen – Dienstleistungsprojekt 15/14, Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie, unter https://www.bmwi.de/BMWi/Redaktion/PDF/H/hochautomatisiertes-fahren-auf-autobahnen,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (abgerufen am 23.09.2016).

Grünvogel, Thomas: Rechtslage für autonomes Fahren, unter http://www.cmshs-bloggt.de/emobilitaet/rechtslage-fuer-autonomes-fahren-in-deutschland/ (abgerufen am 05.10.2016).

Haustein, Berthold, Datenschutzrechtskonforme Ausgestaltung von Dashcams und mögliche Ableitungen für den autonomen PKW, in: Taeger, Jürgen (Hg.): Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 43-59.

Hilgendorf, Eric: Automatisiertes Fahren und Recht, in: Deutscher Verkehrsgerichtstag (Hg.): Tagungsband des 53. Deutschen Verkehrsgerichtstags 2015, Köln, 2015, S. 55-73.

Hornung, Gerrit / Goeble, Thilo: „Data Ownership“ im vernetzten Automobil, CR 2015, Heft 4, S. 265-273.

Jaspers, Andreas/Franck, Lorenz: Connected Car und Beschäftigtendatenschutz, RDV 2015, S. 69-73.

Karg, Moritz: Anmerkung zur Entscheidung des VG Schleswig (Urt. v. 09.10.2013 - 8 A 14/12), ZD 2014, Heft 1, S. 51-56.

Kinast, Dr. Karsten/ Kühnl, Christina: Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, Heft 42, S. 3057 - 3060.

Klindt, Thomas (Noerr), Zeitunglesen unerwünscht – Dobrindt-Entwurf setzt vollautonomem Fahren rechtliche Grenzen, unter https://www.noerr.com/de/newsroom/News/zeitunglesen-unerw%C3%BCnscht-%E2%80%93-dobrindt-entwurf-setzt-vollautonomem-fahren-rechtliche-grenzen.aspx (abgerufen am 05.10.2016).

Lutz, Lennart S. / Tang, M. Sc. Tito / Lienkamp, Markus: Analyse der rechtlichen Situation von teleoperierten (und autonomen) Fahrzeugen, unter www.ftm.mw.tum.de/uploads/media/07_Lutz.pdf (abgerufen am 02.11.2016).

Lohmann, Melinda Florina: Erste Barriere für selbstfahrende Fahrzeuge überwunden – Entwicklungen im Zulassungsrecht, www. http://sui-generis.ch/17, Abschnitt III (abgerufen am 05.10.2016).

Mielchen, Daniela: Verrat durch den eigenen PKW – wie kann man sich schützen?, in: Deutscher Verkehrsgerichtstag (Hg.): Tagungsband des 52. Deutschen Verkehrsgerichtstags 2014, Köln, 2014, 241-255.

Neidhart, Hermann: Roboterautos und Wiener Weltabkommen – Mobilitätsrevolution durch vollautomatisiertes Fahren?, ZAP 2016, Heft 10, 503 - 504.

Reibach, Boris: Smart Cars – Smart Privacy Law? Regionale Datenschutzregulierung des KFZ, in: Taeger, Jürgen (Hg.): Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 13-27.

Schulzki-Haddouti, Christiane: IT-Sicherheitsgesetz für Autos in den USA vorgestellt, unter http://www.heise.de/newsticker/meldung/IT-Sicherheitsgesetz-fuer-Autos-in-den-USA-vorgestellt-2761772.html (abgerufen am 02.11.2016).

Schumacher, Volker A.: Update Immaterialgüterrecht, in: Taeger, Jürgen (Hg.): Smart World – Smart Law? Weltweite Netze mit regionaler Regulierung, Edewecht 2016, S. 309-321.

Voßhoff, Andrea: Moderne Kraftfahrzeuge – rollende Datenspeicher?!, in: BfDI, 25. Tätigkeitsbericht zum Datenschutz vom 17.06.2015, S. 208 – 209, unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/25TB_13_14.pdf?__blob=publicationFile&v=10 (abgerufen am 29.08.2016).

Weichert, Thilo: Datenschutz im Auto, in: Deutscher Verkehrsgerichtstag (Hg.): Tagungsband des 52. Deutschen Verkehrsgerichtstags 2014, Köln, 2014, S. 285-312.

Weichert, Thilo: Wer ist für das Internet verantwortlich?, ZD 2014, Heft 1, S. 1-3.